# KRİTİK ALTYAPILARA YÖNELİK SİBER TEHDİTLER VE TÜRKİYE İÇİN SİBER GÜVENLİK ÖNERİLERİ

Bilge Karabacak
Başuzman Araştırmacı
TÜBİTAK-BİLGEM
Bilişim Sistemleri Güvenliği Bölümü
bilge@uekae.tubitak.gov.tr

**Özet**

*Kritik altyapılar devlet ve toplum düzeninin sağlıklı bir şekilde işlemesi için gerekli olan ve birbirleri arasında bağımlılıkları olan fiziksel ve sayısal sistemlerdir. Kritik altyapıların korunması konusu gelişmiş ülkelerin önemli gündem maddelerinden birisidir. Çalışma yapan ülkeler, kritik altyapıların korunması ile ilgili yasal ve teknik çalışmalarda ciddi yol almışlardır. Ülkemizde, kritik altyapılar konusunda resmileşmiş herhangi bir politika veya mevzuat çalışması bulunmamaktadır. Kritik altyapıların güvenliği konusunda ülkemizin önünde uzun bir yol olduğu söylenebilir. Makalede kritik altyapı tanımı yapılmış ve kritik altyapıların siber altyapıya olan bağlılığı konusunda değerlendirmelere yer verilmiştir. Kritik altyapılara yönelik gerçekleştirilen siber güvenlik olaylarına değinilmiştir. Ülkemizin hâlihazırdaki durumu aktarıldıktan sonra kritik altyapı güvenliği için gerçekleştirilmesi gereken çalışmalara yer verilmiştir. Makale, siber tehditler ilgili gelecek öngörüsü ile sona erdirilmiştir.*

***Anahtar Kelimeler:*** *Kritik altyapı, SCADA sistemleri, siber tehdit*

## 1. Giriş

Günümüzde bilgi teknolojileri enerji, sağlık, ulaşım, finans gibi birçok sektörde temel iş süreçlerinin sayısallaştırılması ve otomasyonunda kullanılmaktadır. Kurumların ve bireylerin bilgi ve iletişim teknolojilerine bağımlılığı gün geçtikçe artmaktadır. Bilgi teknolojileri, devlet ve toplum düzeninin sağlanması adına kritik bir rol üstlenmiş durumdadır. Bilgi ve iletişim teknolojilerin sağladığı birçok faydanın yanı sıra bu teknolojiler ile birlikte yeni bir tehdit türü olarak siber tehditler hayatımıza girmiştir. Siber tehditlerden korunmak için birey seviyesinden ülke seviyesine kadar alınması gereken karşı önlemler bulunmaktadır. Ülke seviyesinde gerçekleştirilmesi gereken önemli çalışmalardan birisi de kritik altyapıların korunması (Critical Infrastructure Protection-CIP) başlığı altına değerlendirilmektedir. Bu kapsamda bir devlet politikası olarak belirlenen adımlar ülkede faaliyet gösteren kritik altyapı işletmecileri tarafından gerçekleştirilmektedir.

Kritik altyapı terimi ilk defa 15 Temmuz 1996 tarihli Amerika Birleşik Devletleri Başkanlık Emri'nde kullanılmıştır [1]. Bu başkanlık emrinin ardından Ekim 1997'de "Amerika Birleşik Devletleri Başkanlık Komisyonu'nun Kritik Altyapıların Korunması Hakkında Raporu" hazırlanmıştır [2]. Yeni bir kavramı tanıtmak ve bu kavram hakkında bilgilendirme yapmak amacıyla hazırlanan Başkanlık Komisyonu Raporu'ndan yedi ay sonra "Başkanlık Karar Direktifi" dönemin başkanı Bill Clinton tarafından 22 Mayıs 1998 tarihinde imzalanmıştır [3, 4]. Bu direktif, Amerika Birleşik Devletleri'nin kritik altyapılarını işleten tüm kurumlarına (kamu ve özel sektör) gönderilmiştir. Söz konusu direktifte kritik altyapılar ekonominin ve devletin sağlıklı bir işlemesi için ciddi öneme sahip olan fiziksel ve siber sistemler olarak tanımlanmıştır. Ayrıca kritik altyapıların kamu ve özel sektör tarafından işletilen iletişim, enerji, finans,

ulaşım, su sistemleri, acil durum servislerini kapsadığı ancak bu sistemlerle de sınırlı olmadığı ifade edilmiştir. Direktifte ulusal hedefler, kritik altyapıların listesi, kurumların gerçekleştirmesi gereken adımlar, eşgüdüm ile ilgili hususlar, yeni yapılanmalar ve ulusal koordinatör ile ilgili bilgilere yer verilmiştir. Başkanlık karar direktifinde, geçmiş senelerde kritik altyapıların fiziksel ve mantıksal olarak ayrı ve bu nedenle bağımlılığı olmayan sistemler olduğu belirtilmiş, bilgi teknolojilerindeki gelişmelerin hem altyapıların kendisini etkilediğini hem de altyapılar arasındaki ilişkileri ve bağımlılığı ciddi bir şekilde artırdığı ifade edilmiştir. Başkanlık Karar Direktifi'nin ardından Amerika Birleşik Devletleri'nde gerek kamu sektöründen gerekse özel sektörden kritik altyapı işletmecileri altyapıların güvenliğinin sağlanması ile ilgili koordineli çalışmalara başlamışlardır.

Ülkemiz, kritik altyapılarını henüz belirlemiş durumda değildir. Bu nedenle, kritik altyapıların birbirleri ile olan ilişkileri, bu altyapıların bilgi teknolojilerine bağımlılıkları, kritik altyapıların barındırdığı fiziksel ve sayısal açıklıklar ve kritik altyapılara yönelik siber tehditlerin kabiliyetleri konusunda da veri bulunmamaktadır. Gelişmiş birçok ülke kritik altyapıların korunması ile ilgili programlar yürütmektedir. Bu programlarda, siber tehditler ve bu tehditlere karşı alınması gereken karşı önlemler çok önemli bir yer tutmaktadır. Ülkemizde de kritik altyapıların korunması ile ilgili çalışmalar gerçekleştirilmelidir.

Makalenin ikinci bölümünde siber altyapının kritik altyapılar içerisinde yeri ve önemi anlatılmıştır. İkinci bölümde kritik altyapıları kontrol etmek ve izlemek amacıyla kullanılan SCADA (Supervisory Control and Data Acquisition) teknolojisinden bahsedilmiş ve siber tehditlerin SCADA sistemlerini kullanarak kritik altyapılara verdiği zararlar örnek olaylarla anlatılmıştır. Makalenin üçüncü bölümünde ülkemizde kritik altyapılar konusunda geçmiş senelerde gerçekleştirilen çalışmalar özetlenmiş ve ülkemizin hâlihazırdaki durumu ortaya konmuştur. Makalenin dördüncü bölümünde ülkemizde gerçekleştirilmesi gereken teknik ve yasal çalışmalar ayrıntılı olarak aktarılmıştır. Makalenin beşinci bölümü sonuç bölümüdür. Sonuç bölümünde siber tehditler ile ilgili gelecek öngörüsü yapılmış ve sonuç ifadelere yer verilmiştir.

## 2. Siber Altyapı, Siber Tehditler ve SCADA Sistemleri

Bilgi teknolojileri istisnasız olarak bütün kritik altyapılarda kullanmaktadır. İletişim altyapısı, Internet altyapısı gibi kritik altyapılar tamamen bilgi teknolojilerinden oluşmaktadırlar. Bankacılık, acil durum servisleri gibi kritik altyapılar bilgi teknolojilerini yoğun şekilde kullanmaktadırlar. Enerji üretim tesisleri, barajlar gibi kritik altyapılar SCADA olarak adlandırılan ve bu yapıları kontrol eden ve izleyen bilgi teknolojilerini içermektedirler. Sonuç olarak, bilgi teknolojilerinin kritik altyapılar için bir siber altyapı oluşturduğu söylenebilir. Bu siber altyapının en önemli aktörü ise Internet olarak karşımıza çıkmaktadır; Amerika Birleşik Devletleri'nde kritik altyapılar, verimlilik ve kullanılabilirliği artırdığı ve maliyetleri düşürdüğü için gün geçtikçe Internet ile daha çok bağlantılı hale gelmektedir [5].

Barajlar, termik santraller, enerji dağıtım üniteleri gibi kritik altyapıların yönetimi ve izlenmesinde uzun yıllardan bu yana SCADA olarak adlandırılan endüstriyel kontrol sistemleri kullanılmaktadır [6]. Yetmişli ve seksenli yıllarda SCADA sistemlerinin başka ağlar ile bağlantısı yoktu, dokümante edilmemişti, herkes tarafından bilinen bilgi ve iletişim teknolojilerini içermemekte; bunun yerine altyapıya özel olarak geliştirilmiş

teknolojileri içermekteydi. SCADA sistemleri günümüzde yaygın olarak kullanılan ve bilinen standart yazılım, donanım, işletim sistemi ve ağ protokollerini barındırmaya başlamıştır. Ayrıca, kritik altyapıları yöneten ve izleyen birçok SCADA sistemi kurumsal ağlara ve Internet'e bağlantılı hale gelmeye başlamıştır [5]. Sonuç olarak, SCADA sistemleri sayısal savaşa ve sayısal terörist ataklarına çok daha fazla bir şekilde açık duruma gelmiş ve güvenlikleri geçmişe göre ciddi şekilde sorgulanmaya başlamıştır [7, 8, 9]. Internet fiziksel olarak milyonlarca alt ağdan oluşan ancak mantıksal olarak birleşik bir alandır. Internet erişimi olan bir kurum veya kişi aslında Internet erişimi olan milyonlarca diğer nokta ile iletişim halindedir. Bu hem çok büyük bir avantajdır; hem de siber tehdit açısından bakıldığı zaman korkunç bir gerçektir. Çünkü artık günümüzde kritik altyapıların bağlantılı hale getirildiği Internet aynı zamanda siber teröristlerin ve bilgisayarlar korsanlarının da kullandığı bir ortamdır.

Kuzeydoğu Elektrik Kesintisi, kritik altyapıların bilgi teknolojilerine bağımlılığını ortaya koymak için oldukça çarpıcı bir örnektir. Kuzeydoğu Elektrik Kesintisi, Amerika Birleşik Devletleri'nin sekiz eyaletinde ve Kanada'nın bazı şehirlerinde 50 milyon kişiyi etkileyen, bazı şehirlerde iki gün süren, 11 kişinin ölümüne ve altı milyar dolar zarara yol açan Amerika Birleşik Devletleri tarihinin en ciddi elektrik kesintisidir. "Kuzeydoğu Kesintisi 2003" olarak tarihe geçen olay bir dizi hatanın ve teknik arızanın aynı anda yaşanması sonucu oluşmuştur. Arızalardan birisinin de, enerji yönetim sisteminde kullanılan bir yazılımdaki böcek (bug) olduğu tespit edilmiştir [10].

Siber uzaydaki tehditler asimetrik tehditlerdir. Tehditlerin asimetrikliğine katkı yapan en önemli iki unsur anonimlik ve elde edilebilirliktir. Bir kritik altyapıyı hedef alan ve ciddi bir zarara yol açan siber saldırı yan dairede bulunan bir kişisel bilgisayardan veya alışveriş merkezindeki kablosuz ağı kullanan bir diz üstü bilgisayardan yapılmış olabilir. Saldırıyı gerçekleştiren siber teröristleri bulmak neredeyse imkânsız olabilir. Örneğin, yan dairedeki komşumuz gerçekte suçsuz olabilir. Bilgisayar, delil bırakmak istemeyen siber teröristler tarafından ele geçirilmiş olabilir. Siber araçların mali açıdan elde edilebilirliği diğer gerçek savaş ekipmanları ile karşılaştırılmayacak kadar düşüktür. Bir sıcak savaşta kritik altyapılara zarar verebilecek bir bombardıman uçağının maliyeti 100 milyon dolarken ve bu uçağı parası olan herkes elde edemezken, kritik altyapılara zarar vermek için kullanılabilecek yazılım ve donanımlara sadece 1000 dolar karşılığında ve zahmetsiz bir şekilde sahip olunabilir.

İkisi Amerika Birleşik Devletleri'nde biri de yoğun olarak İran'da gerçekleşmiş olan ve kritik altyapıları hedef alan üç adet siber saldırı, asimetrik tehditlerin verebileceği zararları anlamak açısından faydalı olacaktır. Ağustos 2001'de Amerika Birleşik Devletleri'nin Kaliforniya eyaletinin büyük kısmına elektrik dağıtımında kullanılan bilgisayar sistemine siber saldırganların yetkisiz bir şekilde girdiği medyada yer almıştır. Sızmanın iki hafta boyunca gerçekleştiği tespit edilmiştir. Elektrik dağıtımında kullanılan SCADA sistemine Internet'ten erişilebilmektedir. Sızmaya sebep olan sistem açıklığının bilgisayar korsanları sisteme herhangi bir zarar vermeden kapatıldığı bildirilmiştir. Olay enerji endüstrisinde yaşanan ilk siber saldırılardan birisi olduğu için ciddi bir şok dalgası yaratmıştır.

İkinci olay Ağustos 2003'te gerçekleşmiştir. Ohio eyaletindeki Davis-Besse nükleer santralindeki özel bir bilgisayar ağına "Slammer" isimli zararlı yazılım bulaşır ve bu zararlı yazılım güvenlik izleme sistemini beş saat boyunca devre dışı bırakır. Basında yer alan haberlere göre santral personeli kurum

ağı önünde yer alan güvenlik duvarı tarafından korunduklarını düşünürken bu olayın gerçekleşmesi şaşkınlığa yol açmıştır. Bu örnekte de santralin özel bilgisayar ağı Internet ile bağlantılı durumdadır. Güvenlik duvarları Internet'ten gelen tehditlere karşı %100 koruma sağlamaz. Güvenlik duvarları servis bazında kısıtlama sağlarlar. İzin verilen servisler üzerinden yapılan sızmaları ve illegal siber aktiviteleri güvenlik duvarları tespit edilip engellenmeyebilir.

Üçüncü örnek, ilk iki siber olaydan çok farklı bir kategoridedir. Üçüncü örnek Stuxnet isimli SCADA sistemlerine yönelik programlanmış olan ve en karmaşık siber silah olarak nitelendirilen zararlı yazılımdır. Stuxnet, SCADA sistemler için yazılmış bilinen ilk zararlı yazılımdır. Özellikle İran'ın nükleer tesislerini etkilemiştir. Bilgi güvenliği uzmanları böylesine karmaşık bir yazılımın ancak ulusal düzeyde bir çabayla yazılmış olabileceğini ve bağımsız bilgisayar korsanlarının başaramayacağı bir çalışma olduğu belirtmişlerdir. Stuxnet yazılımı, İran'ın nükleer enerji altyapısını hedef alan bir yazılım olarak uzunca bir süre bilgi ve enerji güvenliği profesyonellerinin gündemini meşgul etmiştir. Zararlı yazılım Temmuz 2010'da keşfedilip tanımlanmıştır. Ağustos 2010 tarihi itibarıyla dünyada etkilenen bilgisayarların %60'ının İran'da olduğu tespit edilmiştir [11]. Stuxnet, İran'ın Natanz şehri uranyum işleme merkezindeki santrifuj sistemlerini ve Bashehr şehrindeki nükleer reaktör türbinlerini hedef almıştır. Bu ekipmanların kontrol sistemlerini ele geçirmiş ve operatörler tarafından kullanılamaz duruma getirmiştir. Stuxnet'in daha önce hiç bir zararlı yazılımda görülmeyen özellikleri tespit edilmiştir. Öncelikle, sadece nükleer santrallerde kullanılan belli marka ve model SCADA sistemlerini hedef alan bir yazılımdır. Eğer bulaştığı bilgi sisteminde hedef aldığı SCADA sistemi yoksa kendisini etkisiz hale getirmekte ve sisteme bir zarar vermemektedir. Zararlı yazılımların hazırlanmasında yaygın olarak kullanılmayan bir programlama diliyle hazırlanmıştır. Microsoft Windows işletim sisteminin o zamana kadar bilinmeyen dört adet açıklığını aynı anda kullanmıştır. Ayrıca, işletim sistemi seviyesinde güvenin oluşması ve kolaylıkla yayılması için Güney Kore'deki iki adet firmaya ait sayısal sertifikaların gizli anahtarlarını kullanmıştır. Stuxnet yazılımı tespit edilince yapılan inceleme sonucunda bu anahtarların çalındığı ortaya çıkmıştır. Bu özelliklerinde de görüldüğü üzere Stuxnet kendisinden önceki zararlı yazılımların hiç birisine birçok yönden benzememektedir. Gerek bu özellikleri gerekse hedef aldığı sistemler göz önüne alındığı zaman bireylerden ziyade ülkeler seviyesinde bir çalışma sonucunda oluşturulmuş olması küçük bir ihtimal değildir.

Stuxnet'in amacı, kendini gizleyerek SCADA sistemlerinin kontrolü ele almak ve SCADA sistemlerini çalışmaz duruma getirmekti. Diğer taraftan, SCADA sistemlerinin çalışmasını engellemeyen, kendisini belli etmeden çalışan, aynı zamanda uzun süreli istihbarat toplayan ve kendisinden önceki yazılımlardan dersler çıkarılarak hazırlanmış bir yazılımın vereceği zararlar çok daha ciddi olacaktır.

## 3. Türkiye'deki Durum

Ülkemizde, kritik altyapılara yönelik olarak herhangi bir yasal düzenleme bulunmamaktadır. Hâlihazırda bir mevzuat çalışması da yapılmamaktadır.

Geçtiğimiz senelerde, kritik altyapıların korunmasını içeren bilgi güvenliğine yönelik iki adet çalışma yapılmış ancak bu çalışmalar sonuca ulaşmamıştır. Bu çalışmalardan ilki Ulusal Sanal Ortam Güvenlik Politikası hazırlanması çalışmalarıdır. Estonya bilgi sistemlerine Rus bilgisayar korsanları tarafından Nisan ve Mayıs 2007'de koordine ataklar gerçekleştirilmiştir. Bu ataklar,

Dünya'da yaşanan ilk siber savaş olarak nitelendirilmiştir. Bu ataklardan sonra NATO Sayısal Savunma Konsept belgesi hazırlanmıştır. Bu belgenin bir gereği olarak NATO üyesi ülkeler Sanal Ortam Savunma Politikalarını hazırlamaya başlamışlardır. NATO'nun Sanal Ortam Savunma Politikası hazırlanması talebi Dışişleri Bakanlığı tarafından Başbakanlık'a iletilmiş, Başbakanlık Mayıs 2008'te söz konusu politikanın TÜBİTAK koordinasyonunda hazırlanmasını resmen talep etmiştir. Politika dokümanı TÜBİTAK ile birlikte 19 adet kamu kurumunun katılımı ile hazırlanmıştır. Politika belgesi hazırlanması çalışmalarına katılacak kurum listesi, Başbakanlık tarafından koordinatör kurum olarak TÜBİTAK'a bildirilmiştir. Bu kurumlar, Cumhurbaşkanlığı, Başbakanlık, Genelkurmay Başkanlığı, Dışişleri Bakanlığı, Adalet Bakanlığı, Milli Savunma Bakanlığı, Maliye Bakanlığı, Ulaştırma Bakanlığı, İçişleri Bakanlığı, Devlet Planlama Teşkilatı Müsteşarlığı, Dış Ticaret Müsteşarlığı, Hazine Müsteşarlığı, Merkez Bankası, Milli Güvenlik Kurulu Genel Sekreterliği, Milli İstihbarat Teşkilatı Müsteşarlığı, Bankacılık Düzenleme ve Denetleme Kurumu, Emniyet Genel Müdürlüğü ve Bilgi Teknolojileri ve İletişim Kurumu'dur. Politika dokümanı, Temmuz 2008 – Kasım 2008 ayları arasında hazırlanmış; bu sürede tüm kurumların katıldığı üç adet toplantı gerçekleştirilmiştir. Üçüncü toplantının ardından, politika belgesinde son düzenlemeler yapılmış, katılımcı kamu kurumlarının çoğunluğunun onayı ile belge Başbakanlık'a Ocak 2009'da resmi olarak teslim edilmiştir. Hâlihazırda, Başbakanlık'ın belgeyi onaylaması beklenmektedir. Ülkemizde kritik altyapıların güvenliği ile ilgili atılmış ilk adım bu politika belgesidir. Politika belgesinde "Ulusal kritik bilgi ve iletişim altyapıları tespit edilecek ve bu altyapılar sanal ortamdan gelecek tehdit ve saldırılara karşı korunacaktır. Ayrıca, ülke içerisindeki kritik bilgi ve iletişim sistem altyapıları, bunların birbirleriyle ilişkileri, kritiklik seviyeleri ve sorumluları da tespit edilecektir." ifadeleri yer almaktadır. Ayrıca "Kritik bilgi ve iletişim sistem altyapısına sahip kurumlar için personelin ve kurumun sahip olduğu teknik birikim, imkân ve kabiliyetlerin artırılması sağlanacaktır." ifadesi de politika belgesinde yer almaktadır. Belgede "Ulusal Kritik Bilgi ve İletişim Sistem Altyapısı"; işlediği bilginin gizliliği, bütünlüğü veya sürekliliği zarara uğradığı takdirde,

a. Askeri, milli, kültürel, toplumsal ve iletişimsel güç unsurlarının,
b. Ülke ekonomisinin,
c. Halk sağlığının,
d. Kişisel mahremiyetin,
e. Kamu emniyetinin ve kamu düzeninin,

zarar görmesine yol açabilecek sistemler ve bu sistemleri oluşturan altyapılar olarak tanımlanmıştır.

Ülkemizde kritik altyapıların güvenliğini içeren ikinci çalışma bir mevzuat çalışmasıdır. Bu çalışma 2009 sonbaharında gerçekleştirilmiştir. Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü bünyesinde oluşturulan ve çalışmalarına fiilen 3 Mart 2009 tarihinde başlayan e-Mevzuat Çalışma grubu, 7 Ağustos 2009 tarihi itibarıyla "e-Devlet ve Bilgi Toplumu Kanun Tasarısı Taslağı"nı hazırlamıştır. E-devlet ve Bilgi Toplumu Kanun Tasarısı Taslağı'nda kritik altyapı ve kritik bilgi altyapısı terimleri geçmemiş; bunun yerine "Kritik Bilgi Sistemi" ifadesi kullanılmıştır. Taslak içerisinde "Kritik Bilgi Sistemi"nin tanımı "İşlevlerinin tamamen veya kısmen yerine getirilememesi halinde kamu güvenliği ve düzenini önemli derecede etkileyen bilgi sistemleri" olarak tanımlanmıştır. Kanun taslağında geçen "Bilgi Toplumu Ajansı" içerisindeki "Bilgi Toplumu Dairesi"nin

görevlerinden bir tanesi de "kritik bilgi sistemlerini belirlemek ve bu sistemler için uygulanacak asgari güvenlik standartlarını tespit etmek" şeklinde belirtilmiştir. Söz konusu kanun tasarısı ile ilgili olarak da 2009 sonbaharından bu tarihe kadar herhangi bir gelişme olmamıştır. Sonlandırılmamış olan bu iki taslak çalışma dışında ülkemizde kritik altyapılar konusunda resmi bir çalışma bulunmamaktadır.

Bu iki çalışmanın yanı sıra kritik altyapı işletmecilerinin katılımı ile yapılan ve Ocak 2011'de düzenlenen Ulusal Siber Güvenlik Tatbikatı'ndan bahsetmek uygun olacaktır. TÜBİTAK BİLGEM UEKAE (Ulusal Elektronik ve Araştırma Enstitüsü) ve Bilgi Teknolojileri ve İletişim Kurumu koordinasyonunda gerçekleştirilen hazırlık çalışmaları 2010 yılı Şubat ayında başlamıştır. Tatbikatın planlanma süreci yaklaşık bir yıl sürmüştür. Bu süreçte tatbikata katılacak taraflar davet edilmiş, ilgili taraflarla görüş alışverişinde bulunulmuş ve tatbikatın düzenleneceği yerin belirlenmesiyle lojistik ihtiyaçların karşılanması için çalışmalar yapılmıştır. Bu çalışmalara paralel olarak gerçekleştirilecek saldırıların ve yazılı enjeksiyonların planlaması yapılmıştır. Ulusal Siber Güvenlik Tatbikatı 2011, finans, bilgi teknolojileri ve iletişim, eğitim, savunma, sağlık sektörlerinin; adli birimlerin, kolluk kuvvetlerinin ve çeşitli bakanlıkların ilgili birimlerinin temsilcilerinden oluşan 41 kamu kurumunun, özel sektör kuruluşunun ve sivil toplum kuruluşunun katılımıyla 25-28 Ocak 2011 tarihlerinde gerçekleştirilmiştir. Tatbikatta katılımcı kurum/kuruluşlardan bilişim, hukuk ve halkla ilişkiler uzmanı statüsündeki 200'e yakın personel görev almıştır. Katılımcı kurumların siber saldırı durumunda verecekleri tepkilerin gerçek ortamdaki ve simülasyon ortamındaki saldırılarla ölçülmesiyle, kurumların hem teknik kabiliyetleri hem de kurum içi ve kurumlar arası koordinasyon yetenekleri değerlendirilmiştir.

25-28 Ocak 2011 tarihleri arasında gerçekleştirilen Ulusal Siber Güvenlik Tatbikatı 2011'in (USGT – 2011) ilk iki günlük bölümünde katılımcılar çalışmalara kendi kurumlarından katılmıştır. USGT - 2011'in son iki günlük bölümü ise toplu halde TOBB Ekonomi ve Teknoloji Üniversitesi (ETÜ) Konferans Salonu'nda gerçekleştirilmiştir. USGT – 2011'de katılımcı kurumların teknik kabiliyetlerini tespit etmek ve kurumlara olası saldırılara karşı müdahalede deneyim kazandırmak amacıyla hem gerçek saldırılar hem de yazılı ortamda senaryolar gerçekleştirilmiştir.

USGT – 2011 kapsamında, hem yazılı ortamda gerçekleştirilen senaryolar, hem de gerçek saldırılar sonucunda bazı temel eksiklikler tespit edilmiştir. Bu eksiklikler arasında, sistem yöneticilerinin teknik yetersizliği, sistem yöneticilerinin bilgi güvenliği boyutunda yetersizliği, kurumsal bilgi güvenliği yönetim sistemi eksikliği, kurum içi koordinasyonun yetersizliği ve sistem tasarımı aşamasında güvenliğin göz ardı edilmesi dikkat çekmektedir. Bu eksikliklerin, kritik altyapı işletmecisi kurumlarda bulunması doğrudan kritik altyapıların güvenliğini etkileyebilecek birer unsur olarak karşımıza çıkmaktadır.

Kritik altyapıların güvenliği konusunda ilerleme kaydetmiş ülkelerin çalışmaları incelendiği zaman, çalışmaların temelini tüm kritik altyapıları birden kapsayan hükümet çalışmaları olduğu görülmektedir. Tüm kritik altyapıları içerisine alan bir çerçeve çalışma ile temel atılmadığı durumda -makalenin ilk bölümünde ifade edilmiş olan ilişkilerden ve bağımlılıklardan dolayı- birçok hususun gözden kaçacağı ve eksik bir çalışma olacağı değerlendirilmektedir. Amerika Birleşik Devletleri'nin tüm kritik altyapıları içine alan çalışmaları makalenin birinci bölümünde

aktarılmıştı. Bu temel çalışmaların ışığında ve çerçevesinde kritik altyapı işletmecisi kurumlar sektörlere özel çalışmalar yapmışlar ve ciddi yok kat etmişlerdir.

## 4. Yapılması Gereken Çalışmalar

Kritik altyapıların güvenliğine yönelik farklı seviyelerde yapılması gereken birçok çalışma bulunmaktadır. Bu çalışmaların bir kısmı mevzuat çalışmaları gibi tüm ülkeyi ilgilendiren çalışmalarken bir kısmı da bireylerin yapması gereken teknik çalışmalardır. Bu başlık altındaki karşı önlemler, gelişmiş ülkelerin ve uluslararası organizasyonların hazırlamış oldukları kılavuz dokümanlardan faydalanılarak hazırlanmıştır. [3, 12, 13, 14].

OECD ve NATO üyesi ülkelerin birçoğunun hükümetler seviyesinde tanımlanmış kritik altyapıların korunması programı bulunmaktadır. Bu ülkelerde kritik altyapıların korunması ülke mevzuatı içerisine girmiştir. 2007 senesinde hazırlanmış olan bir OECD dokümanında Avustralya, Kanada, Japonya, Güney Kore, Hollanda, İngiltere ve Amerika Birleşik Devletleri'nin kritik altyapıların korunması ile ilgili yaptıkları çalışmalar karşılaştırılmıştır [15]. Kritik altyapılar ile ilgili çalışma yapan ülkelerin tamamı ilk aşamada bütün altyapıları ilgilendiren temel karşı önlemleri belirlemektedir.

Ülkemizde kritik altyapıların korunması ile ilgili olarak gerçekleştirilmesi gereken en öncelikli dört adım sırası ile aşağıdaki gibidir:

- Üst seviye yürütmeden (Örn: Başbakanlık) destek ve katılım
- Destekleyen mevzuatın hazırlanması ve yürürlüğe girmesi
- Kritik altyapıların korunması ile ilgili politika belgesi hazırlanması
- Çalışmalar için yeterli seviyede bütçe ayrılması

Bu dört adet maddedeki adımlar gerçekleşmeksizin kritik altyapıların korunması adına gerçekleştirilecek daha alt seviyedeki adımların başarısızlıkla sonuçlanması kaçınılmazdır [16].

Kritik altyapıların korunması ile ilgili olarak gelişmiş ülkelerde olduğu gibi ülkemizde de resmi çalışmaların başlatılması gerekmektedir. Bu kapsamda, kritik altyapıların korunmasına yönelik politika belgesinin, politika belgesini detaylandıran stratejinin ve eylem planının hazırlanması gerekmektedir. Bütün bu belgeler için destekleyici mevzuat hazırlanmalı, güncellenmesi ve değiştirilmesi gereken hâlihazırdaki mevzuat tespit edilmeli ve değişiklikler yapılmalıdır. Gerek mevzuat gerekse politika belgesi kritik altyapıların korunması için rol ve sorumlulukların belirlenmesinde kritik bir yol oynayacaktır.

Sayısal savunma ile ilgili çalışmaları organize edecek bir ulusal yürütme organı oluşturulmalıdır. Bilgi paylaşımı için hükümet ile kritik altyapı işleticileri (özel veya kamu) arasında ortaklık kurulmalıdır. Yürütme organının asıl sorumluluğu koordinasyon olmalıdır. Kritik altyapıları işleten kamu sektörüne ve özel sektöre yapılması gereken çalışmaları bildirmelidir. Yürütme organının yapacağı ilk çalışmalardan birisi de kritik altyapıların ve aralarındaki bağımlılıkların belirlenmesi için ülke çapında yapılacak risk analizi çalışmasını organize etmek olmalıdır. Yürütme organı, devletin belirlediği politikaları kritik altyapı işletmecilerine uygulatan bir kurum olmalıdır. Yürütme organı hâlihazırdaki düzenleyici ve denetleyici kurum temsilcilerinden oluşmalıdır. Kritik altyapıların göz ardı edilmeyecek önemli bir kısmının özel sektörün işlettiği düşünülürse özel sektör ile işbirliği ve koordinasyon diğer önemli bir çalışma kalemi olarak değerlendirilebilir.

Kullanıcı bilincini artırmak en öncelikli alınması gereken karşı önlemlerden birisidir. Kullanıcı,

bilgi sistemleri ile az veya çok teması olan herkestir. Bilinçlendirme sürekli yapılması gereken bir süreçtir. Uzun süreli eğitimler ile karmaşık kavramları tanıtmak ve "ne" sorusuna yanıt aramak gerekir. Kısa süreli kurslarla, "nasıl" sorusunun cevaplanması ve bu bağlamda işlerin nasıl düzgün bir şekilde yapılacağının öğretilmesi gerekir. Ayrıca, belli bir zaman dilimine sıkıştırılmamış olan sürekli bilinçlendirme faaliyetleri ile "niçin" sorunun personel tarafından yanıtlanabilir duruma getirilmesi gerekir. Sayısal savunma ve kritik altyapıların korunması ile ilgili ulusal bilincin oluşturulması adına çalışmalar da gerçekleştirilmelidir. Kritik altyapıları işleten kurumların gerçekleştirmesi gereken çalışmalardan, vatandaşın yapması gerekenlere kadar birçok konuyu kapsayan bilinçlendirme programı için ulusal medya, Internet siteleri gibi kaynaklar kullanılmalıdır.

Siber olaylara karşı tepki yeteneği geliştirmek amacıyla ulusal çapta bilgisayar olaylarına müdahale ekibi oluşturulmalıdır. Kritik altyapıları işleten kurumlar da etkin bilgisayar olaylarına müdahale ekiplerini oluşturulmalıdırlar. Ayrıca farklı bilgisayar olaylarına müdahale ekipleri arasında koordinasyon yeteneği olmalıdır. Bilgisayar olaylarına müdahale ekiplerinin ülke çapında etkinliği olmalıdır. Hükümetlerle birlikte çalışan, olaylara müdahale eden, hacker gruplarını takip eden ve izleyen ekiplerin faaliyete geçmesi siber güvenlik için önemli bir adım olacaktır.

Internet altyapısının güçlü ve alternatifli bir duruma getirilmesi dağıtık servis dışı bırakma saldırılarından en az seviyede zarar görmek için gereklidir. Telekomünikasyon altyapısı ve Internet önemli kritik altyapılardır. Gelişmiş ülkelerin durumu da göz önüne alındığı zaman kritik altyapılarının çok daha fazla şekilde kritik iletişim altyapısına ve Internet'e bağlı olacağı öngörüsü yapılabilir. Bu bağlamda, Internet servis sağlayıcılarının etkin yönetimi ve koordinasyonu diğer önemli bir karşı önlemdir. Ayrıca, güçlü ve alternatifli Internet altyapısının oluşturulması gerekmektedir.

Ülkemiz sayısal savaş konusunda uluslararası işbirliğine önem vermelidir. Gelişmiş ülkeler ve OECD, NATO gibi organizasyonlar sayısal güvenlik ve sayısal savunma konusunda ciddi yol almışlardır. Türkiye bu tecrübelerden faydalanmalıdır. Tüm dünyayı içine alan ve sınırları olmayan devasa bir ağ durumundaki Internet sayısal saldırıların da kaynağıdır. Ülkemiz bilgi sistemlerine yapılacak bir sayısal saldırının kaynağı başka bir ülkedeki bilgisayarlar olabilir. Uluslararası işbirliği saldırılara karşı kısa sürelerde önlem almak için gerekli bir şarttır. OECD gibi çok uluslu organizasyonların çalışmalarını takip etmek ise ortak politika oluşturmak, standardizasyona kavuşmak ve birlikte çalışma kültürü edinmek için önemli fırsatlar sunmaktadır.

Üst seviyede bir politika ve program dâhilinde yapılmadığı zaman ve ülke çapında bir sahiplenme olmadığı müddetçe teknik seviyedeki karşı önlemlerin süreklilik arz etmesi beklenemez. Diğer taraftan, teknik karşı önlemler, kritik altyapılara yönelik siber saldırıları engelleyen veya zararları en aza indirgeyen olmazsa olmaz karşı önlemlerdir. Ancak, mutlaka belli bir denetim çerçevesi ve sistematik içerisinde gerçekleştirilmelidir. Makalenin dördüncü bölümünde son olarak teknik karşı önlemlere yer verilmiştir.

SCADA sistemlerindeki teknik açıklıkları sürekli olarak takip etmek ve gerekli yamaları yapmak gerekir. Güvenlik marketini yakından takip edip en son çıkmış güvenlik önlemlerinden haberdar olmak ve bu önlemlerden faydalanmak kritik altyapı güvenliği adına kritik bir çalışmadır.

Bilgi güvenliğini sistemler kurulduktan sonra gerçekleştirilmesi gereken adımlar olarak değil; en baştan itibaren dikkate alınması

gereken bir tasarım bileşeni olarak değerlendirmek gerekir. Birçok güvenlik açığının nedeni, güvenliğin en baştan düşünülmemiş olması ve güvenlik çözümlerinin yama mantığı ile sonradan yapılmasıdır. Güvenlik, sistemlere sonradan eklenebilecek bir bileşen olarak görülmemelidir.

Piyasada standart olarak kullanılan ticari yazılımlardan veya yabancı firmalara yaptırılan yazılımlardan ziyade mümkün olduğu kadar SCADA sistemlerine özel olarak tasarlanmış yazılımların milli imkânlarla geliştirilmesi de bir diğer güvenlik önlemidir. Böylece açıklıkların birçok kişi tarafından bilinip keşfedilmesinin önüne geçilmiş olacaktır. Amaca uygun milli yazılımların kolaylıkla geliştirilebilmesi için kritik altyapıların güvenliği ile ilgili araştırma ve geliştirme faaliyetlerinin başlatılması ve bu faaliyetlerin desteklenmesi gerekir. Siber güvenlik konusunda araştırma ve geliştirme faaliyetlerinin yapılması ve bu faaliyetlerin finanse edilmesi faaliyetlerinin bir devlet politikası olması gerekir. Bir araştırma geliştirme faaliyeti sonucu olarak; ortak kullanılabilecek ve tutarlı bilgiler içeren siber güvenlik kılavuzları hazırlanmalı, standartlara katkı yapılmalı ve iyi pratikler belirlenmelidir.

Güvenlik sertifikası almış yazılım ve donanımların kullanımı da SCADA sistemleri için dikkat edilmesi gereken diğer bir hususdur. Bilgi işleyen yazılım ve donanımlar için Ortak Kriterler (Common Criteria) standardı dünyada genel kabul görmüş bir güvenlik değerlendirme ve sertifikalandırma standardıdır.

Bilgi güvenliği ihlallerinin çoğunluğu yetkisiz kullanımdan kaynaklanmaktadır. Sadece yetkili personele işini yapacak kadar sınırlı alanda yetki verilmesi ve bunun profesyonel bir yazılım ile takip edilmesi de güvenliği artıracak diğer bir hususdur.

Kritik altyapıyı kontrol eden SCADA sisteminin Internet'e bağlı olmasının gerçekten bir gereksinim olup olmadığı gözden geçirilmelidir. "Internet'e bağlı olmasının getirdiği faydalar, getirdiği risklerden fazla mıdır?", "kritik altyapının Internet'e bağlı olmadığı durumda oluşan maliyet karşılanabilecek bir maliyet midir?" gibi soruların yanıtı aranmalıdır. Bu konuda bir durum analizi ve risk analizi yapılmalıdır.

Kritik altyapının açıklıklarını belirlemek ve gerekli önlem almak için periyodik güvenlik testleri ve tatbikatlar düzenlenmesi diğer kritik bir karşı önlemdir. SCADA sistemlerinin bağımsız kuruluşlar tarafından periyodik olarak test ve denetimden geçirilmesi güvenliği ciddi şekilde artıracaktır.

Son olarak taşınabilir USB depolama cihazları ile ilgili sıkı politikaların uygulanması gerekmektedir. Stuxnet'in sıkı bir şekilde korunan belki de Internet'e bağlı olmayan İran nükleer santralinin SCADA sistemlerine USB depolama cihazı yardımı bulaşmış olma ihtimali yüksektir. Personel, evindeki Internet'e bağlı bilgisayarında kullandığı USB depolama cihazını nükleer santral kontrol bilgisayarlarında da kullanmış olabilir. SCADA sistemlerinde kurumsal kriptografik yazılımlardan güvenlik duvarlarına, saldırı önleme sistemlerinden biyometrik güvenliğe kadar birçok karşı önlem kullanıyor olsa da en zayıf halka prensibi bilgisayar güvenliğinde de karşımıza çıkmaktadır. En zayıf halka insandır ve sistemlerin güvenlik seviyesi insanların bilinç seviyesi kadar olmaktadır. Sistem kullanıcılarının ve teknik sistem yöneticilerinin bilerek veya bilmeden yaptıkları basit hatalarla birçok karmaşık güvenlik önleminin pratikte bir faydası kalmamaktadır. Bilgisayar ağının önüne ne kadar güvenlik duvarı, saldırı önleme sistemi konulsa da, SCADA sistemini kullanan bir operatör evinde kullandığı bir USB depolama cihazını SCADA bilgisayarına takarsa o sistemi tehditlere açık hale getiriyor

demektir. Gerçekten de USB depolama cihazları zararlı yazılımların bulaşmasında çok büyük pay sahibidir. Çünkü bu cihazlar, hemen hemen herkes tarafından kullanılmaktadır. Bu cihazlar yardımı ile farklı güvenlik seviyesindeki iki bilgi sistemi arasında veri taşıma oldukça pratikleşmiştir.

## 5. Sonuç

Önümüzdeki zaman diliminde Stuxnet benzeri kritik altyapıları hedef alan siber silahlar üretilecektir. Stuxnet bir başlangıçtı ve devamı gelecektir. SCADA sistemlerine yönelik siber saldırılarda ve servis dışı bırakma girişimlerinde artış olması da olasıdır. Bu siber ataklara, gizlice, açıkça veya dolaylı olarak hükümetler sponsor olacaklardır. Eğer bir devletin veya hükümetin siber yeteneği yeterli değilse, yetenekli bilgisayar korsanları para karşılığı çalıştırılacaktır. Bu "outsource" faaliyeti günümüzde yapılmaya başlanmıştır, daha da yaygınlaşacaktır. Ayrıca, geçtiğimiz aylarda Türkiye gündemine giren "anonymous" gibi hacker gruplarının sayısı ve faaliyetleri önümüzdeki zaman diliminde artacaktır. Din, dil, millet farkı olmaksızın belli bir amaç ve ülkü doğrultusuna ve para almaksızın toplu bir siber taarruz içerisinde bulunmak prestijli bir durum ve bir gençlik başkaldırısı olarak da görülmektedir.

Bütün bu gelecek öngörülerini makalenin ikinci bölümünde yer verilen yaşanmış örneklerle yan yana koyduğumuz zaman gelecek adına kaygılanmamak elde değildir. Eğer yeterli önlemler alınmazsa gelecekte siber saldırıların ciddi sonuçlar doğurması kaçınılmazdır. Makalenin üçüncü bölümünde de ifade edildiği gibi ülkemizde kritik altyapılar belirlenmesi ve güvenliği konusunda hâlihazırda bir çalışma yoktur. Siber tehditler, kritik altyapıları ciddi şekilde etkileyecek bir boyuta gelmiştir. Bu nedenle, makalenin dördüncü bölümündeki karşı önlemlerin hayata geçirilmesi önem arz etmektedir.

**Kaynakça**


[1] Executive Order EO 13010, Critical Infrastructure Protection, http://www.fas.org/irp/offdocs/eo13010.htm, 1996 (10 Ağustos 2011'de erişildi)

[2] The Report of the President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures, 1997

[3] USA Presidential Decision Directive/NCS-63, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm, 1998 (10 Ağustos 2011'de erişildi)

[4] Jones A., "Critical Infrastructure Protection", Computer Fraud & Security, s. 11-15, 2007

[5] Fischer W., Lepperhoff N., "Can Critical Infrastructure rely on the Internet", Computers & Security, Cilt. 24, s. 485-491, 2005

[6] Jayawickrama, W., "Managing Critical Information Infrastructure Security Compliance: A Standard Based Approach Using ISO/IEC 17799 and 27001", Book Chapter: On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Cilt 4277/2006, s. 565-574, 2006

[7] Shea D. A., "Report for Congress, Critical Infrastructure: Control Systems and the Terrorist Threat", 2003

[8] Lemos R., "SCADA System Makers Pushed Toward Security". SecurityFocus. http://www.securityfocus.com/news/11402, 2006 (10 Ağustos 2011'de erişildi)

[9] Maynor D., Graham R., "SCADA Security and Terrorism: We're Not Crying Wolf", Blackhat Conference, http://www.blackhat.com/presentations/bh-

federal-06/BH-Fed-06-Maynor-Graham-up.pdf, 2006 (10 Ağustos 2011'de erişildi)

[10] Andersson G., Donalek P., Farmer R., Hatziargyriou N., Kamwa I., Kundur P., Martins N., Paserba J., Pourbeik P., Sanchez-Gasca J., Schulz R., Stankovic A., Taylor C., Vittal, V., "Causes of the 2003 Major Grid Blackouts in North America and Europe, and Recommended Means to Improve System Dynamic Performance", IEEE Transactions on Power Systems, Cilt. 20, No. 4, s. 1922-1928, 2005

[11] Chen T. M., "Stuxnet, the Real Start of Cyber Warfare?", IEEE Network, The Magazine of Global Internetworking, Cilt 24, No. 6, s. 2-3, 2010

[12] OECD, Working Party on Information Security and Privacy, "Recommendations of the Council on the Protection of Critical Information Infrastructures", 2008

[13] Commission of the European Communities, "Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience- COM(2009) 149 final", 2009

[14] G8 Principles for Protecting Critical Information Infrastructures, G8 Justice & Interior Ministers, 2003

[15] OECD, Ministerial Background Report, "Development of Policies for Protection of Critical Information Infrastructures", 2007

[16] Karabacak B., Özkan S., "Critical Infrastructure Protection Status and Action Items of Turkey", International Conference on eGovernment Sharing Experiences, eGovShare2009, 8-11 Aralık 2009, Antalya

[17] McDaniel P., McLaughlin S. "Security and Privacy Challenges in the Smart Grid", IEEE Security & Privacy, Cilt 7, No. 3, s. 75-77, 2009

[18] Watson J., "Co-provision in sustainable energy systems: the case of micro-generation", Energy Policy, Cilt 23, No. 17, s. 1981-1990, 2004

# KRİTİK ALTYAPI GÜVENLİĞİNE YÖNELİK ÖZGÜN ÇÖZÜMLER: SANAL HAVA BOŞLUĞU

Ali IŞIKLI

***Abstract – Critical infrastructure control systems are becoming more accessible through Internet with recent improvements in Information and Communication system technologies. Which also results in a open threat of crtitical infrastructures to siber terrorist activities. This paper briefly defines the critical infrastructures, which siber terrorist activities are they facing and how to protect them.***

***Özet* - Bilgi ve iletişim teknolojilerinin gelişmesi, Internet ağının ve kullanımının yaygınlaşması sonucu, geçmişte tek başına çalışan kritik altyapıları kontrol eden ve yöneten sistemler, kurumsal ağlara ve Internet'e bağlı çalışır hale gelmiştir. Bu gelişmenin neticesinde kritik altyapı sistemleri, günümüzde siber terörün hedefi haline gelmiştir. Bu makalede kritik altyapıların tanımı ve bu yapıların siber saldırılara karşı nasıl korunması gerektiği anlatılmaktadır.**

***Anahtar kelimeler*—Kritik Altyapı, Kritik Altyapı Güvenliği, Siber Terörizm, Sanal Hava Boşluğu, Güvenlik.**

## I. GİRİŞ

Kritik altyapılar nelerdir? Kritik altyapılar ile ilgili ortak uluslararası bir tanım bulunmamakla birlikte, her altyapı unsurunu kritik altyapı olarak değerlendirmemek gerekir

Amerika Birleşik Devletleri'nde gerçekleştirilen 11 Eylül 2001 tarihli terrorist saldırıların ardından yasalaşan USA PATRIOT ACT 2001'e (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terorism Act of 2001) göre kritik altyapı, "hasar görmesi veya etkisizleştirilmesi halinde ulusal halk sağlığını, güvenliği, ekonomik güvenliği veya tümünü olumsuz etkileyecek fiziki veya sanal tüm varlık ve sistemler kritik altyapı sistemleri" şeklinde tanımlanmıştır [1].

2004 yılında Avrupa Birliği (AB) Meclisine sunulan "Terörist Saldırılara Karşı Kritik Altyapıların Korunması" başlıklı metinde kritik altyapılar, kesilmesi ve/veya hasar görmesi halinde vatandaşların güvenliği, sağlığı ve ekonomik refahı üzerinde veya üye hükümetlerin etkin ve verimli işleyişi üzerinde ciddi olumsuz etkiler oluşturacak fiziki ve bilgi teknolojileri tesisleri, hizmetleri ve varlıkları olarak tanımlanmış ve aynı yıl içinde Kritik Altyapılar İçin Avrupa Programı (EPCIP: European Programme for Critical Infrastructure Protection) ve Kritik Altyapı Erken Bilgi Ağı (CIWIN: Critical Infrastructure Warning Information Network ) yasalaştırılmıştır [2].

Ülkemizde, Mart 2009 tarihinde başlayan e-Mevzuat çalışma grubu, Ağustos 2009 tarihi itibari ile "e-Devlet ve Bilgi Toplumu Kanun Tasarısı Taslağı"nı hazırlamıştır. Hazırlanan bu kanun taslağında kritik altyapı sistemleri ile ilgili bir çalışma bulunmazken, "Kritik Bilgi Sistemi" başlığında "işlevleri tamamen veya kısmen yerine getirilmemsi halinde kamu güvenliği ve düzenini önemli derecede etkileyen bilgi sistemleri" şeklinde bir tanımlama yapılmıştır [3].

Bu tanımlamalar çerçevesinde, üretimde ve günlük yaşamda sürekli hizmet vermesi gereken; fiziksel ve/veya siber bir saldırıya maruz kaldığında bir ya da birden fazla ülkenin ulusal ve/veya uluslar arası çıkarlarını etkileme, kamu sağlığını tehdit etme, çevre kirliliği, para ve itibar kaybına neden olabilecek potansiyele sahip altyapı unsurları "Kritik Altyapı" olarak tanımlanabilir.

Enerji hatları, bankacılık ve finans, bilgi teknolojileri ve iletişim, ulaşım, kamu sağlığı ve su sevkiyatı gibi hususlar kritik altyapılar için yapılan genel tanım içerisinde yer almaktadır.

Bu çalışmada kritik altyapıların güvenliğini sağlamak üzere ne tür tedbirlerin alınması ve uygulanması gerektiği incelenmiştir. Bildirinin devamında bu incelemenin ayrıntıları anlatılmaktadır.

## II. KRİTİK ALTYAPILARA YÖNELİK SALDIRILAR

Kritik Altyapı tesisleri, stratejik önemleri nedeni ile terörist saldırıların öncelikli hedefleridir.

Bilgi teknolojilerindeki gelişme ve Internet'in yaygınlaşması ile beraber kritik altyapı kontrol sistemleri de değişim göstermiştir. Geçmişte, fiziksel unsurlardan tamamen izole endüstriyel kontrol sistemlerinden oluşan, barajlar, termik santraller, enerji dağıtım üniteleri, uçuş kontrol sistemleri, su dağıtım şebekeleri v.b. kritik altyapıların birçoğu günümüzde, bilgi ve iletişim teknolojileri ile yönetilebilir ve izlenebilir duruma gelmiştir.

Kritik altyapıların yönetimi ve izlenmesinde uzun yıllardan bu yana SCADA (Supervisory Control And Data Acquisition) olarak adlandırılan endüstriyel kontrol sistemleri kullanılmaktadır. Önceleri, başka ağlar ile bağlantısı olmayan, bilgi ve iletişim teknolojileri içermeyen veya altyapıya özel olarak geliştirilmiş teknolojileri içeren SCADA sistemleri, günümüzde yaygın olarak kullanılan ve bilinen yazılım, donanım ve ağ protokollerini barındırmaktadır. Ayrıca, kritik altyapıları yöneten ve izleyen birçok SCADA sistemi kurumsal ağlara ve Internet'e bağlantılı hale gelmeye başlamıştır [4].

Bu gelişmeler ile birlikte günümüzde sıcak savaş senaryolarının yerini kritik altyapı unsurlarına yönelik siber

saldırılar almaktadır.

British Columbia Institute of Technology'den (BCIT) Eric Byres ve arkadaşlarının, 2001-2006 yılları arasında yaptıkları Endüstriyel Güvenlik Olayları Veritabanı (ISID – Industrial Security Incidents Database), 2002 yılı ve sonrasında SCADA sistemlerinde yaşanan güvenlik olaylarında ciddi bir artış olduğunu göstermektedir. 1982'den 2006 yılı ortasına kadar hakkında bilgi topladıkları ve ISID veritabanına kaydettikleri 116 olay ile ilgili olarak Eric Byres ve arkadaşlarının hazırladıkları rapor, literatürde gerçek olayları içeren en önemli kaynak olarak dikkati çekmektedir. Bu rapora göre, 2002 yılı ve sonrasında denetim/otomasyon sistemlerinde yaşanan güvenlik vakalarında ciddi artış olduğunu ve 1982'den bu yana bilgi sahibi olunan toplam 116 olayın78'inin 2002-2006 yılları arasında gerçekleştiği görülmektedir. Yine aynı raporda, 1982-2001 yılları arasındaki 23 güvenlik olayının sadece %26'sı dış kaynaklı ve çoğunluğu kazara iken 2002-2006 döneminde olayların %60'ının dış kaynaklı ve saldırı amaçlı olduğu tespiti yer almaktadır. Kaydedilen bu olayların dışında birçok güvenlik olayı, işletmecilerin, kamuoyunun duyması ve neticesinde itibar kaybı yaşaması gibi endişelerinden ötürü duyurulmamaktadır [5].

Kaydedilen siber saldırılardan bazıları şunlardır:

- 2000 yılında Avustralya'nın Moroochy eyaletinde 28 Şubat ile 23 Nisan tarihleri arasında arıtma tesisinden en az 40 defa pis kanalizasyon suları parklara, nehirlere hatta Hyatt Regency otelinin zeminine bırakılmıştır. Bu kirli sularla Eyaletteki marina yaşamı yok olmuştur.
- 2003 senesinde ABD'nin sekiz eyaletinde 50 milyon kişiyi etkileyen, bazı şehirlerde 2 gün süren, 11 kişinin ölümüne ve 6 milyar dolar zarara yol açan ve tarihe "2003 Northeast Blackout" olarak geçen ABD tarihinin en önemli elektrik kesintisinin nedenlerinden birisinin elektrik dağıtımında kullanılan yazılımda oluşan bir hata olduğu saptanmıştır.
- Ağustos 2003'te Ohio'da faaliyet gösteren, Davis-Besse nükleer santralinin izole bilgisayar ağına Slammer solucanı bulaşmış ve santralin izleme sistemini beş saat boyunca çalışamaz duruma getirmiştir. Internet kaynaklı bilgisayar solucanlarının izole ağlara bulaşması, bu ağların ne derece izole olduğunun sorgulanmasına yol açmıştır.
- Ekim 2003'de ABD'nin en yoğun limanlarından olan Houston Limanı'nın bilgisayar sistemi saldırıya uğramış ve limanın bir süre hizmet vermesi engellenmiştir.
- 2007 Nisan ve Mayıs aylarında, Rus bilgisayar korsanlarının Estonya bilgi sistemlerine sızması, bu sistemlerin faaliyetlerini durma noktasına getirmesi neticesinde ülke çapında ekonomik ve toplumsal zararlar yaşamıştır
- 30 Ocak 2009 tarihinde birçok ülkenin bilgisayar sistemine yayılan ve önemli zararlar veren Conficker virüsü Atatürk Havalimanı'nın dış hatlar terminalinde çalışan bilgisayarları da etkilemiştir.
- 2010 yılı Temmuz ayında keşfedilen ve İran nükleer zenginleştirme programını hedeflediği düşünülen Stuxnet yazılımı, SCADA sistemlerini hedefleyen bilinen en tehlikeli zararlı yazılımdır. Daha önce endüstriyel sistemlere yapılan ataklarda genellikle sistemin ele geçirilmesi, yetkinin kötüye kullanılması gibi ataklar yapılmıştı. Bu atak zararlı yazılım sistemlerine fiziksel zarar veriyor olması ile de bir ilktir.

Yukarıda sayılan ve bunlara ilave edilebilecek daha onlarca saldırı gösteriyor ki yaygın olarak kullanılan SCADA sistemlerinde yönetimsel ve teknik olarak gerekli tedbirler alınmalıdır.

Her şeyden önce kritik altyapı sistemlerine yönelik fiziksel ve/veya siber tehditler konusunda farkındalığın geliştirilmesi gerekmektedir.

Saldırılara sıklıkla maruz kalan- başta Amerika Birleşik Devletleri olmak üzere- devletler ve çeşitli uluslararası kuruluşlar, kritik altyapı güvenliğine yönelik çalışmalar gerçekleştirmiş ve bu altyapıların korunması için gerekli mevzuat ve yasaları çıkartmışlardır. Amerika Birleşik Devletleri USA PATRIOT ACT 2001 ile ulusal kritik altyapı güvenliğini sağlamaktadır. NATO ise Estonya'ya düzenlenen siber ataklardan sonra Sanal Savunma Yönetim Birimi'ni kurmuş (Cyber Defense Management Authority – CMDMA), NATO Sayısal Savunma Konseptini tamamlamış ve yürülüğe almıştır [6]. Avrupa Güvenlik ve İşbirliği Teşkilatı'nın (AGIT) Ekim 2007 tarihinde Madrid'de düzenlenen 15. Bakanlar Konseyi Toplantısı'nda "Kritik Enerji Altyapılarının Terörist Saldırılardan Korunması Kararı" onaylanmıştır [7].

Görüldüğü gibi bir çok ülke ulusal ve/veya uluslar arası çerçevede kritik altyapıların saldırılara karşı korunması yönünde yönetimsel olarak tedbirlerini almışlardır

## III. KRİTİK ALTYAPILARA YÖNELİK SİBER SALDIRILARA KARŞI ALINACAK ÖZGÜN GÜVENLİK ÖNLEMLERİ VE SANAL HAVA BOŞLUĞU SİSTEMİ ÇÖZÜMÜ

Kritik altyapı sistemlerinde kullanılan denetim sistemlerine yönelik elektronik tehditlerin detaylı olarak incelenmesi ve asgari önlemlerin alınması gereklidir. Günümüz kritik altyapı sistemlerinin maruz kalabileceği elektronik tehditler, bilgisayar sistemlerine uygulanabilecek tehditlerden farklı değildir. Bu noktadan hareketle:

- Kritik altyapı sistemlerine olan erişim yöntemleri,
- Kritik altyapı sistemlerinin güncelleme ve destek yönetimleri,
- Yazılım ve yapılandırma hataları karşısında alınacak tedbirler

belirlenmeli, gerekli güvenlik prosedürleri geliştirilmeli; bu prosedürler eksiksiz ve periyodik aralıklar ile uygulanmalıdır.

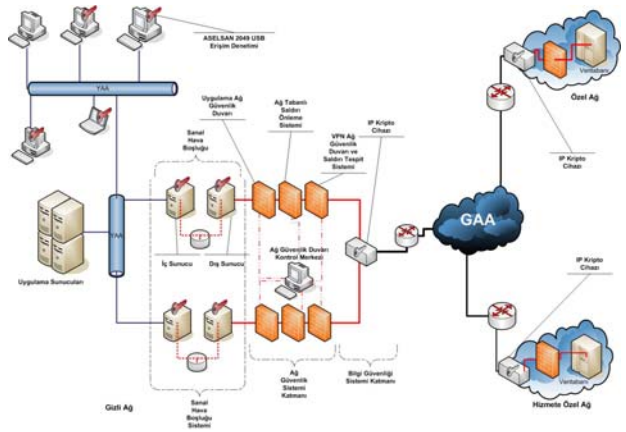
Birçok SCADA sisteminin kurumsal ağlara ve Internet'e bağlantılı hale gelmeye başladığı yukarıda ifade edilmiştir. Gerekli güvenlik tedbirlerini almadan SCADA sistemlerini doğrudan dış bağlantılara açmak tehlikeye davetiye çıkartmaktır. Günümüzde birçok kamu/kurumsal sistem güvenlik duvarları, kurumsal anti virüs yazılımları ile korunmaktadır. Bazı kamusal/kurumsal ağlar dış ağlardan izole bir yapıda hizmet verirken, bazı kamusal/kurumsal ağların dış dünya ile bağlantısı kaçınılmazdır. Bu bağlantı ihtiyacı dışa açılacak ağın maruz kalacağı tehditleri beraberinde getirmektedir.

Yaygın olarak kullanılan güvenlik duvarı anlayışını bir adım öteye taşıyan Sanal Hava Boşluğu Sistemi gerçek zamanlı hizmet alan/veren kuruluşlar için gündemde olan güvenlik tehditlerine karşı durmak ve onları ortadan kaldırmak amacıyla tasarlanmıştır.

Dış ağ (Internet) ile kurum ağı (iç ağ) arasında konuşlandırılan sistem (Şekil.1), kendi içinde TCP/IP tabanlı iletişim kullanmamakta ve böylece iki ağ arasında yüksek düzeyde güvenlik sağlayan bir "Sanal Hava Boşluğu" (Virtual Air Gap) sınırı oluşturmaktadır. Sistemin bu özelliği güvenlik düzeyi yüksek (kritik) görev yapan kurumsal ağlar için düşük güvenlik seviyesine sahip ağlara güvenli olarak bağlanma konusunda arzu edilen bir güvenlik çözümü sağlamaktadır.

SAHAB yönlendirilebilir bir protokolün doğrudan yüksek güvenlik seviyesine sahip ağa erişmesini engellemektedir. SAHAB, üzerlerinde özelleştirilmiş bir işletim sistemi bulunan iç ve dış iki sunucu ve ortaklaşa kullanılan disk ünitesinden oluşmaktadır. Veri akışı ortak disk ünitesi üzerine okuma/yazma şeklinde gerçekleşmektedir.

Günümüzde kurumlar için yerel ağ kavramı artık, iç ağ/dış ağ ayrımı yapılmaksızın, kurumdaki herhangi bir kişiye, herhangi bir yerden erişebilmek anlamında genişlemiştir. Ama bu gelişime paralel olarak, güvenlik uzmanları da ağlarına karşı olan tehditlerle başa çıkabilmek için daha karışık güvenlik politikaları uygulamak zorunda kalmaktadır. Bu tehditlerden en başta geleni, önemli ağ kaynaklarını dış veya yerel ağdan gelebilecek muhtemel saldırılara karşı korumaktır.




Şekil.1 Sanal Hava Boşluğu Sistemi'nin bir ağ sisteminde genel kullanımı.

Ağ güvenliğini korumak tabi ki sadece özellikli kaynaklara erişim denetimi sağlamaktan ibaret değildir. Bundan başka, komple bir ağ güvenliği çözümü:

- Ağ kullanıcıların kimliklerinin belirlenmesi
- Kayıtlı IP'leri optimize şekilde kullanma
- Ağ trafiğinin tümünün içeriğine güvenlik politikasını uygulama
- Saldırıları gerçek zamanlı olarak belirleme ve önlem alma
- Denetim bilgilerinin tümünün kayıtlarını tutma özelliğine sahip olmalıdır.

Ayrıca güvenlik politikası, kurum içerisinde kullanılan mevcut ve ileride kullanılması muhtemel bütün uygulamalara tatbik edilebilmeli ve bağlantı sorunlarına, ağ performans düşüklüklerine yol açmamalıdır.

İlgili kurum/kuruluş tarafından alınacak diğer güvenlik önlemleri gereğince, SAHAB sistemin dışında ve ona ek olarak çeşitli diğer güvenlik teknolojilerin dış ve iç ağ üzerinde barındırılması da mümkündür. Sistem tasarımı kurumsal ağ üzerinde konuşlandırılmış olan, kurumca uygulanan diğer güvenlik önlemleri ile tümleşik çalışabilecek şeklide gerçekleştirilmiştir.

## IV. SONUÇ

Ülkemizde kritik altyapı ve güvenlik bilincinin henüz olgunluk seviyesine ulaşmadığı, üst düzey devlet yönetimince konu ile ilgili olarak yeterli ve ciddi çalışmaların henüz gerçekleştirilmemesi ile ifade edilebilir. İvedilikle konunun yetkili birimlerce sahiplenilmesi, gerekli yasal düzenlemelerin yapılması ve konu ile ilgili olarak toplumsal bilincin arttırılması gerekmektedir.

Bu çerçevede gerekli bilgi birikimine sahip uzman kadrolar oluşturulmalı, kritik altyapılar belirlenmeli ve bu tesislere yönelik güvenlik riskleri ve tehditler belirlenmelidir. Bu risk ve tehditler çerçevesinde belirlenecek güvenlik politikaları ise eksiksiz uygulanmalıdır.

Kritik altyapıların siber saldırılara karşı korunmasında güvenlik duvarı, anti virüs yazılımlarının yanı sıra sistem yalıtımını sağlayan SAHAB ve haberleşme tarfiğini şifreleyen kripto cihazlarının mutlaka yapılandırılması gerekmektedir.

Güvenlik hedefleri iyi belirlenmiş, güvenlik prosedürleri eksiksiz uygulanan ve temel sayısal güvenlik bileşenleri ile korunan altyapılar, sayısal saldırılara karşı daha dirençli hale gelebilecektir.

Kritik altyapıların güvenliğinin sağlanmasında en önemli faktörün ise insan faktörü olduğu hiçbir zaman unutulmamalıdır.

## KAYNAKLAR

[1] ABD, Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection, http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm

[2] Communication from the Commission to the Council and the European Parliament of 20 October 2004, Critical infrastructure protection In The

Fight Against Terrorism [COM(2004) 702 final – Not published in the Official Journal], http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_en.htm
[3] http://www.basbakanlik.gov.tr/docs/e-devlet/taslak.pdf
[4] TÜBİTAK-UEKAE, Karabacak, B., İki Kritik Kavram: Kritik Altyapılar ve Kritik Bilgi Altyapıları, www.bilgiguvenligi.gov.tr/siber-savunma/, 13 Şubat 2010.
[5] Byres E., Leversage D., Security Incidents And Trends In SCADA And Process Industries, British Columbia Institute of Technology, 2006.
[6] Internet, Cyber Defence Management Authority, http://itlaw.wikia.com/wiki/Cyber_Defence_Management_Authority.
[7] OSCE, Decision No. 6/07 on Protecting Critical Energy Infrastructure from Terrorist Attack, Fifteenth Meeting of the Ministerial Council, Madrid: 29-30 Kasım 2007.

**Ali IŞIKLI**
1974 yılında Almanya'da doğdu. İlk,orta ve lise öğrenimini Mersin'de tamamladı. 1991 yılında Hacettepe Üniversitesi Elektrik Elektronik Mühendisliği bölümünü kazandı ve 1996 yılında mezun oldu. 1996 yılında çalışmaya başladığı ASELSAN Haberleşme ve Bilgi Teknolojileri Grubu Kripto ve Bilgi Güvenliği Müdürlüğü'nde Sistem Tasarım Lideri olarak görevini sürdürmektedir.

# Siber Güvenlik için Kontrollü Ağ Erişimi

A.Uğur Duman

***Özet— Bu çalışmada ağ güvenliği kavramları, güvenli birl ağ için gereken kriterler ve güvenli ağ erişim çözümleri "Siber Güvenlik" kapsamında incelenmiştir. Uygulamada yaygın olarak kullanılan kontrollü ağ erişim yöntemlerinin çalışma mantığı anlatılmış ve bir NAC uygulama örneği verilmiştir.***

***Anahtar Kelimeler—Kontrollü ağ erişimi, NAC Uygulama yöntemleri, NAC Uygulama Örneği, Yerel Ağ güvenliği***

***Abstract: In this paper, Network Security subject is described briefly. Network Access Control (NAC) logic and general methods and NAC deployment modes and tips are explained.***

***Index Terms— LAN Security, NAC, NAC deployment, Network Access Control***

## I. GİRİŞ

TEKNOLOJİNİN her geçen gün daha da ivmelenerek hızlı bir şekilde gelişmesinin etkileri her alanda kendini hissettirirken, bu değişiklikleri en yakından takip edip ayak uydurma zorunluluğu hisseden kesim doğal olarak BT sektörü olmaktadır. Günümüzde hemen her türlü sistemin BT teknolojileri üzerinden yönetilmesi sonucunda bu sistemler bir yandan hayatımızı kolaylaştırmakta ancak kontrollerini sağladıkları sistemlerin kesintiye uğramasının ya da hatalı çalışmasının çok büyük etki yaratacak bir gücünün olması sebebiyle de kaçınılmaz olarak birer hedef durumuna gelmektedirler. Bu yüzden BT sistem yöneticileri bir yandan kontrol ettikleri sistemlerin güvenli bir şekilde çalışır ve ulaşılabilir durumda olmalarını sağlamaya çalışırlarken bir yandan da sistemlerindeki bilgi kaynaklarının bilgi güvenliği standartlarına uygun olarak korunması ve bilgi bütünlüğünün sağlanması için çalışmakta ve olası tehditlere karşı önceden önlemler alma planlamaları yapmaktadırlar.

BT sistemlere yapılan saldırıların yoğunluk, saldırı tipleri, amaçları ve nedenleriyle çok fazla çeşitlik kazandığı günümüzde, organize bir şekilde düzenlenen ve adına "Siber Savaşlar" denilen uluslararası çapta büyük saldırılar dönemi başlamıştır. Yaşadığımız iletişim çağında Internet'in yaygınlaşmasıyla birlikte siyasi veya toplumsal olayların tepkilerinin de siber saldırılarla verilebildiği, karşılıklı sanal saldırıların Dünya çapında etkili olabildiği hatta savaş nedeni olarak nitelendirildikleri gözlenmektedir. Ülkelerin ticari, ekonomik, sivil ve askeri sistemlerinin kontrolleri büyük ölçüde dijital ortam üzerinde olması nedeniyle bu siber saldırılara karşı güvenlik önlemleri geliştirme ihtiyacı her geçen gün artmaktadır. Günümüzde siber saldırıların büyük bir bölümü ekonomik amaçlarla yapılsa da, ülkelerin teknoloji, savunma, enerji, ulaşım gibi temel ve kritik alt yapıları da bu tür saldırıların hedefi olmaya başlamıştır.

Bu durumda bilgi güvenliği sadece BT yöneticilerini ve kullanıcılarını ilgilendiren bir durum olmaktan çıkmış, uluslararası boyutlarda birer devlet politikası haline gelmeye başlamıştır. Söz konusu siber saldırılara karşı alınması gereken önlemler ve çözümler "Siber Güvenlik" kavramı olarak karşımıza çıkmaktadır. Siber Saldırılara karşı ne tür güvenlik çözümleri alınabileceğini incelediğimizde bilgi güvenliği ve ağ güvenliği kavramlarının bir arada ele alınması gerektiği ortaya çıkmaktadır.

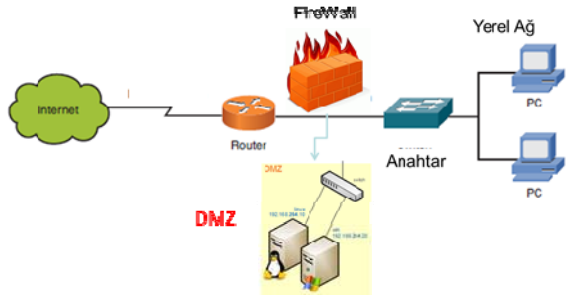
## II. AĞ GÜVENLİĞİ RİSK DEĞERLENDİRMESİ

Ağ güvenliği kavramından bahsedilirken genel eğilim Internet üzerinden gelen saldırı ve tehditlere gore önlemler almaktan yanadır. İnternet üzerinde açık kaynaklara ulaşılabilirliğin bir yerel ağa ulaşmaya nazaran çok daha kolay olması bu noktaları dış tehditler için açık hedef haline getirdiği için "Siber Saldırılar" sayısal olarak daha büyük oranda bu kaynaklara yapılmakta ve ağ güvenliği söz konusu olduğunda bu saldırılara karşı önlemler alınmasına öncelik verilmektedir. Ancak ağ güvenliği konusuna yaklaşırken internet'e açık kaynakları korumak ve dışarıdan gelecek tehditlere karşı önlem almak yanında yerel ağ üzerinden gelebilecek saldırılara karşı korumanın da özenle planlanması gerekmektedir. Internet üzerinden gelen bir saldırı sonucu bir şirketin genelde DMZ bölgesinde bulundurulan Web sitesinin ele geçirilmesi yada servis veremeyecek hale getirilmesi hizmet kesilmesi sebebiyle iş kaybı zararlarına sebep olabilirken aynı şirketin kendi iç ağından yapılan hedef odaklı bir saldırı ile kritik sistemlerinin ele geçirilmesi durumunda gizli/ önemli bilgilere ulaşılması, çalınması, silinmesi veya sistemin tamamen çalışamaz hale getirilmesinin çok daha büyük zararlar verebileceği göz önünde tutulmalıdır. 2009

Bildiri Ağustos 15, 2011 tarihinde gönderilmiştir.

A. Uğur Duman TAI-TUSAŞ, Bilişim Hizmetleri Müdürlüğü, Operasyon ve Ağ Yönetimi, 06980, Akıncı, Ankara, Türkiye (telefon: 90-312-8111800; faks: 90-312-8111800; e-posta: uduman@ tai.com.tr).

yılında Microsoft firması tarafından yapılan bir araştırmaya göre saldırıların yaklaşık %40'lık bir oranının yerel ağ'dan gelen saldırılar olduğu sonucu ortaya çıkmıştır. Bu durumda dışarıdan gelen saldırılara karşı önlem almanın yanında "Yerel Ağ'" güvenliği konusu da özel bir çalışma alanı olarak ele alınmalıdır. Yerel ağı korumak için alınan önlemler planlanırken "Risk Analiz"lerinin doğru yapılması, dışarıdan veya içeriden gelebilecek kötü amaçlı saldırıların verebileceği zararlar açısından incelenerek önceliklerin belirlenmesi son derece önemlidir. (Bu konuda alınacak önlemler için; "teknik açıkların kapatılması" standartlarını belirleyen "ISO 27002 Standart"larının rehber olarak kullanılması ve kontrollerin bu standartlara göre yapılması önerilir.)




*Şekil 1.Tipik bir Yerel Ağ örneği*

Yerel Ağ'ların güvenliği (*Şekil 1.)* en genel anlamda dış dünyadan çeşitli güvenlik katmanlarıyla korunmaya alınarak izole etme yöntemleriyle çözülmeye çalışılmaktadır. Ancak değişik lokasyonlarda birimleri bulunan şirket çalışanların ortak kaynaklara ulaşma ihtiyacı sebebiyle bu lokasyonların MetroEthernet ya da bulut teknolojileriyle birbirine bağlanmaları, VPN ile uzak bağlantı ihtiyaçları, Wireless sistemler üzerinden bağlantılar ve akıllı iş telefonlarının da iş yaşantısının bir parçası olması ile yerel ağ nerede başlayıp nerede biter konusu giderek daha da karmaşık hale gelmekte ve "Yerel Ağ Güvenliği" için klasik izole yöntemlerine göre daha gelişmiş "akıllı" çözümlere ihtiyaç duyulmaktadır.

Bir yerel ağ'ın güvenli olarak nitelendirilebilmesi için; ağ içerisinde bulunan bir çok cihazın bir arada sorunsuz, verimli, kesintisiz ve güvenli bir şekilde çalışması ve aynı zamanda ağ'da sürdürülen hizmetlerin gerektirdiği gizlilik ve güvenlik seviyesini hiç düşürmeden istenen standartlara uygun olarak risklerin en aza indirildiği bir hizmet sunabilen bir ağ alt yapısı olması şartlarını karşılaması gerekmektedir. Bu güvenlik gerekleri yerine getirilirken aynı zamanda kullanıcıların ihtiyaç ve beklentilerinin de karşılanması gereği bu konuda her sistem için kendine özgü en uygun çözümlere karar verip bunları devreye almamızı zorunlu kılmaktadır. Özetle; bir yerel ağ alt yapısının güvenlik standartlarını oluştururken o ağ üzerinden hizmet vereceğimiz tüm sistemlerin ihtiyaçları ve yapısı belirleyici faktör olmalıdır ve yerel ağı koruma yöntemlerinde bu konu üzerinde uzmanlaşmış "akıllı" ve dinamik sistemler kullanmamız gerekmektedir. Bu yaklaşım "Kontrollü Ağ Erişimi" kavramı olarak karşımıza çıkmaktadır.

## III. KONTROLLÜ AĞ ERİŞİMİ

*Kontrollü Ağ Erişimi* ya da BT dünyasında bilinen adıyla NAC (Network Access Control) genel anlamda bir ağa bağlanacak uç sistemleri kontrollü ve istenilen kural ve standartlara göre söz konusu ağa dahil etmek ve ağı gerçek zamanlı olarak denetim altında tutmak amacıyla kurulmuş bir alt yapı sistemi olarak tanımlanabilir.

Ağ kaynaklarına erişmek isteyen birbirinden çok farklı uç sistemlerin bu isteklerini değerlendirip, girişlerinin o ağ için belirlenmiş güvenlik politikalarına uygunluğunu belirlemek ve sakıncalı bulunan cihazları ya da bilgisayarları ağa dahil etmeme işlemleri yapılabildiği gibi, bir yazılım eksikliğinden dolayı girişleri uygun bulunmayan uç sistemler için gerekli yönlendirmeler yapılıp eksikliklerini tamamlaması ve gerekli düzeltmeler sonrası ağa alınması da sağlanabilir.

Böylece bir yerel ağ için uygulanması istenen işletim sistemi, yazılım ve donanım standartları NAC sistemi tarafından sürekli olarak uygulanabilir ve denetlenebilir.

Bu sisteme göre örneğin son kullanıcılar çalışma ihtiyaçlarına göre aşağıda *Şekil 2*'de gösterildiği şekilde gruplandırılarak ve bu gruplara göre değişik seviyelerde yetkilendirilerek ağa dahil edilebilirler.


*Şekil 2.Yerel Ağ Erişim Skalası*

NAC genel anlamda; ağ yapısına dahil edilen tüm cihaz ve bilgisayar'ların önceden belirlenmiş güvenlik standartlarına uygun olmasını sağlamak ve tüm sistemin bu standartların dışına çıkmadan çalışmasını garantilemek için çözümler sunan bir teknolojidir. NAC hem yerel ağ üzerinden hem de uzak lokasyonlardan ağ'a bağlanma isteği olan uç noktalar için farklı çözümleri olan ve her kurumun yerel ağ güvenliği için değişik seviyelerdeki ihtiyaçlarına uygun olarak şekillenebilen esnek bir çözüm olarak tasarlanmıştır.

Ağ Güvenliği çözümleri sunan firmaların değişik NAC çözümlerinin karşılaştırması yapıldığında çözümlerin hepsinin ortak adının NAC olarak nitelendirilmesine karşın farklı teknolojiler kullandıkları ve farklı ihtiyaçlara öncelik verdikleri görülmektedir, bu açıdan farklı NAC çözümlerinden hangisi ağ güvenliği uygulanacak sistem için belirlenmiş öncelikleri ve ihtiyaçları karşılıyorsa çözüm olarak bu seçenek tercih edilmelidir.

## IV. NAC UYGULAMASININ ÖNEMİ

Yetkisiz veya ağa dahil olması sakıncalı bulunan bir uç sistem giriş yaptığında, ağ üzerinde bulunan bilgi kaynaklarının hem bütünlüğü hem de gizliliği tehlikeye girer.

Örneğin; ağa dahil edilmiş kötü amaçlı bir misafir veya yetkisiz kullanıcı ağ trafiğini çeşitli programlarla dinleyerek ağ hakkında bilgi toplayabilir ve bu bilgileri kullanarak yetkisiz giriş denemeleri yapabilir, çeşitli yöntemlerle ağ trafiğini yanlış yönlendirebilir, sistemlerin çalışmalarını engelleyebilir yada kritik bilgileri, şifreleri ele geçirebilir. Öte yandan yetki açısından uygun bulunan kuruma ait bir bilgisayar'ın üzerinde AntiVirus/ AntiSpam/AntiMalware vb. gibi koruyucu program kurulumları olmadan ağa dahil edilmesi içeride potansiyel bir risk noktası oluşturur. Söz konusu bilgisayar Virus/Trojan gibi programlar aracılığıyla kullanıcısından bile habersiz şekilde ağ kaynaklarına saldırı noktası haline getirilebilir. NAC çözümü bu tür istenmeyen durumları engellemek için de kullanılabilen bir teknolojidir.

NAC uygulaması kablolu veya kablosuz yerel ağa, ağ içerisinden yada internet üzerinden herhangi bir uç sistemin bağlanması durumunda; ağda uygulanması istenen güvenlik politikalarına göre otomatik olarak bu kuralların işletilmesini sağlayabilir ve söz konusu uç sistem için gerekli kontrolleri yaptıktan sonra en genel anlamda ağa dahil edilip edilmeyeceğine karar vererek işlemi gerçekleştirebilir. Uygun bulunup onaylanarak ağa alınan uç noktalar için de geçmiş bilgileriyle anlık bilgilerini karşılaştırarak trafik analizleri yapabilir ve söz konusu uç sistemden beklenmeyen bir davranış ya da uygunsuzluk tespit ettiği zaman ağ bağlantısını kesebilir ve sistem yöneticileri için konuda alarm üretebilir. Sonuç olarak NAC; bir yerel ağın belirlenmiş olan güvenlik standartlarına uygun çalışmasını sağlamasını garanti edebilen önemli bir seçenek olarak karşımıza çıkmaktadır. En önemli avantajı hem internet üzerinden hem de yerel ağdan gelebilecek saldırılara karşı değişik çözümler ve önlemler sunabilmesi ve böylece "Siber Güvenlik" açısından önemli bir savunma politikası geliştirebilme olanağı sağlamasıdır.

## V. NAC UYGULAMALARININ GENEL MANTIĞI

NAC çözümleri üreten firmaların ürünlerini incelediğimizde hepsinin son kullanıcı uyumluluk kontrollerine odaklandığı görülmektedir.NAC uygulanılan bir ağa bağlanma girişiminde bulunan bir bilgisayar gerekli kontrolleri yapılıp onaylanma aşamalarından geçinceye kadar ağ'da bulunan kaynaklara ulaşamazlar, sadece kontrollü bir trafik sistemi aracılığıyla onay işlemleri için kendilerini tanıtmaya izin verecek düzeyde ve önceden belirlenmiş portlar üzerinden belirlenmiş noktalara kontrollü olarak kimlik bilgilerini gönderebilirler.

Örneğin onay sistemi olarak AD Etki Alanı onayı (SSO) kontrolü kullanılıyorsa AD yöneticisi konumundaki DC sunucular ile belirli portlar üzerinden haberleşebilir ve kendini
tanıtmak için gereken bilgileri ağ içerisindeki bu DC sunucularına gönderebilir. Onay işlemleri için gereken şartları sağlayan uç sistemler yerel ağa'a dahil edilirler, bu aşamada geçersiz kullanıcı bilgisi veya başka herhangi bir uyumsuzluk yüzünden sisteme kabul işlemi sonlanmamış ise yerel ağ'a giremezler. Eğer söz konusu uyumsuzluk "düzeltilebilir hata" seviyesinde tanımlanmış bir eksiklikten kaynaklanıyor ise bu eksikliğin tamamlanması amacıyla bu bilgisayar'lar belirli bir süre için karantina bölgesine alınır ve istenen düzeltmeleri yapabilmeleri için bu işlemler için hazırlanmış kaynaklara gene kontrollü olarak yönlendirmeleri yapılıp güncellemelerini tamamlama işlemleri sonrasında yapılan ikinci bir kontrol sonucu onay alabilirlerse ağa dahil olmalarına izin verilir.

## VI. NAC İLE KONTROL EDİLEBİLEN ÖZELLİKLER

NAC sistemleri özellikle uç sistemlerin ağa kontrollü olarak dahil olmaları işlemleri üzerinde uzmanlaşmış oldukları için uç sistemlerin bir çok özelliğini tarayarak çeşitli düzeylerde bir çok farklı kontroller yapabilirler, bu kontrol sonuçlarını kullanarak ağ yöneticileri ağa giren sistemleri tanıyıp gruplandırıp ihtiyaçlarına uygun politikalar hazırlayabilirler. NAC sistemleri özet olarak aşağıdaki kontrolleri yapabilmektedirler.

- AD Domain ya da LDAP üzerinden "bilgisayar kimlik" doğrulama kontrolleri,
- AD veya Lokal Database üzerinden "kullanıcı kimlik" doğrulama kontrolleri,
- İşletim sistemi, yama ve servis paketi, AntiVirüs, AntiSpyware, Antimalware vb. yazılımların olduğu kontrolü veya bunlara ait güncellik kontrolleri,
- Kayıt Defteri (Registry) değerlerinin kontrolleri,
- Çalışan Servislerin kontrolleri,
- Cihazlar için MAC ID, MAC Vendor ya da IP, kullanılan portlar , protokoller vb. kontroller.

NAC çözümleri yukarıdaki özellikleri kullanarak oluşturulan kurallarla aşağıdaki listede belirtilen güvenlik ihtiyaçlarını karşılayabilirler.

*Bilgisayarlar açısından;*

- Yerel ağa dahil olma girişiminde bulunan bilgisayarların tanımlanan güvenlik politikalarıyla uyumundan emin olunmasını sağlayarak ağın standartlarını belirler.
- Güvenlik politikalarıyla uyumsuz bilgisayarların yerel ağa dolayısıyla ağdaki bilgi kaynaklarına erişimini engeller.
- Ağ dışına çıkmış dizüstü bilgisayarların problemli bir şekilde geri dönüşlerinde girişlerini ancak gereken düzeltmeler yapıldıktan sonra ağa alınmasını sağlar, böylece dışarıdan gelebilecek virus, solucan, zararlı yazılım gibi güvenlik tehditlerine karşı da ağda koruma sağlar.
- Yerel ağ'a girmek isteyen ziyaretçi sistemlerini de kontrol edebilen ve belirlenen minumum standartları sağladıkları takdirde onlara izin verilen ölçüde yetki verebilen (örneğin sadece internete çıkış izni) ihtiyaçların karşılanmasını sağlar.

*Cihazlar açısından ;*

- Yerel Ağ'da çalışan yönetilebilen ve yönetilemeyen tüm IP /MAC-ID bazlı cihazların izlenmesi, tanımlanması, gruplanmasını sağlar. Oluşturulan gruplamalara göre bu cihazların ağa dahil edilip edilmemeleri konusundaki kuralları uygulayarak erişim kontrollerini sağlamasıyla güvenli bir ağ altyapısı sağladığı için olası riskleri azaltır.
- Cihazlar için tanımlanmış rollere gore aynı tarz cihazlar

için ortak işlemleri otomatik olarak yürütebilir, böylece ağın sürekli olarak denetlenmesini sağlar, geçmişe dönük kontrollerle gerçek zamandaki farklılıkları karşılaştırarak değişiklikleri raporlar, şüpheli ağ trafiği hareketleri için uyarılar oluşturur, böylece "Yerel Ağ" güvenliğinin arttırılmasına önemli bir katkı sağlar.

## VII. NAC KONTROL ADIMLARI

NAC ile ağ güvenliği temel olarak 4 aşamada sağlanır:

- Kimlik Doğrulama
- Yetkilendirme
- Güvenlik Taraması
- İyileştirme

Bu aşamaların detaylarını incelediğimizde yapılan işlem adımları aşağıdaki gibi özetlenebilir.

- *Tespit (Detect):* Ağa bağlanma isteğinde bulunan tüm cihazların tespitleri yapılır, türlerine göre belirlenir ve tanımlama işlemleri yapılır.
- *Doğrulama (Authenticate)*: Ağa giren kullanıcı veya cihazların belirlenen politikalara göre kimlik doğrulama işlemleri yapılır.
- *Değerlendirme (Assess):* Uç sistemlerin belirlenen politikalarla uyumluluğu veya güvenlik açıkları değerlendirme işlemleri yapılır.
- *Onaylama (Authorize):* Kimlik doğrulanması veya uygulanacak kurallara göre değerlendirmenin sonucunda uç sistemlerin ağı kullanabilmeleri için onay işlemleri yapılır.
- *Düzeltme (Remediate):* Bilgisayarların eksikliklerini tamamlama, problemlerini iyileştirme işlemleri
- *İzleme (Monitor):* Ağa bağlanan ya da bağlanma isteğinde bulunan aygıtları ve kullanıcıların izlenmesi ve kontrol edilmesi işlemleri
- *Karantina (Contain):* bütün ağ çevresini olumsuz etkilerden korumak için problemli uç sistem ya da kullanıcıları karantina altına alma işlemleri.

Bu kontrol adımlarını (*Şekil 3*) uygulayarak kim, hangi yetkiyle,hangi kaynaklara, nereden ulaşıyor bilgileri dahilinde kontrollü bir ağ erişimi için kullanılacak araçlar elde edilmiş olur.


*Şekil 3. Kontrol adımları*

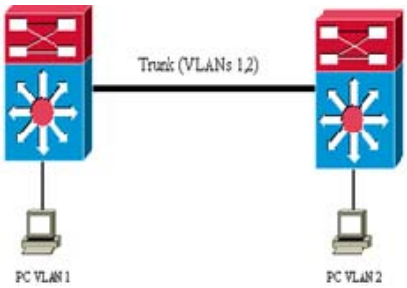
## VIII. NAC UYGULAMA TEKNİKLERİ

NAC teknolojilerinin genel çalışma prensipleri incelediğinde ağ haberleşme katmanlarının (OSI katmanları) birbirleriyle ilişkileri ve bu katmanlarda çalışan cihazların özelliklerinin kullanılarak işlemlerin yürütüldüğü görülmektedir. NAC sistemleri, OSI katmanları standartlarını kullanarak kontrollerini ve işlemlerini gerçekleştirirler. OSI katman modeli, verinin bilgisayar üzerinde bir programdan, ağ ortamından geçerek diğer bilgisayar üzerindeki başka bir programa nasıl ulaşacağının standartlarını tanımlar. Cihazlar ve bilgisayarlar birbirleriyle OSI katmanları standartlarına uygun olarak haberleşirler. NAC ürünleri üreten firmalar OSI katman yapısı içerisinde cihazların birbirleriyle nasıl haberleştikleri konusuyla derinlemesine ilgilenir ve bu katmanlarda kullanılan standartlardan yararlanarak ağ yapısını tanıma ve ağ trafiğine müdahale etme yöntemleri oluştururlar. NAC çözümleri kontrol işlemlerini gerçekleştirirken MAC_ID, IP, VLAN, 802.1X Port güvenliği tekniklerini, ARP, DHCP ve SNMP çalışma mantıklarını ve OSI katmanlarının çalışma prensiplerini kullanarak yerel ağı son kullanıcı risklerinden koruma amaçlı çözümler üretirler.

Bu çözümlerden donanım bazlı NAC çözümlerinin mantığının anlaşılması için öncelikle kullandığı temel teknolojilerden biri olan Vlan (Virtual LAN- Sanal Yerel Alan Ağ) çalışma mantığından bahsedilmesi gerekmektedir. Vlan, bir yerel ağı mantıksal olarak bölümlere ayırma yöntemi olarak tanımlanabilir ve OSI 2. katmanında çalışır, Vlan kullanılan bir ağda, aynı Vlan'da bulunan uç kullanıcılar sadece kendi yayın alanlarına (broadcast domain) sahip olacaklarından birbirleri ile haberleşebilirler, ancak farklı Vlan'larda bulunan uç kullanıcılar ile gerekli konfigurasyonlar yapılmadığı sürece iletişim kuramazlar.

Bir yerel ağ'da Vlanlar oluşturulduktan sonra bir Vlan'a başka Vlan'lardan ulaşabilmek için üzerlerinde bir Interface tanımlanır ve bu interface için bir adresleme bilgisi (IP ve subnet) verilir, böylece bu Vlan dışarıdan erişilebilir hale gelir, eğer böyle bir interface tanımı yapılmazsa söz konusu Vlan ile dış bağlantı kurulamaz. Ayrıca üzerlerinde interface tanımlanmış Vlan'ların diğer Vlan'larla iletişimlerini kontrol etmek amacıyla Anahtar arası bağlantı noktalarında (Trunk) Vlan geçişleri için izin tanımlamak da mümkündür. İzin verme (Allowed VLAN) tanımı yapılan bir Trunk üzerinden sadece kendisine izin verilmiş VLAN'lara ait trafik geçebilir. Ve izin verilen Vlan uç noktaları birbirleri ile haberleşebilir.

NAC programları yukarıda bahsedilen VLAN tanımlamalarını kontrol ederek ağ trafiğini durdurabilirler ve NAC sunucularının kontrol sonuçlarına göre uç kullanıcı trafiğini tasarım aşamasında tanımlanan politikalara uygun VLAN'lara yönlendirebilirler. Ağa girmesi uygun olmayan uç kullanıcıları karantina Vlan'ına, misafir kullanıcıları Internet Vlan'ına ya da belirlenen uç "Rol" lerine göre Rol Vlan'ına alabilirler.




*Şekil 4. VLAN'lar arası haberleşme*

Şekil 4'de örneği verilen VLAN1 ve VLAN2 üzerinde interface ve adresleme bilgileri tanımlanmaz ise veya bu Vlan'ları birbirine bağlayan Switchlerin birbirlerine bağlandıkları "Trunk" portları üzerinde bu Vlan'lar için karşılıklı izin tanımlamaları yapılmazsa bu iki farklı Vlan'daki PC'ler birbirleriyle haberleşemezler.

## IX. NAC BİLEŞENLERİ

NAC sistemi; farklı görevler yapan sunucuların bir arada çalışması ile oluşturulur, bu sunuculardan Yönetici (CAM) ve Uygulayıcı (CAS) sunucuları sistemin temel işlemleri yerine getirirler, son kullanıcıların ağa dahil edilip edilmeyeceği kararları, gereken kontrollerin yapılması ve sonuçların uygulanmasından sorumludurlar. Ayrıca "Gruplayıcı" (Profiler) ve "Bilgi Toplayıcı" (Collector) sunucuları diğer önemli bileşenlerdir. NAC Sunucuları;

- *NAC Manager (CAM):* Tüm NAC sisteminin yöneticisi durumundadır. Bu sunucuya önce kontrol edeceği CAS sunucuları tanıtılır, sonra yöneteceği ağın yapısı, IP ve VLAN yapılandırılması, Anahtar cihazlar (switch), DNS, DHCP, AD bilgileri vb. tanıtılır. Uç kullanıcılara uygulanacak politikalar, standartlar, kurallar vb. tüm kontroller bu sunucu üzerinde tanımlanır.
- *NAC Server (CAS) :* Ağa erişim kontrolünü gerçekleştiren uygulama sunucusudur. Ağa erişme isteğinde bulunan bir uç sistem CAS sunucu tarafından portları kontrol edilebilen Anahtar (Switch) üzerinden bağlanma isteğini iletir CAS sunucusu CAM sunucusundan aldığı bilgiye göre uç kullanıcı için yapılacak işlemi uygular, tanımlanan politikalara uygun olarak port trafiğini kontrol eder. Ağın ihtiyaçlarına uygun sayıda CAS sunucu kullanılabilmektedir.
- *NAC Agent (NA) :* İstemci tarafında çalışan NAC ajanıdır. Yüklü olduğu bilgisayarları tarayarak makina hakkında bilgi toplama ve bu bilgileri NAC sunucularına sunma ve onay işlemleri için aracılık yapma işlevleri vardır.
- *NAC Collector Server :*Ağ içerisinde bulunan tüm cihazları gerçek zamanlı olarak tarayarak; NetMap, NetTrap, NetWatch, NetInquiry, NetRelay gibi ağ tarama yöntemleri ile topladığı bilgileri Profiler sunucusuna aktarır.
- *NAC Profiler Server :* Collector sunucularından gelen bilgileri toplayarak ağ içerisindeki cihazların analizlerini yaparak özelliklerine göre cihazları tanımaya yönelik kontroller ve sınıflamalar yapar ve son kullanıcıların tanımlanmış grup ya da "Roller" e atamalarını yapar, sonuçları CAM sunucusuna bildirir.
- *Guest Server :* Ağ üyesi olmayan ziyaretçi sistemlerin, örneğin; ziyaretçi dizüstü bilgisayarların sadece Internet'e çıkma ihtiyaçlarını sağlamak için kullanılan bileşendir.

Bu bileşenlerin ortak çalışmaları sonucunda NAC sistemi tüm son kullanıcıların ihtiyaçlarına uygun esnek çözümlerle ağ güvenliği ve standartlarını uygulama işlemlerini yürütebilmektedir.

NAC sunucularının kendi aralarında güvenli bir şekilde bilgi alış verişlerini yapabilmelerini garantilemek için güvenilir bir sertifika sunucusu tarafından verilen bir kök sertifika ve her sunucu için ayrı ayrı üretilen sertifikalar aracılığı ile karşılıklı olarak kendilerini tanıtmaları yöntemi kullanılır, bu sertifika değişim işlemleri sonucunda sunucular karşılıklı güven ilişkileri kurarlar ve karşılıklı olarak haberleşecek duruma getirilirler.

## X. CAS SUNUCU UYGULAMA MODLARI

NAC uygulanması planlanan ağ yapıları ve uygulama ihtiyaçları çeşitlilik gösterdiğinden ilk adım olarak NAC uygulaması yapılacak ağ için analiz yapılarak NAC'ın hangi seçeneklerine uygun olduğuna karar vermek gerekmektedir. Bu aşamada son kullanıcı tarafında uygulayıcı sunucu rolündeki CAS sunucu üzerinde ağın yapısına göre aşağıdaki *Tablo 1'*de gösterilen modları ve seçeneklerini kullanarak doğru NAC tasarımını yapmak önemlidir.

| CAS Uygulama Modları | Seçenekler |
|---|---|
| Trafik Modları | Virtual veya Real_IP Gateway |
| Trafik Akış Modları | In-Band veya Out-of-band |
| Kullanıcı ulaşım Modları | Layer 2 veya Layer 3 |

*Tablo 1. Cas Modları*

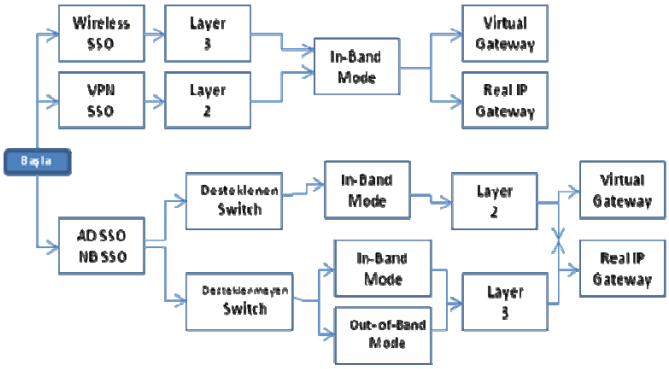
- *Trafik Modu:* CAS sunucu paketleri uçtan uca doğrudan aktaracak şekilde (Bridged) çalışacaksa Virtual Gateway, IP yönlendirmeleri yapacak şekilde (IP Routing) çalışacak ise Real IP Gateway Modu olarak ayarlanmalıdır.
- *Trafik Akış Modu:* CAS sunucu üzerinde eth0 ve eth2 olmak üzere 2 adet ethernet çıkışı bulunmaktadır, bu 2 çıkışın ağa bağlanma yöntemine göre 2 farklı seçenekle ağ trafiğini kontrol edebilmektedir. CAS sunucunun ethernet çıkışları; ağa giriş istekleri henüz onaylanmamış (güvenilmeyen) taraf ile yerel ağ (güvenilen) tarafa seri olarak bağlanır ise yani tüm trafik CAS sunucu üzerinden geçirilerek trafiği her an kontrol edebilir duruma getirilirse bu "In-Band" modudur. VPN gibi uzak bağlantılar veya kablosuz ağ bağlantıları için bu mod uygundur. Gerçek zamanlı olarak sürekli ağ trafiği analizi yapma ve gerektiğinde şüpheli trafiği durdurma olanağı verdiğinden yüksek

güvenlik gerektiren kritik alt yapı sistemleri için uygundur. Eğer CAS ethernet çıkışları söz konusu iki tarafa mantıksal olarak bağlanır ve trafiği sadece uç kullanıcıları onaylama işlemi sırasında kontrol edilmesi yeterli bulunur ise "Out-of-Band" modu seçilir. Bu modda da istenirse "Passive Remediation" yöntemi ile belirlenen aralıklarla ara kontroller yapmak mümkündür.

- *Kullanıcı Ulaşım Modu:* Uç kullanıcılar yerel ağ içerisinde bulunuyorlar ise yani uç noktalar MAC-ID'leri üzerinden kontrol edilecebilecek durumda ise CAS "Layer 2" modunda çalıştırılır, eğer uzak lokasyonlardan ulaşacak kullanıcıların örneğin VPN ile bağlanacak kullanıcıların da kontrollerinin yapılması isteniyor ise tanımlamaları IP'ler üzerinden yapılacağından bu durumda "Layer 3" modu seçilir. Bu modda örneğin yerel ağa sadece önceden güvenli olduğu belirtilen IP'lerin girmesi sağlanabilir.

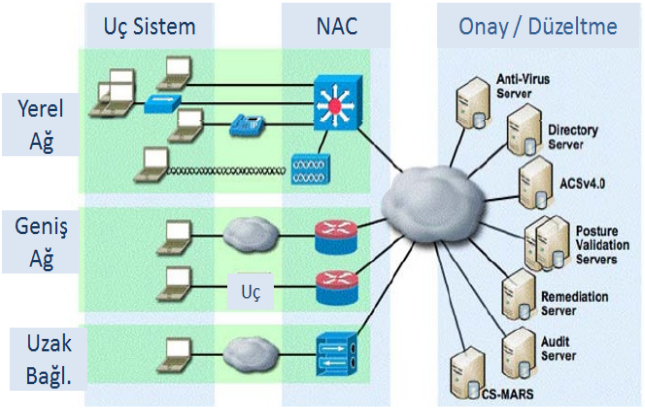
Yukarıda verilen bilgiler ışığında NAC uygulaması yapılması planlanan bir ağın fiziksel yapısına, lokasyonların birbirleriyle bağlantı koşullarına, kullanılan cihazlara ve ağ için uygulanacak güvenlik politikalarına göre aşağıda gösterilen (*Şekil 5*) algoritma kullanılarak uygun olacak seçeneklere göre CAS sunucularının uygulama modlarına karar verilir.

*Şekil 5. CAS Mod'ları algoritması*




Bu modlar farklı kombinasyonlarla bir arada kullanılabilirler. Örneğin; yerel ağ tarafını kontrol edecek CAS sunucusu "Out-of-band" ve "Layer 2" modunda çalıştırılırken uzak bağlantıları karşılayacak CAS sunucusu ise "In-Band" ve "Layer 3" modunda çalıştırılarak yerel, geniş yadauzak tüm uç kullanıcılar (*Şekil-6)* NAC kontrollü olarak ağa alınabilmektedirler. Bu açıdan NAC uygulanacak ağın fiziksel yapısı ve güvenlik ihtiyaçlarına uygun olarak özenli bir analiz ve tasarım çalışması yapılması ve sonrasında uygulamayı devreye almadan önce hazırlık ve pilot aşamalarının dikkatle planlanarak her durum için testlerinin yapılması son derece önemlidir.

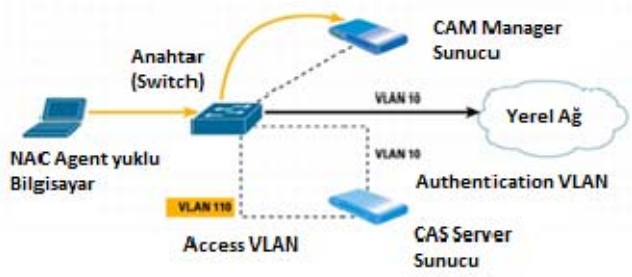
*Şekil 6. Farklı ihtiyaçlar için NAC çözümleri*




## XI. NAC TASARIM ÖRNEĞİ

Aşağıdaki yapıda (*Şekil 7*) Virtual Gateway, Out-of-Band, Layer 2 seçenekleri ile NAC uygulanmış bir yerel ağ için kontrollü ağ erişiminin çalışma örneği gösterilmektedir.

*Şekil 7. Örnek NAC çözümü*




NAC Kontrol Adımları;

- Ağa giriş isteğinde bulunan bir son kullanıcının bağlı bulunduğu Anahtar (switch) port'u CAS sunucu tarafından önce VLAN 110 olarak tanımlanmış "Access VLAN"ına yani "güvenilmeyen taraf"a alınır, bu VLAN'da onay işlemleri tamamlanana kadar bekletilir, bu sırada sadece kendisine onay verecek sistemlerle özel portlar üzerinden haberleşebilir, örneğin DHCP sunucusundan IP alabilir, DC sunucuya login bilgilerini gönderebilir, ancak bu aşamada ağdaki diğer kaynaklara ulaşamaz.
- Uç kullanıcı NAC üzerinde tanımlanmış kurallara göre onay alırsa (örneğin AD_SSO üzerinden kendisinin girmeye çalıştığı ağa ait bir domain üyesi PC olduğunu kanıtlarsa ve diğer şartları sağlarsa) VLAN10 olarak tanımlı "Authentication VLAN" ına yani "güvenilir" şirket ağına kendisine uygun Rol ya da Vlan tanımı ile alınır, onaylanmaz ise ağa giremez, "Access VLAN"ında kalır.
- Eğer PC üzerinde tespit edilen bazı eksiklikleri sebebiyle girişi engellenen bir şirket uç kullanıcı ise uygulanan politikalar doğrultusunda isteğe bağlı olmak üzere karantinaya alınıp eksikleri tamamlandıktan sonra ağa dahil olabilir. Bu seçeneği gerçekleştirmek için söz konusu eksiklikleri gidermek için "Remediation" sunucularının kurulması gerekmektedir.

Eğer NAC sistemin de dışarıdan gelen ziyaretçilerin internet ihtiyaçlarını karşılamak için bir "Guest Server" kullanılıyor ise ağa giriş bağlantısı yapan ziyaretçiler "Guest server" üzerinde kendileri için kısıtlı süre için geçerli olacak şekilde tanımlanmış kullanıcı ID'leri ve password'leriyle giriş yaparak sadece Internet'e çıkış işlemlerini gerçekleştirebilirler.

## XII. SONUÇ VE DEĞERLENDİRME

NAC uygulamasının ağ yöneticilerinin ağ üzerindeki kontrol ve yönetim gücünün arttığı ve önemli bir oranda güvenlik iyileştirmesi gerçekleştirilebildiği görülmektedir. NAC sistemleri Ağ güvenliğinin istenilen standartlara gelmesi ve değişik seviyedeki güvenlik ihtiyaçlarına cevap verebilmesi ve sürekli kontrol sağlayabilmesi açısından Siber saldırılara karşı önlemler alabilmemiz için gerekli bileşenleri ağ yöneticilerine sunmaktadır. Siber saldırılarına karşı önlem geliştirme konusunda en önemli faktörlerden birisi ağda gerçekleşen şüpheli ağ hareketlerinden, sisteme izinsiz yada yetkisiz erişme girişimlerinden ya da sakıncalı bulunan cihazlardan haberdar olunması yani tehditlerin farkına varılmasıdır. NAC sistemi hazırlanan kurallar gereği sakıncalı bulunan uç sistemlere veya cihazlara giriş izni vermediği gibi ağa girmesine izin verilmiş bulunan uç noktalar üzerinde şüpheli ağ hareketleri oluştuğunda da ağ yöneticilerini uyararak önceden önlem alma olanağı sunmakta ve tüm ağ elemanlarını gerçek zamanlı olarak izlenme olanağı da vermektedir.

Bu değerlendirmeler ışığında NAC çözümleri , ağdaki tüm trafiği port ve protokoller bazında dinamik olarak takip ve kontrol edebilme, istenilen güvenlik seviyesinde ve gerekli olduğu ölçüde ağ trafiğine izin verebilme olanakları ve her türlü PC/cihaz hareketlerinden ağ yöneticilerini haberdar etme yetenekleri ile "Siber Saldırılar"a karşı proaktif önlemler oluşturma çalışmalarımız sırasında önemli bir denetim ve destek mekanizması olarak karşımıza çıkmaktadır. NAC çözümü savunma sistemlerinde kullanılan dost ve düşman sistemleri ayırt etme yeteneği bulunan cihazların ağ karşılığı olarak nitelendirilebilecek düzeyde bir koruma, ayırt etme ve saldırı tespit olanakları sunmaktadır.

Sonuç olarak NAC; Ağ güvenliğini tehdit eden saldırı tiplerine karşı önemli bir koruma kalkanı kurma olanağı sağlamaktadır, ayrıca IDS ve IPS gibi diğer saldırı tespit ve saldırıdan koruma sunucuları ile birlikte kullanıldığında dışarıdan gelebilecek "Siber Saldırılar"a karşı farklı teknolojiler kullanan çok katmanlı bir güvenlik çözümü de yakalanmış olacağından "Siber Güvenlik" açısından arzu edilen seviyede standartlar sağlanabilecektir.

## KAYNAKLAR


[1] http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/bilgi-guvenliginde-iso-27000-standartlarinin-yeri-ve-oncelikli-iso-27002-kontrolleri.html

[2] http://www.sde.org.tr/tr/haberler/1531/siber-saldiri-savas-sebebi-mi.aspx

[3] http://www.tubitak.gov.tr/sid/0/cid/21886/index.htm;jsessionid=122D580937878F69C4C9D54A5A49B706

[4] https://mosaicsecurity.com/categories/81-network-access-control

[5] http://www.bidb.itu.edu.tr/?d=496

[6] http://www.olympos.net/belgeler/vlan/vlan-ag-mimarisi-52526.html

[7] http://www.netcom.com.tr/index.php/coezuemlerimiz/network-guevenlii/itemlist/category/127-iç-tehditler

[8] http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/48/cam/48cam-book.html

[9] http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/48/cas/48cas-book.html

[10] http://www.cisco.com/en/US/docs/security/nac/profiler/configuration_guide/311/Profiler311I-C.html

[11] net_design_guidance0900aecd80417226.pdf


**A. Uğur DUMAN :** İzmir-1961, Lisans diplomasını ODTÜ Elektrik-Elektronik Mühendisliği bölümünden aldı. Çeşitli firmaların yurt içi ve yurt dışı lokasyonlarında OS sistem yöneticiliğinden donanım ve network uzmanlığına BT alanında geniş bir skalada çalışmaları oldu. 1998 yılından bu yana çalıştığı TAI'de Ms Windows sistemlerin; alt yapı tasarımlarından planlanma, kurulum, işletim, enterprise sistemler yönetimi, kullanıcı sistem yönetimleri ve sistem desteği ve eğitimleri gibi konularda çalışmalarda bulundu, TAI-TUSAŞ adına dış projelerde (e-sigorta, vedop) AD tasarımları konusunda danışmanlık yaptı. Daha sonra Ağ Yönetimi alanına geçiş yaptı, halen yerel ve uzak ağ alt yapısı elemanlarının işletim, destek ve yönetimi, Internet ve yerel ağ güvenliği, bilgi güvenliği, data haberleşmeleri yönetimi vb. konularında çalışmalarını sürdürmektedir. TAI-TUSAŞ yerel ağında ağ güvenliği çözümü olarak Cisco NAC uygulamasını hayata geçirmiştir.

# Siber Terör Saldırılarından Korunmaya Yönelik Bulanık Mantık Tabanlı Karar Destek Modeli

Kerim Göztepe[1] Ahmet Ejder[2]

***Özet*--Bilgisayar ve iletişim teknolojilerindeki gelişmeler, geçmişle kıyaslanamayacak derecede ileri ve geniş kapsamlı değişikliklerin ortaya çıkmasına sebep olmuştur. Yeni teknolojilerin kullanılması bireylere, Siber Terör Saldırılarından Korunmaya Yönelik Bulanık Mantık Tabanlı Karar Destek Sistemirmalara ve devlet yönetimine büyük yararlar sağladığı gibi beraberinde birtakım problemler de getirmiştir. Devletler; ülkeleri tehdit eden, bilgi bankalarındaki gizli bilgilere ulaşan, toplumun günlük yaşantısına zarar veren siber terörizmle karşı karşıya kalmıştır. Yakın bir zamana kadar daha çok bireysel ve kurumsal sorunlara yol açan siber terör, artık suç organizasyonları, profesyonel kişiler, siber aktivistler gibi çeşitli gruplar tarafından kamu ve ülke güvenliğini tehdit edebilecek boyutlara ulaşmıştır. Bu çalışmada siber terör saldırıları karşısında daha bilinçli hareket etmek, kritik sistemlere yapılacak siber saldırılar karşısında neler yapılabileceğini önceden görmek maksadıyla bulanık mantık tabanlı karar destek sistemi geliştirilmiştir. Geliştirilen model, farklı kriterleri bulanık mantıkla değerlendirmekte ve siber terör saldırılarına karşı nasıl hareket edilmesi gerektiğini ortaya koymaktadır.**

***Anahtar Kelimeler*--**Siber terör, bulanık mantık, karar destek sistemi

***Abstract*--Computer and communication technology developments in comparison with the last has led to the emergence of highly advanced and far-reaching changes. The use of new technologies to individuals, companies and state administration has also offered great benefits for some problems with it. States has faced cyber-terrorism which threaten nations, reaching the confidential data banks, damaging the everyday life of the society. Until recently, leading to more individual and institutional problems of cyber terrorism, today criminal organizations, professional people, such as cyber-activists groups in the country has reached proportions that threaten the security of public and state. Fuzzy logic-based decision support system was developed in this study in order to act more conscious against cyber-terror attacks and see what can be done in advance against cyber attacks on critical systems. The developed model evaluates different criteria using fuzzy logic and reveals how to act against cyber-terror attacs.**

[1] Kerim Göztepe, Ph.D, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent,İSTANBUL, 0212-398-0100, (kerimgoztepe@yahoo.com)

[2] Ahmet Ejder, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent,İSTANBUL (a_ejders@yahoo.com), 0212-398-0100,

***Index Terms*--**Cyber-terror, fuzzy logic, decision support systems.

## I. GIRIŞ

TEKNOLOJİ devriminin en önemli iki unsuru bilgisayar ve internet sayesinde, insanlar elektronik ticaret yapmakta, banka hesaplarını kontrol edip faturalarını yatırmaktadır. İnternetin sağladığı imkânlarla istenilen hemen hemen her türlü bilgi, ses-görüntü verisi ve yazılıma erişilebilmektedir. Bilgisayarlar ülkeler arasındaki fiili sınırları ortadan kaldırmıştır. Ancak bu durum yeni ve son derece etkili bir tehdidin ortaya çıkmasına sebep olmuştur: siber terör. Tüm dünyada olduğu gibi Türkiye'de de bilgisayar korsanları, siber aktivistler ve terör örgütleri gibi siber saldırı düzenleyebilecek yeteneğe sahip kişi veya gruplar bilgisayar ve internet teknolojilerini yakından takip etmektedir. Bu kişi veya gruplar siber dolandırıcılık, propaganda, gizli bilgileri ele geçirme, istihbarat toplama gibi birçok faaliyeti yapabilecek yetenektedir [1],[2],[3].

Siber saldırılar, siber saldırı türleri, bunların etkinliği ve sonuçları üzerine yapılan çalışmalarda artış yaşanmaktadır. Siber saldırıların sebep olacağı mali ve diğer zararların önlenmesine yönelik Rees ve diğ.[4] bir karar destek sistemi ortaya koymuşlardır. Prichard ve MacDonald [5], çalışmalarında 11 Eylül saldırılarında teröristlerin kullandıkları veya kullanmış olabilecekleri yöntemleri incelemiştir. Özkan çalışmasında, bilişim teknolojisinden yararlanarak kritik tesis ve sistemlere, kamu kuruluşlarına, banka ve finans merkezlerine siber saldırılarda bulunabilecek terör örgütlerini incelemiştir [3]. Garricka muharebe alanında meydana gelecek siber saldırılara karşı koymak maksadıyla bir metodolji geliştirmişlerdir [6].

## II. SIBER TERÖR

Stanford Taslağı olarak bilinen belge, siber terörizmle ilgili tanımlara açıklık getirmeye çalışmıştır. Bu belgede siber terör "hukuken yetkili kılınmış görevlilerinin eylemleri dışında, siber sistemlere karşı girişilen ve kişi veya kişilerin ölümü ya da yaralanması, kamu düzeninin bozulması veya önemli ekonomik zararlara neden olması muhtemel olan şiddet, bozma ve engelleme eylemlerinin kasıtlı şekilde yapılması veya yapılacağı tehdididir" ifadesiyle tanımlanmıştır [7]. Genel bir ifadeyle siber terörizmi, terör eylemlerinin bilgisayar ve bilgisayar sistemleri kullanılarak icra edilmesi şeklinde tanımlamak da mümkündür [3].

Siber saldırıları düzenleyenler teknolojiyi etkin biçimde kullanarak geçmişten günümüze kabiliyetlerini artırmıştır. Bilinen ilk siber suç, Minneapolis Tribune'de yayınlanan "Bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" başlıklı makale ile 18 Ekim 1966'de kamuoyuna yansımıştır [8]. Rusya-Gürcistan savaşında başta devlet başkanlığı web sitesi olmak üzere Gürcistan'ın neredeyse tüm web sayfaları bloke edilmiştir. Finans merkezleri, haberleşme sistemleri ve elektrik santralleri ciddi sıkıntı yaşamıştır [11]. İnternete uygulanan "filtre" karşısında temel hak ve özgürlüklerin ihlal edileceğini savunan "Anonymous" (Anonim) adlı uluslararası kırıcı (hacker) topluluğu Telekomünikasyon ve İletişim Başkanlığı'nın (TİB) web sitesine DDos saldırıları gerçekleştirmiştir [10]. Tüm bu saldırılar gelecekte siber güvenliğin önemini ortaya koymaktadır. Zamanında alınmayan bilişim tedbirleri Gürcistan-Rusya savaşında olduğu gibi ülkeyi kaosa sürükleyebilir.

Aslında siber saldırıların ortaya çıkardığı güvenlik sorunu öylesine önemli bir hal almıştır ki NATO gibi klasik tehdit algılaması üzerine inşa edilmiş bir kuruluştan da önemli ilgi görmüştür. En son 2010 yılında Lizbon'da yapılan NATO Zirvesi'nde NATO'nu yeni kapsamlı yaklaşımı ve konsepti ortaya konmuş ve siber tehdit de bu konseptin önemli bir bacağını oluşturmuştur. NATO yeni konseptinde siber tehdidin nereden geleceğiyle pek ilgilenmemiş ve daha çok böyle bir tehdidin varlığından ve nasıl tedbir getirileceğinden söz etmiştir [22]. Konuya tehdit perspektifinden bakıldığında tehdidin kaynağı, tehdidin etkin hale gelmesi ve tehdidin etkisini göstermesinden sonraki sonuçları önem arz etmektedir. Bu makalede tehdidin etkisini göstermesinden sonraki sonuçları sorgulama alanı dışında bırakılarak bizatihi "tehdidin kaynağı" ve "tehdidin etkin hale gelmesi" aşamasındaki boyutları incelenmeye çalışılacaktır.

Siber tehdidin karmaşık yapısı, insan ve makina özelliklerini birlikte taşıması, kanal ve ajanlarının oldukça farklı ve yeni yaratımlara açık yapısı bu konunun çözüm kümesinin (0,1) elemanlarından daha fazlasından oluşması olasılığını artırmaktadır. Bu nedenle konunun bulanık mantıkla modellenmesinin daha yararlı olacağı değerlendirilmektedir. Dolayısıyla mevcut çalışmada güdülen maksatlardan biri bizatihi çözüm kümesine ulaşmak olduğu kadar bu konunun sunulan bulanık model mantığıyla çalışılmasının uygulanabilirliğini de göstermektir.

## III. BULANIK MANTIK

Zadeh belirsizliğin temsili için araç olarak, bulanık kümeler (fuzzy sets) teorisini geliştirmiştir [14]. Bulanık mantık, insan düşüncesinin ortaya koyduğu sözel bilgileri matematiksel verilere çevirmekte ve bunları bulanık küme teorisi ile ifade edebilmektedir [15],[17]. Bulanık mantıkla ilgili tanımlar aşağıda ifade edilmiştir.

**Tanım 1:** Bulanık küme teorisinde, üyelik fonksiyonlarının değer aralığı [0,1] değerleri arasında yer alır. $\mu_{\tilde{A}}(x)$ ; $\tilde{A}$ bulanık kümesinin üyelik fonksiyonudur. Bu fonksiyonun alacağı değere, $x$ elemanının $\tilde{A}$ bulanık kümesindeki üyelik değeri denir ve $\mu_{\tilde{A}}(x) \rightarrow [0,1]$ şeklinde gösterilir [16].

Bir $\tilde{A}$ bulanık kümesi, $x$ elemanı ve $\mu_{\tilde{A}}(x)$ derecesinin bir kümesi olarak tanımlanabilir ve

$\tilde{A} = \{(x, \mu_{\tilde{A}}(x)) | x \in X\}$ şeklinde ifade edilir. Eğer $\tilde{A}$ bulanık kümesinin elemanları kesikli ise,

$$\tilde{A} = \sum_{i=1}^{n} \mu_{\tilde{A}}(x_i)/x_i = \mu_{\tilde{A}}(x_1)/x_1 + \mu_{\tilde{A}}(x_2)/x_2 + \ldots + \mu_{\tilde{A}}(x_n)/x_n \quad (1)$$

sürekli ise,

$$\tilde{A} = \int_x \mu_{\tilde{A}}(x)/x \quad (2)$$

şeklinde ifade edilir. Formüllerde kullanılan sigma ve integral işaretleri matematiksel bir anlam belirtmez.

**Tanım 2:** Bir $\tilde{A}$ bulanık kümesinin desteği (support), $\mu_{\tilde{A}}(x) > 0$ olacak şelikde bütün $x \in X$ 'lerin oluşturduğu kesin kümedir ve $S(\tilde{A}) = \{x \in X | \mu_{\tilde{A}} > 0\}$ şeklinde ifade edilir [12].

**Tanım 3:** $\tilde{A}$ bulanık kümesinin üyelik fonksiyon derecesi en az $\alpha$ seviyesinde olan elemanlarının kesin kümesi $\alpha$ – seviye kümesi olarak adlandırılır ve $\tilde{A} = \{x \in X | \mu_{\tilde{A}}(x) \geq \alpha$ şeklinde ifade edilir.

**Tanım 4:** Bir $\tilde{A}$ bulanık kümesi $\forall x_1, x_2 \in X \; ve \lambda \in [0,1] için$

$\mu_{\tilde{A}}(\lambda x_1 + (1 - \lambda x_2) \geq \min(\mu_{\tilde{A}}(x_1), \mu_{\tilde{A}}(x_2))$ koşulunu sağlıyorsa konvekstir.

**Tanım 5**: $X$ üzerinde tanımlı bir $\tilde{A}$ bulanık kümesinin yüksekliği, $\mu_{\tilde{A}}(x)$'in en küçük üst sınırıdır ve

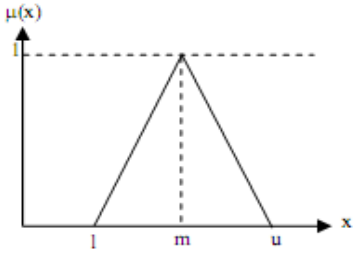
$hgt(\tilde{A}) = \sup_{x \in X} \mu_A(x)$ ile ifade edilir [13].

**Tanım 6:** $\tilde{C} = \tilde{A} \cap \tilde{B}$ kesişim işleminin üyelik fonksiyonu, $\mu_{\tilde{C}}(x) = min\{\mu_{\tilde{A}}(x), \mu_{\tilde{B}}(x)\}, x \epsilon X$ olarak tanımlanır.

**Tanım 7:** $\tilde{D} = \tilde{A} \cup \tilde{B}$ birleşim işleminin üyelik fonksiyonu, $\mu_{\tilde{D}}(x) = max\{\mu_{\tilde{A}}(x), \mu_{\tilde{B}}(x)\}, x \epsilon X$ olarak tanımlanır [12].

**Tanım 8:** $\tilde{A}$ bulanık kümesinin $\overline{\tilde{A}}$ tümleyeni, $\forall x \in X \; için \; \mu_{\tilde{A}}(x) = 1 - \mu_{\tilde{A}}(x)$ üyelik fonksiyonu ile tanımlanmıştır.

**Üçgensel Bulanık Sayı:** Bir üçgen bulanık sayı (triangular fuzzy number -TFN) $(l|m, m|u)$ veya $(l, m, u)$ şeklinde gösterilir [21]. Bir bulanık olay için $l$, $m$ ve $u$ parametreleri, sırasıyla mümkün en küçük değeri, en çok beklenen değeri ve mümkün olan en büyük değeri temsil eder. Şekil 1.'de örnek olarak bir bulanık üçgen sayı verilmiştir.




Şekil 1. Bulanık üçgen sayı $(l,m,u)$

Bir üçgen bulanık sayının lineer gösterimi sol ve sağ taraf şeklinde aşağıdaki üyelik fonksiyonu ile tanımlanabilir [21]

$$\mu(x/\tilde{M}) = \begin{cases} 0, & x < l, \\ (x-l)/(m-l), & l \le x \le m, \\ (u-x)/(u-m), & m \le x \le u, \\ 0, & x > u. \end{cases} \quad (3)$$

## IV. Siber Teröre Yönelik Bulanık Karar Destek Modeli

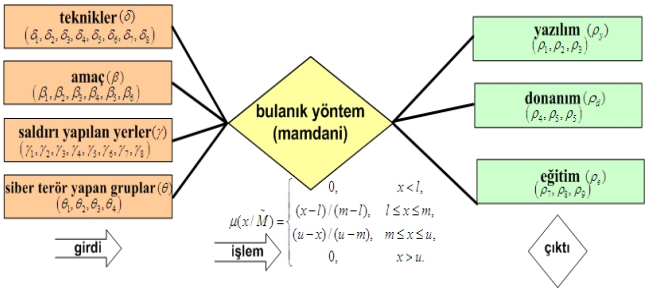
Bu çalışmada herhangi bir kuruluşa yapılacak siber terör saldırısının önlenmesine veya muhtemel bir siber saldırıdan önce sistemin gözden geçirilmesine yönelik bulanık bir karar destek sistemi ortaya konmuştur. Önerilen bulanık karar destek sistemi dört adımdan oluşmaktadır.

### Adım 1: Siber saldırı önleme grubunun oluşturulması

Siber saldırıların önlenmesine yönelik bu konuda tecrübe sahibi uzman bir grup kurulmuştur. Oluşturulan siber karar destek grubunda yer alan tüm personel özellikle kritik kamu bilişim sistemlerinin yönetiminde uzmandır.

### Adım 2: Bulanık karar destek sistemi kriterlerinin belirlenmesi

Belirlenen siber karar destek grubu olabilecek siber saldırıları ve bunları engellemeye yönelik kriterleri daha önce bu konuda yapılan çalışmalarıda[4],[5] değerlendirerek tespit etmiştir. Modelde "teknikler", "amaç", "saldırı yapılan yerler" ve "siber terör yapan gruplar" olarak dört girdi kriteri tanımlanmıştır. Çıktı kriteri olarak "yazılım", "donanım" ve "eğitim" kriterleri belirlenmiştir. Şekil 2' de modelin genel görünümü verilmiştir.




Şekil 2.Tasarlanan model

Modelle ilgili bilgiler Tablo I'de verilmiştir. Tablonun sol tarafındaki girdi sütununda modelde kullanılan kriterler, tanım sütununda kriterlere ait sayısallaştırılan ifadeler verilmiştir. İfadelerin bulanık değerleri ise "bulanık değerler" sütununda verilmiştir. Sayısallaştırılan ifadelerin belirlenmesinde ve bulanık değerlerin atanmasında uzman kişilerin görüşlerinden yararlanılmıştır.

TABLO I
MODELIN KRITERLERI, KISALTMALARI VE BULANIK DEĞERLERI

| Girdi | Tanım | Simge | Bulanık Değer |
|---|---|---|---|
| Teknikler ($\delta$) | Ağ saldırısı | $\delta_1$ | [0 0 0,1] |
| | DoS saldırısı | $\delta_2$ | [0,05 0,1 0,2] |
| | Virüs | $\delta_3$ | [0,1 0,3 0,5] |
| | E-mail virüs | $\delta_4$ | [0,1 0,5 0,7] |
| | Truva atı | $\delta_5$ | [0,6 0,7 0,8] |
| | Sosyal mühendislik | $\delta_6$ | [0,8 0,9 1] |
| | Zararlı yazılım | $\delta_7$ | [0,9 1 1] |
| | Mantık bombası | $\delta_8$ | [0,5 0,6 0,65] |
| Amaç ($\beta$) | Hizmet dışı bırakmak | $\beta_1$ | [0 0 0,2] |
| | Web syfsını ele geçirmek | $\beta_2$ | [0,1 0,3 0,6] |
| | Küçük düşürmek | $\beta_3$ | [0,3 0,5 0,65] |
| | Gizli bilg. ele geçirmek | $\beta_4$ | [0,8 0,85 0,9] |
| | Kritik sist. ele geçirmek | $\beta_5$ | [0,4 0,6 0,8] |
| | Kontrol etmek | $\beta_6$ | [0,85 1 1] |
| Saldırı yapılan yerler ($\gamma$) | Haberleşme | $\gamma_1$ | [0 0,3 0,6] |
| | Banka ve finans | $\gamma_2$ | [0,2 0,3 0,4] |
| | Elektrik santralleri | $\gamma_3$ | [0,8 0,85 0,9] |
| | Petrol ve doğalgaz dağıtım | $\gamma_4$ | [0,85 0,9 1] |
| | Su şebekesi | $\gamma_5$ | [0,7 0,8 0,85] |
| | Ulaştırma | $\gamma_6$ | [0,5 0,6 0,7] |
| | Acil hizmetler | $\gamma_7$ | [0,45 0,55 |
| | Kamu kuruluşları | $\gamma_8$ | [0,4 0,65 |
| Siber terör yapan gruplar ($\theta$) | Bilgisayar korsanları | $\theta_1$ | [0 0,4 0,8] |
| | Siber aktivistler | $\theta_2$ | [0,7 0,85 1] |
| | Sistem düşmanları | $\theta_3$ | [0,7 0,8 0,9] |
| | Özel personel | $\theta_4$ | [0 0,1 0,2] |
| **Çıktı** | **Tanım** | **Simge** | **Bulanık Değer** |
| Yazılım ($\rho_y$) | Milli yazılım | $\rho_1$ | [0 0,25 0,5] |
| | Güncelleme | $\rho_2$ | [0,2 0,5 0,7] |
| | Ulusal bilgi merkezi | $\rho_3$ | [0,5 0,75 1] |
| Donanım ($\rho_d$) | Fiziksel kontrol | $\rho_4$ | [0 0,25 0,5] |
| | Kritik bilgisayarlar | $\rho_5$ | [0,3 0,5 0,7] |
| | Teknik destek | $\rho_6$ | [0,6 0,8 1] |
| Eğitim ($\rho_e$) | Kullanıcı eğitimi | $\rho_7$ | [0 0,3 0,6] |

| | | |
|---|---|---|
| **Farkındalık** | $\rho_8$ | **[0,3 0,5 0,7]** |
| **Kullanıcı kontrolü** | $\rho_9$ | **[0,6 0,8 1]** |

**Teknikler:** Siber saldırı yapan kişi veya gruplar farklı teknikler kullanmaktadır. Bu kriter siber saldırıların hangi teknik kullanılarak yapıldığını ifade eder. Siber saldırılarda en çok kullanılan tekniklerden olan "ağ saldırıları, DoS, virüs, e-maille virüs gönderme, truva atı, insanların kandırılarak bilgilerinin ele geçirilmesi (sosyal mühendislik), zararlı yazılım (malware) ve mantık bombası gibi yöntemler sayısallaştırılarak modele girilmiştir. Diğer kriterlere ait bilgiler Tablo I'de olduğu gibidir.

**Amaç:** Siber saldırıların genellikle bir amacı vardır. Eğlence amaçlı saldırıların yanında çok özel amaçlara sahip siber saldırılar gerçekleşebilir.

**Saldırı yapılan yerler:** Siber saldırıları gerçekleştirenler amaçları doğrultusunda ki hedeflere saldırı düzenlerler. Bu çalışmada devlet kuruluşlarıyla birlikte hassas sivil kuruluşlar da göz önüne alınmıştır.

**Siber terör yapan gruplar:** Siber terör yapan kişi veya kişilerin belirli bir özelliği yoktur. Heyecan arayan bir öğrenci iyi korunan sistemlere bile ciddi zararlar verebilir. Bununla birlikte en tehlikeli kişiler profesyonel bilgiye sahip, belirli hedefler için saldırı düzenleyen kişilerdir.

**Çıktı:** Tehdit algılamasının değerlendirilmesi sonucunda, değerlendirmeyi yapan ilgili kurum veya kuruluş modelin çıktılarına göre var olan sistemini yeniden gözden geçirmeli, eğer yeni bir sistem kurulacaksa model değişik senaryolara göre çalıştırılmalı ve elde edilen sonuçlar yazılım, donanım ve sistem kullanıcılarının eğitimi açısından incelenmelidir.

**Adım 3. Uygulama kuralları ve çıkarım yönteminin belirlenmesi**

Tasarlanan modelde bulanık çıkarım yöntemleri içerisinde en yaygın kullanılan yöntem olan Mamdani kullanılmıştır. Bir bulanık kural, 'eğer. ise, ... olsun' şeklinde ( *z değeri a ise, t değeri b olsun gibi*) sözel girdi ve çıktı terimlerine sahip olmalıdır. 'eğer ...' bölümüne durum; '... olsun' bölümüne ise sonuç ya da karar kısmı adı verilir. Bulanık kural örneği aşağıda verilmiştir [19].

$$IF\ (x_1 = A_{11})\ AND\ (x_2 = A_{12})\ THEN\ (z_1 = C_1) \quad (4)$$

$$IF\ (x_1 = A_{21})\ OR\ (x_2 = A_{22})\ THEN\ (z_2 = C_2) \quad (5)$$

Siber terör saldırılarının engellenmesine yönelik bulanık karar destek modelinde 78 kural tanımlanıştır.

**Durulaştırma:** Bu çalışmada Mamdani yöntemi kullanıldığından sonuç değerleri bulanık olarak elde edilmiştir. Bu nedenle durulaştırma aşamasına ihtiyaç vardır. Durulaştırma işlemi bulanık modelin son aşaması olup bulanık bilgiler kesin sonuçlara dönüştürülür [18].

Durulaştırma işleminde en çok kullanılan yöntemler "yükseklik" ve "ağırlık merkezi" yöntemidir. Bu çalışmada durulaştırma işlemi için eşitlik 6'da ifade edilen "ağırlık merkezi yöntemi (centroid)" kullanılmıştır. Tüm durulaştırma işlemleri MATLAB programında gerçekleştirilmiştir.

$$y^* = \frac{\sum_{i=1}^{n} y_i \mu_{\tilde{A}}(y_i)}{\sum_{i=1}^{n} \mu_{\tilde{A}}(y_i)} \quad (6)$$

**Adım4. Siber tehdit engelleme bulanık karar destek sisteminin uygulanması**

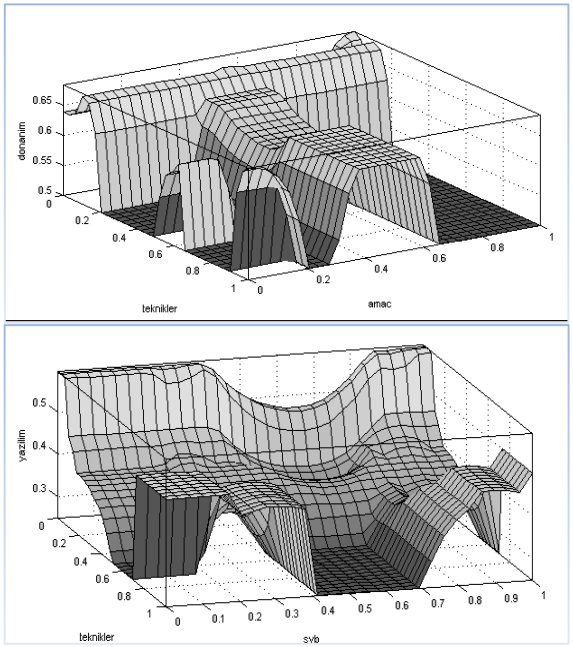
Geliştirilen model siber saldırılara karşı alınması gereken tedbirlerle ilgili bulanık karar destek sistemi ortaya koymaktadır. Siber tehditlere karşı en uygun kararların alınabilmesi için Tablo I' de verilen küme ve kriterler değerlendirilmiştir. Modelin uygulanmasıyla ilgili iki örnek siber saldırı senaryosu aşağıda verilmiştir.

**Senaryo 1:**"Ağa saldırı ($\delta = \delta_1$)" tekniği kullanılan, saldırı amacının "hizmet dışı bırakma ($\beta = \beta_1$)" ve saldırı yapılan bölgenin haberleşme sistemleri ($\gamma = \gamma_1$) olduğu bir sistem sunucusuna yapılan bir siber saldırının kuralı eşitlik 7'de ifade edilmiştir.

$$if\ [(\delta\ is\ \delta_1) and\ (\beta\ is\ \beta_1) and\ (\gamma\ is\ \gamma_1)]$$

$$then\ [(\rho_d\ is\ \rho_6)] \quad (7)$$

Bu durumda sisteme "teknik destek ($\rho_d = \rho_6$) " sağlanmalıdır (Şekil 3).




Şekil 3. Senaryo 1. çözüm uzayı

**Senaryo 2:** "Özel eğitimli $(\theta = \theta_4)$" kişilerce "zararlı yazılım $(\delta = \delta_7)$ kullanılarak "kontrol $(\beta = \beta_6)$ edilmek istenen bir "kamu kuruluşu $(\gamma = \gamma_8)$" sistemine organize siber saldırılar yapılmaktadır. Bu tip bir saldırıya karşı "milli yazılım $(\rho_y = \rho_1)$" kullanılmalı özel üretim "kritik bilgisayarlar" $(\rho_d = \rho_5)$ temin edilmeli ve bu bilgisayarların "kullanıcıları $(\rho_e = \rho_7)$ eğitilmelidir" (Eşitlik 8).

$$if \begin{bmatrix} (\delta\ is\ \delta_7) and\ (\beta\ is\ \beta_6) and\ (\gamma\ is\ \gamma_8)\ and \\ (\theta\ is\ \theta_4) \end{bmatrix}$$

$$then\ [(\rho_y\ is\ \rho_1)\ and\ (\rho_d\ is\ \rho_5)\ and\ (\rho_e\ is\ \rho_7)] \quad (8)$$

## V. SONUÇ

Günümüzde internet kullanımının ve internete erişiminin yeni mobil teknolojilerle birlikte hem kolay hem de rahat olması internetin basit, yaygın ve cazip bir araç yapmıştır. Toplumsal hayatı kolaylaştıran onlarca uygulama, bilgi, doküman internet ortamına taşınmıştır. Bu durum kötü niyetli kullanıcılar ve dolandırıcılar, gizli belgelere ulaşmak isteyen özel eğitimli kişiler, siber aktivistler gibi internet ortamının sunduğu sınırsızlıktan yararlanmak isteyen kişilere fırsatlar sunmaktadır. İnternetin yaygın olarak kullanılmaya başlanmasıyla birlikte sağlık, eğitim, finans başta olmak üzere tüm kamu kurumları ve özel sektörün yoğun olarak bilişim teknolojilerini bünyelerine entegre etmeleri sonucu, bu kurum ve kuruluşlara ait sistemlere yapılacak bir siber saldırı günlük hayatı felç edecektir.

Bu çalışmada mevcut bir siber saldırıya karşı gösterilecek reaksiyon veya olabilecek siber saldırılara karşı alınabilecek tedbirleri tespit etmek amacıyla bulanık mantık temelli bir karar destek sistemi geliştirilmiştir (modelin tüm yapısı Ek-A'da verilmiştir). Modelin kriterleri daha önce bu konuda yapılan çalışmalar ışığında siber saldırılar konusunda tecrübeli uzman personel ile bilişim uzmanları tarafından tespit edilmiştir. Tespit edilen kriterler kullanılma yaygınlığı ve vereceği zararlar dikkate alınarak sayısallaştırılmıştır. Modelin hassasiyetinin artırılması için çok sayıda kural belirlenmiştir. Çeşitli test senaryolarının modelde çalıştırılması sonucu gerçekleşen olaylar için alınan tedbirlere çok yakın sonuçlar elde edilmiştir. Özellikle kamu bilişim sistemlerinde milli yazılım kullanılması ve bilinçli kullanıcı önemli bir konu olarak karşımıza çıkmaktadır.

Saldırı tekniklerinin ve verdiği zararların zaman içinde değişmesi modelin güncellenmesini zorunlu kılmaktadır. Siber saldırıları engelleme bulanık karar destek modeli yeni kriterler (siber saldırganların psikolojisini değerlendirilen kriterler gibi) ve kurallar eklenerek geliştirilebilir.

## EKLER

Siber terör bulanık karar destek sistemi MATLAB model bilgileri Ek-A'da verilmiştir.

## KAYNAKLAR

[1] AEM (Ankara Emniyet Müdürlüğü), Bilişim Suçları Büro Amirliği Tespitleri, 2004.
[2] F.Yamaç, S.Dokurer ve M. Özcan, "Bilişim Suçları", http://www.inetr.org.tr/inetconf7/bildiriler/86.doc> (11.11.2005).
[3] T.Özkan, 2006, "Siber Terörizm Bağlaminda Türkiye'ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analizi", Yüksek Lisans Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, 2006
[4] L.P. Rees, et al., Decision support for Cybersecurity risk planning, Decis. Support Syst., doi:10.1016/j.dss.2011.02.013.,2011
[5] J.J. Prichard and, L.E. MacDonald, Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks, Journal of Information Technology Education, Volume 3. 2004
[6] B.J.Garricka, J.E. Hallb et.al, Confronting the risks of terrorism: making the right decisions, Reliability Engineering and System Safety, 86,p.129-176,2004
[7] M.Özcan, "Cybercrimes: Infrastructure Threats from Cyberterrorist", Cyberspace Lawyer, 4 No:2, (Cyberspace Law 23'den aktaran Mehmet Özcan, Siber Terörizm ve Ulusal Güvenlik: İnternet ve Hukuk, -İstanbul: Bilgi Üniversitesi Yay., s.309),2002
[8] E. Aydin, Bilişim Suçları ve Hukukuna Giriş, Ankara, s.13.,1992
[9] http://haber.ekolay.net/Haber/2705/786920/ve-siber-saldirilar-basladi.aspx, 12.06.2011, erişim tarihi 15 Temmuz 2011.
[10] http://news.cnet.com/8301-1009_3-10014150-83.html, 01.08.2008, erişim tarihi 15 Temmuz 2011.

[11] H. J Zimmermann, Fuzzy Sets Theory and Its Applications, Seconds, Revised Edition, Sixth Printing, Kluwer Academic Publishers, Boston / Dordrecht / London. 1993
[12] M., Sakawa, Fuzzy Sets and Interactive Multiobjective Optimization, Plenum Pres,New York. 1993
[13] L.A, Zadeh, Fuzzy sets. Information Control 8,p. 338-353, 1965
[14] L.A, Zadeh, , Is There a Need for Fuzzy Logic?, Information Sciences, 2008
[15] H.J. Zimmermann, Fuzzy Set Theory and its Applications, Kluwer Academic Publishers, London.,1994
[16] D. Dubois, H. Prade, An introduction to fuzzy systems Clinica Chimica Acta 270,3-29.,1998
[17] H.T.Nguyen, Fuzzy and Random Sets. Fuzzy Sets and Systems. 156(3),p.349–356.,2005
[18] M.M. Mazzucco,, A. Bolzan, R.M. Barcia and R.A. F. Machado, Application of genetic algorithms to the adjustment of the supports of fuzzy sets in a mamdani controller. Braz. J. Chem. Eng., 17 (4),p. 625-638., 2000
[19] M. Cerrada, J. Aguilar, E. Colina and A. Titli, Dynamical Membership Functions: An Approach for Adaptive Fuzzy Modelling. Fuzzy Sets and Systems, 152(3),p.513–533.,2005
[20] D.Y. Chang, Applications of the extent analysis method on fuzzy AHP. European Journal of Operational Research, 95, p.649-655.,1996
[21] NATO, 2010 Lisbon Summit Declaration, http://www.nato.int/cps/en/natolive/official_texts_68828.htm (Erişim tarihi 17.08.2011),

EK-A

**[SİBER TERÖR BULANIK KARAR DESTEK SİSTEMİ MODELİ]**

```
Model
Type='mamdani'
Version=2.0
NumInputs=4
NumOutputs=3
NumRules=78
AndMethod='min'
OrMethod='max'
ImpMethod='min'
AggMethod='max'
DefuzzMethod='centroid'
```

```
[Input1]
Name='teknikler'
Range=[0 1]
NumMFs=8
MF1='agsaldiri':'trimf',[0 0 0.1]
MF2='DoS':'trimf',[0.05 0.1 0.2]
MF3='virus':'trimf',[0.1 0.3 0.5]
MF4='emailvirus':'trimf',[0.1 0.5 0.7]
MF5='truva':'trimf',[0.6 0.7 0.8]
MF6='sosm':'trimf',[0.8 0.9 1]
MF7='malware':'trimf',[0.9 1 1]
MF8='mantikb':'trimf',[0.5 0.6 0.65]
```

```
[Input2]
Name='amac'
Range=[0 1]
NumMFs=6
MF1='hdb':'trimf',[0 0 0.2]
MF2='wseg':'trimf',[0.1 0.3 0.6]
MF3='pro':'trimf',[0.3 0.5 0.65]
MF4='gbeg':'trimf',[0.8 0.85 0.9]
MF5='kseg':'trimf',[0.4 0.6 0.8]
MF6='kontet':'trimf',[0.85 1 1]
```

```
[Input3]
Name='saldırı yapılan bölge'
Range=[0 1]
NumMFs=8
MF1='hab':'trimf',[0 0.3 0.6]
MF2='bvef':'trimf',[0.2 0.3 0.4]
MF3='esant':'trimf',[0.8 0.85 0.9]
MF4='petgs':'trimf',[0.85 0.9 1]
MF5='sus':'trimf',[0.7 0.8 0.85]
MF6='ulsm':'trimf',[0.5 0.6 0.7]
MF7='acilh':'trimf',[0.45 0.55 0.65]
MF8='devb':'trimf',[0.4 0.65 0.85]
```

```
[Input4]
Name='siber terör yapan gruplar'
Range=[0 1]
NumMFs=4
MF1='bilkor':'trimf',[0 0.4 0.8]
MF2='siberak':'trimf',[0.7 0.85 1]
MF3='habcok':'trimf',[0.7 0.8 0.9]
MF4='ozelp':'trimf',[0 0.1 0.2]
```

**KURALLAR**

```
1 1 1 0, 0 3 0 (1) : 1
4 0 0 0, 1 2 1 (1) : 1
1 2 8 2, 1 3 0 (1) : 1
7 6 8 4, 1 2 1 (1) : 1
6 6 1 1, 2 0 0 (1) : 1
0 2 8 4, 1 3 0 (1) : 1
2 1 5 1, 3 3 0 (1) : 1
6 4 2 1, 0 0 1 (1) : 1
6 4 8 2, 0 0 1 (1) : 1
0 2 1 2, 2 0 0 (1) : 1
0 3 8 4, 1 3 0 (0.8) : 1
0 3 6 4, 1 3 0 (1) : 1
0 3 1 3, 2 0 2 (1) : 1
1 3 0 4, 1 2 2 (1) : 1
1 6 0 4, 3 3 1 (1) : 1
1 4 8 2, 2 3 1 (1) : 1
5 4 2 4, 3 0 3 (1) : 1
5 4 8 2, 3 0 3 (1) : 1
5 6 8 3, 1 2 0 (1) : 1
6 6 5 4, 1 3 1 (1) : 1
6 6 6 4, 1 3 1 (1) : 1
6 6 4 4, 1 3 1 (1) : 1
6 6 3 4, 1 3 1 (1) : 1
6 6 7 4, 1 3 1 (1) : 1
7 1 0 0, 1 3 2 (1) : 1
0 6 8 4, 0 1 0 (1) : 1
0 6 8 2, 1 2 1 (1) : 1
0 4 2 1, 2 3 3 (1) : 1
2 3 0 0, 0 3 0 (1) : 1
2 3 1 1, 0 3 0 (1) : 1
2 3 8 2, 0 3 0 (1) : 1
2 3 1 3, 0 3 0 (1) : 1
2 3 1 4, 1 3 0 (1) : 1
2 1 6 4, 1 3 0 (1) : 1
8 1 1 1, 2 3 0 (1) : 1
8 0 8 4, 1 3 0 (1) : 1
8 0 1 4, 1 3 0 (1) : 1
8 0 8 1, 1 2 1 (1) : 1
8 0 1 3, 2 3 2 (1) : 1
0 0 8 4, 1 2 1 (1) : 1
0 0 8 3, 1 2 1 (1) : 1
0 0 8 2, 1 2 1 (1) : 1
0 0 8 1, 1 2 1 (1) : 1
0 0 2 4, 2 3 3 (1) : 1
0 0 2 1, 2 3 3 (1) : 1
0 0 6 4, 1 2 2 (1) : 1
0 0 7 4, 1 2 2 (1) : 1
0 0 3 4, 1 2 2 (1) : 1
0 4 8 4, 3 2 2 (1) : 1
0 4 8 4, 1 1 3 (1) : 1
0 5 8 4, 3 1 2 (1) : 1
0 5 7 2, 1 3 1 (1) : 1
0 5 1 3, 1 3 1 (1) : 1
0 5 4 2, 2 3 1 (1) : 1
1 0 0 1, 2 0 0 (1) : 1
1 0 0 4, 3 0 0 (1) : 1
1 0 0 2, 2 0 0 (1) : 1
2 0 0 4, 1 3 1 (1) : 1
2 0 0 3, 2 3 1 (1) : 1
2 0 0 1, 2 3 1 (1) : 1
0 4 0 4, 0 1 0 (1) : 1
6 0 2 0, 2 0 1 (1) : 1
6 3 7 0, 0 0 1 (1) : 1
3 1 0 0, 2 0 2 (1) : 1
7 1 0 0, 2 0 2 (1) : 1
8 1 0 0, 2 0 2 (1) : 1
5 1 0 0, 2 0 2 (1) : 1
3 3 0 0, 2 0 2 (1) : 1
0 1 1 0, 1 0 0 (1) : 1
0 1 8 0, 3 0 0 (1) : 1
0 2 8 0, 1 0 0 (1) : 1
0 3 8 0, 1 3 0 (1) : 1
0 3 5 0, 2 0 0 (1) : 1
0 3 4 0, 2 0 0 (1) : 1
0 3 3 0, 2 0 0 (1) : 1
1 4 0 0, 3 2 3 (1) : 1
1 5 0 0, 3 2 3 (1) : 1
1 6 0 0, 3 3 1 (1) : 1
```

```
[Output1]
Name='yazilim'
Range=[0 1]
NumMFs=3
MF1='milliy':'trimf',[0 0.25 0.5]
MF2='guncel':'trimf',[0.2 0.5 0.7]
MF3='ubm':'trimf',[0.5 0.75 1]

[Output2]
Name='donanim'
Range=[0 1]
NumMFs=3
MF1='fzkont':'trimf',[0 0.25 0.5]
MF2='kritikblg':'trimf',[0.3 0.5 0.7]
MF3='teknikdstk':'trimf',[0.6 0.8 1]

[Output3]
Name='kullanici egitimi'
Range=[0 1]
NumMFs=3
MF1='kullanicie':'trimf',[0 0.3 0.6]
MF2='farkindalik':'trimf',[0.3 0.5 0.7]
MF3='kullanicikont':'trimf',[0.6 0.8 1]
```

# Açık Kaynak İstihbarat ve Siber Güvenlik

**İlkay ÜNAL**
STM – Savunma Teknolojileri Mühendislik ve Tic.A.Ş., Ankara
iunal@stm.com.tr

***Özet*— Açık kaynak istihbarat, topluma açık kaynaklardan bilgilerin bulunması, seçilmesi ve toplanması suretiyle bilginin yönetilmesi ve analiz edilerek istihbarat üretilmesidir [1]. Açık kaynak istihbarat, resmi ve özel kuruluşlarca bilgi edinmek amacıyla uzun zamandır internet, yazılı ve görsel medya gibi kaynaklar üzerinden üretilmektedir. İnternet ise bilgi kaynağı olarak her geçen gün daha fazla kullanılmaktadır. Fakat son yıllarda internet üzerinden akan bilginin kontrolü, güvenlik ve mahremiyet tartışmalarını da beraberinde getirmektedir. Aynı zamanda bu tartışmalar, kurumlara ve bireylere ait elektronik ortamdaki her türlü bilginin güvenliği konusunda çalışmaların yapıldığı siber güvenlik alanını gündeme getirmiştir. Bildiride, açık kaynak istihbarat, internet üzerinden akan bilginin kontrolü, bilginin toplum güvenliğine olan etkisi, siber güvenlik ve güvenlik adına alınacak önlemlerin etkinliği anlatılmaktadır.**

***Anahtar Kelimeler*— Açık kaynak istihbarat, internet, güvenlik, siber güvenlik.**

## I. GİRİŞ

İNGİLİZCE ve Fransızcada “intelligence”; kelimesi ile ifade edilen ve anlamı “akıl, zeka”; olan istihbarat kelimesinin Türkçede sözlük anlamı, haber almadır. Ancak, istihbarat terminolojisinde haber, sadece ham bilgiyi ifade eder. İstihbarat ise, devlet tarafından belirlenen ihtiyaçlara karşılık olarak açık ya da kapalı kaynaklardan derlenen haber, bilgi ve dokümanların sürekli bir şekilde işleme tabi tutulması sonucu elde edilen üründür[2]. Kapalı kaynaklardan gelen bilgilerin elde edilmesi için devletin yetkili kıldığı kurumlar düzenli çalışmaktadır. Fakat teknolojik gelişmeler istihbarat elde etmek için sadece kapalı kaynakların kullanılmasının yeterli olmadığını göstermektedir. Sağlıklı bir istihbarat üretimi için açık kaynakların da değerlendirilmesi gerekmektedir.

Açık kaynak istihbarat, topluma açık kaynaklardan bilgilerin bulunması, seçilmesi ve toplanması suretiyle bilginin yönetilmesi ve analiz edilerek istihbarat üretilmesidir. İstihbarat uzmanları genellikle açık kaynak bilgilerin yararlı olduğunu ve bu tür bilgilerin gizli kaynaklardan elde edilen veriler gibi toplanması ve analiz edilmesi gerektiğini kabul ederler. Ancak, açık kaynaklardan elde edilen bilgilerin gizli bilgilere göre değeri, bundan dolayı toplama ve analiz için harcanacak zaman ve işgücü konusunda dikkatli olunması gerektiğini düşünürler. Bilgi devriminin başlangıcından bu yana, açık kaynak bilgilerindeki artış ve internetin yaygınlaşması sonucunda istihbarat uzmanlarının açık kaynak istihbarata bakış açısı değişmiştir. Özellikle kamu bilgilerine açık kaynaklardan erişim dramatik bir artış göstermiş ve Dünya daha açık hale gelmiştir. Örneğin, Rusya'da Soğuk Savaş sonrasında açık bilginin gizli bilgiye oranının 20.80 değerinden 80:20 olarak değiştiği tahmin edilmektedir[3]. Bunun sonucu açık kaynaklara yönelik istihbarat çalışmaları artmış, buna paralel internet üzerindeki bilgi akışının denetlenmesi, güvenlik ve mahremiyet konularında tartışmaların başlamasına neden olmuştur.

## II. AÇIK KAYNAK İSTİHBARAT

### *A. Neden Açık Kaynak?*

Amerika Birleşik Devletleri'nde, İstihbarat Yetenekleri konusunda oluşturulan Komisyon, 2005 yılının Mart ayında sunulan Kitle İmha Silahları ile ilgili raporunda aşağıdaki gerekçelerden dolayı açık kaynak istihbaratın sürece dahil edilmesi gerektiğini savunmaktadır[4]:

- Doğası gereği sürekli değişen istihbarat ihtiyacını karşılamak, yabancı ülke ve kültürleri hızlı bir şekilde anlayabilmek için tüm kaynakların kullanılması gerekmektedir. Sosyal, ekonomik ve kültürel bilgilere ulaşmanın en kolay yolu açık kaynaklardır.
- Açık kaynak bilgiler gizli bilgilerin anlaşılması konusunda temel oluşturabilir. Özellikle terörizm konusundaki istihbarat açıklarını açık kaynaklardan elde edilecek bilgiler kapatabilir. Ayrıca bilgiler arasın ilişki kurulmasını sağlayabilir.
- Açık kaynak malzemeler, kaynak ve yöntemlerin korunmasını sağlayabilir. Politika yapıcılar, gizli belgelere dayanan kararları açıklamakta zorlanırken açık kaynaklara dayanan kararları kolaylıkla açıklayabilir.
- Sadece açık kaynaklar bir tarihçeye sahip olabilir. Güçlü bir açık kaynak politikasıyla dünyadaki gelişmeler takip edilebilir ve arşivlenebilir.

### *B. Açık Kaynaklar*

Bazı gözlemcilere göre açık kaynak bilgiler dört gruba ayrılmaktadır[5]:

1. Yaygın olarak bulunabilen veri ve bilgi

2. Hedeflenen ticari veri
3. Bireysel uzmanlar
4. "Gri" kaynak; özel sektör, devlet kurumları veya akademik kurumlar tarafından sınırlı sayıda kopyası üretilen, ulaşımı kısıtlı kaynaklar

Bu dört grup içine aşağıdaki kaynaklar bilgi içerebilir[6]:

- Medya: Gazete, dergi, radyo, televizyon ve bilgisayar
- Internet: Web üzerindeki sosyal paylaşım siteleri, video paylaşım siteleri, vikiler, bloglar ve içeriği kullanıcılar tarafından genişletilen her türlü site
- Kamusal veriler: Hükümet raporları, bütçe gibi resmi veriler, duruşmalar, yasama tartışmaları, basın toplantıları ve konuşmaları, güvenlik duyuruları, çevresel uyarılar, ihale ilanları
- Meslek örgütleri ve akademi: Konferanslar, sempozyumlar, meslek örgütleri faaliyetleri, akademik makaleler ve tezler
- Gözlem ve raporlama: Amatör uçak gözlemcileri, radyo takipçileri ve uydu gözlemcileri başka kaynaklarda bulunmayan önemli bilgiler sağlayabilir. Herkese açık olan dünya uydu görüntüleri (Google Earth), daha önce istihbarat servislerinin elinde olabilen yüksek çözünürlüklü görüntülerin paylaşılmasına ve incelenmesine imkân vermiştir.
- Gri edebiyat: Gezi raporları, çalışma kâğıtları, tartışma kâğıtları, gayri resmi hükümet belgeleri, dava, ön baskı araştırma raporları, çalışmalar ve pazar araştırmaları

İnternet siteleri, kullanıcıların bilgisayar ve akıllı telefonlar üzerinden erişilebilen bilgilerin paylaşılmasına olanak sağlamıştır. Internet artık bir arama aracı olmanın ötesine geçmiş, istihbarat toplamak isteyenlerin keşif ve gözetleme yaptığı açık bilgi kaynağı haline gelmiştir. Bu konuda eğitimli personel, internet sitelerini sürekli takip etmekte ve istihbarat sağlayabilecek niyet ve faaliyetleri toplamaktadır.

### *C. Kullanıcılar*

Açık kaynak istihbarat toplayan ve kullanan başlıca kurumlar aşağıda verilmiştir:

- Hükümet: Açık kaynak faaliyetler, hükümetler arasında önemli bir yer tutmaktadır. Bu faaliyetler genel olarak "gündem takibi", "medya analizi", "internet araştırması" ve "kamuoyu araştırması" olarak adlandırılır.
- İstihbarat servisleri: İstihbarat servisleri uzun zamandır açık kaynak bilgileri kullanmaktadır. ABD'de 11 Eylül saldırılarından sonra US Intelligence Community altında kurulan Ulusal Açık Kaynak Kurumu, açık kaynak istihbarattan sorumlu kurum olarak görev yapmaktadır. Bundan önce benzer görevi 1941 yılında kurulan Dış Yayın Bilgi Servisi yerine getirmekteydi.
- Askeri: Askeri istihbarat birimleri, savunmayla ilgili istihbarata ulaşmak için açık kaynaklardan faydalanmaktadır.
- Kolluk kuvvetleri: Kolluk kuvvetleri, suçların tahmin edilmesi, önlenmesi, soruşturma ve yargılama süreçlerinde açık kaynak bilgileri kullanmaktadır.
- İş dünyası: İş dünyasıyla ilgili istihbarat Ticari İstihbarat, Rakip İstihbaratı ve İş İstihbaratı olarak adlandırılmaktadır. Bunun için medyayı, ticari yayınları, derinlemesine web teknolojilerini kullanan bilgi acenteleri ve özel araştırmacılar çalışmaktadır.

## III. AÇIK KAYNAKLAR VE GÜVENLİK İKİLEMİ

Açık kaynak istihbarat yöntemlerin, artık resmi ve özel kurumlar dışında özellikle yasadışı faaliyetlerde bulunan kişi ve örgütler tarafından da kullanıldığı bilinmektedir. Özellikle terörist örgütlerin bu yöntemleri kullandığını gösteren raporlar yayınlanmaktadır. Örneğin Iraklı direnişçilerin evlerinde, İngiliz askeri üslerini gösteren detaylı Google Earth görüntüleri bulunduğu raporlanmıştır[7]. Resmi ve özel çeşitli gruplar tarafından Google Earth uygulamasının gizlilik ihlallerine ve hatta ulusal güvenliğe yönelik tehditlerin artmasına yol açtığına dair açıklamalar yapılmıştır. Buna yönelik en önemli delil, terörist grupların ilgi alanındaki askeri ve stratejik birçok bölgenin, Google Earth uygulamasıyla kolaylıkla izlenebildiğidir. Açık kaynak istihbarat açısından Google Earth uygulamasına yönelik örnek haberler aşağıda verilmiştir:

- Eski Hindistan devlet başkanlarından APJ Abdul Kalam, Hindistan'daki hassas noktaları sergileyen uygulamanın, ülke güvenliğini tehdit ettiğini ifade etti. Bunun üzerine Google Earth yetkilileri, Hintli yetkililerle işbirliği yaparak bu görüntüleri değiştirdi[8][9].
- Güney Kore hükümeti, uygulamanın, başkanlık sarayı ve kritik askeri tesisler gibi yerlerin görüntülerini, düşman komşusu Kuzey Kore tarafından kullanabilecek şekilde sunduğunu belirtti[10].
- 2006 yılında Google Earth, İsrail'in savunma güçlerini, gizli hava üslerini, Arrow hava savunma sistemlerini, Tel Aviv'deki Savunma Bakanlığına ait yerleşkeleri, Aşkelon'daki enerji tesislerini, Negev çölündeki nükleer tesisleri gösteren yüksek çözünürlüklü görüntüleri yayınlamaya başladı[11][12].
- Sydney yakınlarında bulunan Lucas Heights nükleer reaktörünün işletmecileri, Google yetkililerinden tesise ait görüntülerin çözünürlülüğünün düşürülmesini talep ettiler[13].
- Hamas ve benzeri örgütlerin, Gazze'den gerçekleştirdikleri roket saldırılarında Google Earth görüntülerinden faydalandıkları raporlandı[14][15].

- 2008 yılında yapılan Mumbai saldırılarında sağ ele geçirilen saldırgan, saldırı yapılacak yerleri tanımak için Google Earth görüntülerini kullandıklarını itiraf etti[16].
- İngiltere'de hırsızların Church of England kilisenin kurşun tavanını Googgle Earth ile tespit edip çaldıkları ve sattıkları ortaya çıktı[17].

## IV. GÜVENLİK VE MAHREMİYET

İnternet üzerindeki açık kaynak bilgilerin yol açtığı tehlikelerden en önemlisi güvenlik olmakla beraber diğer önemli konu mahremiyettir. Yine Google Earth uygulamasının bir özelliği olan Streetview, bir Google aracının sokakta gezerken kamerayla 360 derece topladığı görüntülerden oluşmaktadır. Görüntüler daha sonra birleştirilerek kullanıcıya sağlanan arayüzle 3 boyutlu gezinme hissi vermektedir. Bu arada Google aracının gezerken aldığı tüm görüntüler açık hale gelmekte, özel mülkiyetlerin bahçeleri, konutlarda, arabada, sokakta yapılan her eylem sergilenmektedir. Bu şekilde izinsiz kullanım mahremiyet sorununu beraberinde getirmektedir[18]. Bazı resmi makamlar bu görüntüleri kullanarak işlem yapabilmektedir. Örneğin İtalya'da bir iş adamının sahip olduğu gayrimenkulün değerini düşük göstererek az vergi ödediği, Google Earth görüntüleriyle ispatlanmış ve dolandırıcılıktan soruşturma açılmıştır. Bu durum, resmi makamların Google Earth uygulaması kullanmasının yasallığı konusunu gündeme getirmiştir.

Mahremiyetle ilgili tartışmaların yaşandığı diğer internet aracı ise Facebook sosyal paylaşım sitesidir. Alexa istatistiklerine göre Facebook 31 Ekim 2010 itibarıyla; Dünya'nın en fazla ziyaret edilen ikinci sitesidir[19]. Facebook'un şu anda 700 milyondan fazla üyesi bulunmaktadır[20]. Üyeler, site üzerinde kişisel bilgilerini girmekte ve arkadaşlık ilişkileri kurmaktadır. Ayrıca iletişim ve bilgi paylaşımı Facebook üzerinden mümkündür. Facebook ile gündeme gelen mahremiyet ihlalleri aşağıda sıralanmaktadır:

- Kimlik hırsızlığı: Kötü niyetli birisi, başka birisinin kimliğine bürünerek bir hesap açabilir ve diğerlerini taciz edebilir. Aslında bu herhangi bir paylaşım sitesi için geçerlidir[21][22][23]. Fakat popülaritesinden dolayı Facebook, bu konuda sık sık gündeme gelmektedir.
- Hakaret: Üyeler, paylaşım siteleri ve sahteleri üzerinden sorun yaşadıkları diğer üyeler hakkında yalan haber ve hakaret içeren paylaşımlar yapabilmektedir[24].
- Kötü alışkanlıkların paylaşımı: Facebook üyeleri ve Facebook dışından kullanıcılar, Facebook hakkında anoreksi gibi davranışları özendirici içerik taşıdığı konusunda Facebook sitesini eleştirmektedir[25].
- Reklamveren endişeleri: Ağustos 2007 tarihinde İngiltere'de First Direct, Vodafone, Virgin Media, The Automobile Association, Halifax and the Prudential firmaları, Facebook üzerinden yayınlanan reklamları geri çektiklerini duyurdu. Gerekçe olarak reklam vermek istediklerini, fakat British National Party gibi aşırı sağ görüşteki partilerin Facebook sayfalarında reklamlarının çıktığını, marka değerlerini korumak adına bu kararı aldıklarını belirttiler[26].
- Soykırım inkârı: Facebook, kullanım şartlarında belirtmesine rağmen soykırım inkârı, ayrımcılık, ırkçılık gibi içeriklerin engellenmesini garanti edememektir. Bu yüzden zaman zaman eleştiriler almaktadır[27].
- Örgütlenme: Facebook üzerinden açılan gruplar, kısa zamanda büyük rakamlara çıkabilmekte ve insanların suç amaçlı olmak üzere her türlü örgütlenmesine ve iletişimine ortam sağlamaktadır. Bu örgütlenme Arap Baharı gibi toplumsal olayları tetikleyebilmektedir. Bununla beraber Ağustos 2011'de Londra'da meydana gelen yağmalama olaylarında suç işleyenlerin sosyal paylaşım siteleri üzerinden organize oldukları tespit edilmiştir[28].

## V. BİLGİ CASUSLUĞU VE SİBER GÜVENLİK

Kamu ve özel kuruluşlara ait kritik görevlerin ve günlük işlerimizin büyük bölümü, artık elektronik ortamda yürütülmektedir. Elektronik ortamda yürüyen işlere ait bilgilerin bir kısmı açık kaynakken bir kısmı da sadece yetkilendirilmiş kullanıcılara açık durumdadır. Bu bilgilere ulaşmak isteyen kişi veya kişiler, bilgisayar sistemlerindeki güvenlik açıkları konusunda giderek uzmanlaşmakta ve siber güvenlik olarak tanımlanan elektronik sistemlerin güvenliğini tehdit etmektedir.

Siber güvenlik ve bilgi casusluğu konusunda gizli servislerin uzun süredir çalıştığı bilinen bir gerçektir[29]. Gizli bilgiler dahil her türlü bilginin elektronik ortamlarda tutulduğu düşünülürse bilgi casusluğu konusunda bilgisayarlardaki güvenlik açıklarını kullanmak çok şaşırtıcı değildir. Gizli servislerin siber güvenlik ve siber saldırılar üzerine çalıştığına dair en önemli delil, İran'ın nükleer tesislerine yapılan siber saldırıdır. Stuxnet olarak adlandırılan solucan, İran'ın nükleer santralindeki bilgisayar sistemine bulaşmış ve çalışmaların bir süre yavaşlamasına neden olmuştur[30].

Siber güvenlik açıklarını kullanmak için bu konuda uzman olmak dahi gerekmeyebilir. Nitekim Wikileaks.org sitesinde en son yayınlanan ABD diplomasisiyle ilgili gizli bilgiler, Irak'ta görevli, gizli bilgilere erişimi denetlenmeyen bir asker sızdırılmıştır[31]. NATO, bu gibi saldırılardan korunmak için, NATO Güvenlik Ofisi'ne bağlı siber güvenlik için NATO Computer Incident Response Capability (Bilgisayar Olayları Karşılama Kapasitesi) isimli özel bir birim kurmuştur[32]. Bu birim, Mayıs 2007 tarihinde Estonya'ya yapılan kapsamlı siber saldırının önlenmesinde etkin bir rol almıştır. Bu saldırıda bankaların internet servisleri ve ATM'leri durmuş, devletin birçok sitesi çalışmaz duruma gelmiştir. Benzer saldırıların otoyol, havaalanı, nükleer tesis gibi kritik yerlere yapılmasından endişe duyulmaktadır.

## VI. ALINABİLECEK ÖNLEMLER

İnternete erişimin kolaylaştığı günümüzde insanlar yaşamlarının önemli bir kısmını hâlihazırda internete taşımış durumdadır. Artık bankacılık gibi birçok işlem internet üzerinden gerçekleştiriliyor, arkadaşlık ilişkileri ve özel hayat sosyal paylaşım sitelerinden takip ediliyor. Bu derece yoğun bilgi akışının gerçekleştiği internet ortamı, doğal olarak istihbarat elde etmek isteyen kurum ve kişilerin bilgi kaynağı olacaktır. Bu yüzden istihbarat niteliği taşıyan bilgilerin internet ortamına aktarılmaması, devletlerin alacağı en önemli güvenlik önlemi olacaktır.

Kişiler olarak alınabilecek en güvenli önlem, paylaşılması sakıncalı her türlü kişisel bilginin internet ortamında paylaşılmamasıdır. Kişisel bilgilerin üye olunan site tarafından izinsiz paylaşımı söz konusu olabileceğinden, kişilerin buna uygun önlem alması gerekmektedir.

Siber güvenlik konusunda devletler, uzman kadro ve birimler oluşturmakta, yol haritaları hazırlamaktadır. Türkiye'de TÜBİTAK - Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE), T.C. Başbakanlık Devlet Planlama Teşkilatı (DPT) tarafından yayınlanan "Bilgi Toplumu Stratejisi" adlı çalışmanın 88. Maddesi gereği bilgi güvenliğiyle ilgili aşağıdaki konulardan sorumlu olarak belirlenmiştir [33].

- Kamu kurumlarının bilgi güvenliği konusunda bilinçlenmesinin sağlanması, bilgi eksikliğinin giderilmesi ve kurumlar için güncel bilgi güvenliği uyarılarının yayınlanması
- Bilgisayar Olayları Müdahale Ekibi - Koordinasyon Merkezi'nin kurulması ve etkili bir şekilde çalışması
- Kamu kurumlarının bilgi güvenliğinin sağlanması amacıyla alması gerektiği tedbirlerin belirlenmesi
- Kamu kurumlarını hedef alan tehditlerin tespit edilmesi. Bu kapsamda 25-28 Ocak 2011 tarihleri arasında Siber Güvenlik Tatbikatı gerçekleştirilmiştir.

## VII. SONUÇ

Bilgi çağının sonucu olarak internet üzerindeki bilgi her geçen gün katlanarak artmaktadır. Dolayısıyla bilgiye ulaşmak, geçmiş dönemlere göre çok daha kolaylaşmıştır. İstihbarat birimleri de doğal olarak interneti açık kaynak olarak yoğun şekilde kullanmaktadır. İnternet üzerinden elde edilen bilginin kullanılması güvenlik tartışmalarını beraberinde getirmektedir. Bu konuda siber güvenlik çalışmaları başlatılmış, herkesin bu konuda bilinçlenerek gerekli önlemleri alması hedeflenmiştir. Hayatımızı büyük ölçüde kolaylaştıran teknolojinin, bir tehdit aracı olarak kullanılmasını engellemek için başta kamu kurumları olmak üzere herkesin siber güvenlik konusunda bilinçlenmesi ve gerekli önlemleri alması gerekmektedir.

## KAYNAKÇA


[1] http://en.wikipedia.org/wiki/Open_source_intelligence
[2] http://www.mit.gov.tr/isth-olusum.html
[3] Mark M. Lowenthal, Intelligence, From Secrets to Policy, Second Edition, CQ Press (Washington, D.C.), 2003, p. 80.
[4] The Commission on the Intelligence Capabilities, March 2005, 378–379.
[5] Best R.A., Cumming A., CRS Report for Congress, December 2007.
[6] Lowenthal, Mark M. Intelligence: From Secrets to Policy, 2nd Ed. (Washington, D.C.: CQ Press, 2003) p. 79.
[7] http://news.nationalgeographic.com/news/2007/03/070312-google-censor.html
[8] "Kalam Concerned Over Google Earth". 25.01.2007.
[9] Deshpande, Rajeev (2007-02-04). "Google Earth agrees to blur pix of key Indian sites". The Times Of India.
[10] "Google Earth images compromise secret installations in S. Korea". 25.01.2007.
[11] Google 'spying' on IDF". Ynetnews.com. 06.08.2011.
[12] Daily Mail: Google Exposes Israeli Top Secret Sites
[13] "Google Earth prompts security fears". 24.01.2007.
[14] Clancy Chassay in Gaza City and Bobbie Johnson (2007-10-25). "Google Earth used to target Israel". London: Guardian. 25.08.2010.
[15] Hutcheon, Stephen (2009-01-30). "We're not stalking you or helping terrorists, says Google Earth boss". Sydney Morning Herald. 07.11.2009.
[16] Bedi, Rahul. ""Mumbai attacks: Indian suit against Google Earth over image use by terrorists"". Telegraph.co.uk. 06.08.2011.
[17] Ormsby, Avril. "Lead thieves use Google Earth to target churches". Reuters.02.11.2010
[18] http://sites.duke.edu/tlge_cs130/privacy/
[19] http://www.alexa.com/topsites
[20] http://www.facebook.com/press/info.php?statistics
[21] "Woman finds imposter on Facebook". UPI.com. 07.08.2010.
[22] From John Sutter and Jason Carroll CNN (February 6, 2009). "Fears of impostors increase on Facebook". CNN.com. 07.08.2010.
[23] "Fake Profiles On Fakebook/Facebook!". Pc1news.com. 07.08.2010.
[24] "Victim of fake Facebook profile wins thousands in damages", International Herald Tribune]. 13.08.2010.
[25] Pro-anorexia site clampdown urged". BBC News. 30.04.2010.
[26] "Firms withdraw BNP Facebook ads". BBC News. 30.04.2010.
[27] "Facebook won't ban Holocaust denial groups." JTA. 10.05.2009.
[28] http://tr.euronews.net/tag/londra-ayaklanmasi/
[29] http://www.sabah.com.tr/Gundem/2010/11/22/gizli_servislerin_yeni_silahi_siber_saldiri
[30] http://en.wikipedia.org/wiki/Stuxnet#Speculations_about_the_target_and_origin
[31] http://en.wikipedia.org/wiki/WikiLeaks
[32] http://www.ntvmsnbc.com/id/25142902/
[33] http://www.bilgiguvenligi.gov.tr


**İlkay ÜNAL** 1999 yılında ODTÜ Elektrik-Elektronik Mühendisliği bölümünden mezun olmuştur. Sırasıyla Aselsan, Hürriyet ve Mikes firmalarında yazılım mühendisi olarak çalıştıktan sonra 2006 yılında STM firmasında çalışmaya başlamıştır. 2010 yılında ODTÜ Enformatik Enstitüsü Yazılım Yönetimi yüksek lisans programını tamamlayan İlkay Ünal, SSM'de danışman olarak görevine devam etmektedir.

# SİBER SAVAŞ, TEHDİTLER VE ÇÖZÜM ÖNERİLERİ

A.ÖZBİLEN, İ.ÇOLAK, S.SAĞIROĞLU

***Özet*—Konvansiyonel kinetik savaşların aksine siber savaşların kapsamları ve prensipleri henüz tam olarak belirlenmiş değildir. Siber savaşlar ülkenin sadece bilgi varlıklarını değil, tıpkı klasik savaşlarda olduğu gibi ekonomisini, fiziki tesislerini ve insanların can emniyetini de tehdit etmektedir. Türkiye'de ve dünyada muhtemel bir siber savaşa karşı, ilgili işletme, kurum ve kuruluşların görev ve sorumluluklarının tanımlanmasına ihtiyaç vardır. Bu çalışmada, siber savaşın unsurları ve kapsamı, internet servis sağlayıcıların ve internet değişim noktaların rolü üzerine tespit ve değerlendirmelerde bulunulmuştur.**

**Anahtar Kelimeler— Botnet, Siber savaş, DDOS, Internet Değişim Noktaları, Zombi**

***Abstract*—In contradistinction to conventional kinetic warfare, principles and scope of cyber warfares have not been specified yet. Not only information assets but also economy, physical infrastructe and security of human life are threatened by cyber warfare. In Turkey as in the world, mission and responsibility of responsible agencies/organisations/institutions are required to be redefined in the concept of cyber warfare. In this work, elements and scope of cyber warfare, and the role of internet service providers and internet exchange points are determined and evaluated.**

***Index Terms*— Botnet, Cyber Warfare, DDOS, Internet Exchange Points, Zombie**

## I. GİRİŞ

Siber güvenlik ve siber saldırı kavramları birkaç açıdan değerlendirilmekte ve tartışılmaktadır. Bu tartışmalardan ilki, siber saldırının kapsamının ve pratik neticelerinin neler olacağı etrafında şekillenmektedir. Konu etrafındaki diğer temel bir tartışma ise siber saldırıların, klasik fiziki saldırılar gibi önceden tedbir alınması gereken ve üzerinde gerçekten emek harcamaya değer bir konu olup olmadığıdır.

Özellikle son 10 yıl içerisinde gerçekleşen bazı güvenlik vakaları, siber güvenliğinin fiziki güvenlik kadar öneme sahip olduğunu göstermesi bakımından dikkate değerdir. Bir şehir veya ülke genelinde hizmet veren ve işletme altyapısı kısmen veya tamamen bilgi ve iletişim sistemlerine dayanan tesisler ele alındığında, siber saldırı neticesinde ortaya çıkabilecek ekonomik ve sosyal hasarın fiziki saldırılardan çok daha büyük olabileceği değerlendirilmektedir. Örneğin, bir şehir bünyesindeki faaliyet gösteren su iletim ve dağıtım altyapısının yönetim sistemine yönelik siber bir saldırı tüm şehri etkileyebilecekken, fiziki sabotajların genellikle kısmı ektiler taşıyacağı söylenebilir. Benzer biçimde bir havalimanının uçak-kule haberleşmesine yönelik yanıltma saldırısı, tek bir uçağın fiziki olarak ele geçirilmesinden vahim neticelere sebebiyet verebilecektir. Nitekim 2011 Mayıs ayında yaşanan ve çeşitli haberlere konu olan İstanbul Atatürk Havalimanındaki korsan telsiz vakası [1] her ne kadar felaketle sonuçlanmadıysa da, bu tür sistemlerdeki açıklıkların nasıl suiistimal edilebileceği konusunda fikir vermesi bakımından önem arz etmektedir. Benzer biçimde, siber bir saldırının mahsulü olmasa da ülkemizde 03 Haziran 2011 tarihinde yaşanan EFT problemi [2] ekonomine çok geniş kesimlerce hissedilmesine ve sıkıntılar yaşanmasına sebebiyet vermiştir. Bu vakadan çıkarılması gereken sonuçlardan biri de, ülkenin siber varlıkların ülke ekonomisine ve vatandaşlarının refahını geniş ölçüde etkileyebileceğidir.

A.Özbilen, Bilgi Teknolojileri ve İletişim Kurumu, Ankara, Türkiye (aozbilen@btk.gov.tr)
Prof. Dr. İ. Çolak, Gazi Ünv. Teknoloji Fakültesi Elektrik-Elektronik Mühendisliği Bölümü, Ankara, Türkiye (icolak@gazi.edu.tr)
Prof. Dr. Ş. Sağıroğlu, Gazi Ünv. Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, Ankara, Türkiye (ss@gazi.edu.tr)

## II. SİBER SAVAŞIN KAPSAMI

Bir şirketin nispeten az sayıdaki müşteri kitlesini etkileyecek veritabanına yönelik olarak yapılan saldırının "siber savaş" olarak nitelendirilebilmesi için, bir sokak kavgasının veya lokal bir asayiş olayının da savaş olarak nitelendirilmesi gerekir. Peki siber savaşın ne olduğunu yahut kapsamını ne belirler?

Klasik, kinetik savaşın prensipleri bin yılları bulan tecrübeler neticesinde Sun Tzu, Clausewitz, Jomini, Liddel-Hart ve diğer takip eden teorisyenler tarafından belgelendirilmiş durumdadır. Kinetik savaşa ait belirlenen bu prensiplerin bir kısmı siber savaş için geçerli olsa da bir kısım prensipler anlam taşımamaktadır [3].

Klasik kinetik savaşlar ile siber savaşların kapsam açısından kesiştikleri ve ayrıştıkları noktalar muhakkak ki olacaktır. Örneğin, her iki savaş türünde de başarılı ve etkin olmak için Sun Tzu'nun [4] tarif ettiği planlama, strateji, taktik ve taktik değiştirme, istihbarat, tahrip etme, kaynakların kullanımı gibi unsurlar yer almaktadır. Bazı kavramlar ise, birbiriyle birebir örtüşmemekle birlikte benzerlikler kurmaya müsaittir. Örneğin, arazi faktörü kavramı siber alan için sistemin boyutu, hat kapasitesi gibi kavramlara karşılık gelebilir. Benzer biçimde hasmın imkan ve kabiliyetleri arasında, güvenlik duvarlarının varlığı ve yapılandırılma biçimleri, saldırı tespit sistemleri vb. gibi unsurlar değerlendirilebilir. Ancak, havanın

durumu gibi birebir ilgi kurulamayacak şartlardan da bahsetmek gerekir.
Siber savaş, en genel haliyle bir ülkenin tüm bilgi ve iletişim altyapısını kapsayan bir alanda gerçekleşebilir. Ancak daha az imkan ve istihbaratla saldırma imkanı olduğundan, internete doğrudan bağlı bilgisayar ağları ve sistemlerinin hedef seçilmesi daha muhtemel görülmektedir.
Siber bir savaşın verebileceği zararlar, tıpkı klasik savaşlarda olduğu gibi ülkenin fiziki tesislerini, ekonomiyi ve hatta insanların can emniyetini kapsayacaktır. Bu itibarla siber savaşın, tıpkı yerel bir asayiş olayı gibi adi bir vaka sayılabilecek bir şirketin web sayfası saldırmaktan ibaret olmadığı, ülke ekonomisini ve vatandaşlarını etkileyecek ölçekte saldırılar dizisi şeklinde tanımlanabileceği değerlendirilmektedir.

## III. SİBER SAVAŞIN NEDENLERİ

Siber bir saldırı, fiziki bir saldırı veya savaşta için geçerli farklı neden ve motivasyonlarla bağlı olarak gerçekleştirilebilir.

Teknik araçlarla yapılabilecek incelemeler, bize sadece bir saldırının trafiğe dayalı analizi sunabilmektedir. Örneğin, bir saldırı tespit sistemi marifetiyle, yapılan saldırının türünü anlamak mümkündür. Ancak bu bulgular bize saldırının hangi nedenle yapıldığı bilgisini vermez. Zira bir saldırı, sosyal, politik, ekonomik veya kültürel bir çatışmadan kaynaklı bir motivasyonla yapılıyor olabilir [5]. Örneğin bir gaz veya elektrik dağıtım sistemine yapılacak saldırı kapsamlı bir sosyal mühendislik ve beraberinde ciddi bir politik motivasyon gerektirir. Bu yönüyle siber savaş, fiziki savaşta göze alınabilecek güçlü politik bir çatışmanın ürünü olabilir [6].

Sonuç olarak, siber savaş, tıpkı fiziki savaşta olduğu gibi hasma doğrudan zarar verme veya onu bir imkanından mahrum bırakarak ekonomik veya sosyal açıdan ona zarar verme ve böylece karşısındakini bir şeye zorlamak gibi bir nedenden ötürü yapılabilecektir.

## IV. KRİTİK ALTYAPILARA SİBER SALDIRI

Siber saldırı denildiğinde ilk olarak web sunucularına yönelik olarak gerçekleştirilen hizmeti durdurma (Denial of Service) veya indeks sayfasını değiştirme gibi psikolojik etkisi güçlü ancak bıraktığı tahribat nispeten az olan saldırlar hatıra gelmektedir. Ancak gerçekte korkulması gereken saldırlar çoğunlukla bu türden olanlar değildir

Amerika Birleşik Devletleri USA PATRIOT ACT 2001 göre, hasar görmesi veya etkisizleştirilmesi halinde ulusal halk sağlığını, güvenliği, ekonomik güvenliği veya tümünü olumsuz etkileyecek fiziki veya sanal tüm varlık ve sistemler kritik altyapı sistemleri olarak tanımlanmıştır [7]. Benzer şekilde, Avrupa Birliği (AB) Meclisine sunulan "Terörist Saldırılara Karşı Kritik Altyapıların Korunması" başlıklı 2004 yılı tebliğinde kritik altyapılar, kesilmesi veya hasar görmesi halinde vatandaşların güvenliğini, sağlığı ve ekonomik refahı üzerinde veya üye hükümetlerin etkin ve verimli işleyişi üzerinde ciddi olumsuz etkiler oluşturacak fiziki ve bilgi teknolojileri tesisleri, hizmetleri ve varlıkları olarak tanımlanmıştır [8],[ 9]. Bu tanımlardan yola çıkılarak belirli bir bölge veya ülke genelinde hizmet veren su, elektrik, gaz iletim-dağıtım altyapıları gibi fiziki tesislerden bankaların ve kamunun sunduğu çevrimiçi hizmetlere kadar çok geniş yelpazede hizmet veren fiziki varlıklar ve bilgisayar sistemleri kritik altyapı olarak sınıflandırılmaktadır.

Ülke veya bir şehir ölçeğinde hizmet veren fiziki altyapılar, verilen hizmetin gereği dağıtık bir yapıda olan ve birçok farklı bileşeni içeren tesislerdir. İlk bakışta bu tür altyapılar siber saldırılara karşı çok daha sağlam ve dayanıklı görünseler de yapılacak sosyal mühendislik çalışmaları ile haklarında bilgi toplandığında, saldırılara karşı daha az dayanıklı oldukları görülecektir [10]. Zira bu tür altyapılar çoğunlukla, web, e-posta sunucularının önlerinde veya üzerlerinde bulunan güvenlik duvarı, saldırı tespit sistemi gibi güvenlik mekanizmalarına sahip değildirler.

Muhtemel neticeleri itibariyle kıyaslandığında, fiziki kritik altyapılara yönelik saldırıların yol açacağı sosyal ve ekonomik zararın birçok web tabanlı servisin kesintiye uğramasından daha büyük ölçüde olacağı değerlendirilmektedir.

## V. WEB HİZMETLERİNE YÖNELİK SİBER SALDIRILAR VE ZOMBİ BİLGİSAYARLAR

İnternete bağlı her bilgisayar, aynı anda dünyanın herhangi bir noktasında yer alan diğer bir bilgisayara erişebilir durumdadır. Başka bir ifadeyle, internete bağlı herhangi iki bilgisayar birbiriyle iletişime girebileceği gibi birbirine saldırabilecek duruma da sahiptirler.

Web, e-posta sunucu gibi siber varlıklara ait IP adresi bilgisinin ziyaretçiler tarafından çoğu zaman tek bir komut çalıştırmaya bile gerek kalmaksızın öğrenilebilmesi ve internette indirilen araçlar veya kiralanan zombi bilgisayarlar ile kolayca saldırı düzenlenebilmesinin mümkün olabilmektedir.

Kamu hizmeti veren web servislerine yönelik saldırılar ciddi ekonomik ve sosyal zararlara sebebiyet verebilirler. Bu tür saldırılara karşı olarak sadece bir kurum bünyesinde alınabilecek tedbirler yeterli olmayacağı gibi saldırının türüne bağlı olarak elverişli de olamayabilirler. Özellikle, dağıtık hizmet durdurma saldırıları (Distributed Denial of Service ) için, saldırılacak sunucunun önündeki güvenlik unsurlarından çok sunucunun sahip olduğu hat ve donanım kapasiteleri önem ifade etmektedir.

Hizmet kesme saldırılarının çoğunlukla zombi olarak nitelendirilen ve çoğu bilgisayarının ele geçirildiğinden habersiz masum kullanıcıların bilgisayarından yapıldığı bilinmektedir. Örneğin Haziran 2011'de ülkemizde hizmet veren muhtelif kamu web sitelerine yönelik olarak saldırılarda da zombi bilgisayarlar kullanılmıştır [11] . Anonim grubu, diğer benzer saldırılardan farklı olarak "kendi yurtiçi ve

yurtdışı destekçilerinin gönüllü olarak indirdiği ve kurduğu programlar vasıtasıyla bu saldırıları gerçekleştirdiklerini" iddia etmektedir. Ancak bu iddia doğru kabul edilse dahi, bir şekilde saldırı programını gönüllü olarak kuran kullanıcılar, kendi bilgisayarının başkalarının emrine sunmuş bulunmaktadırlar [12]. Bu andan itibaren başlangıçta gönüllülük olsa dahi gönüllüler sonraki eylemlerinin türü, hedefi ve kapsamına katılmasalar bile eyleme iştirak etmek durumunda kalmaktadırlar. Bu durumda başlangıçta hangi saik ile bu programı kurmuş olurlarsa olsunlar, neticesinde doğabilecek hukuki ve cezai sorumluluktan kurtulmak kullanıcılar açısından mümkün olmamaktadır. Benzer saldırılarda bilgisayarı iradesi dışında başkalarının hizmetine geçen kullanıcıların durumu ise ne yazık ki daha karmaşık bir hal almaktadır. Zira, böyle bir duruma isteyerek mi yoksa istemeden mi geçtiklerinin tespitinin inceleme yapılmadan anlaşılması çoğu durumda mümkün görünmemektedir.

Bugün artık zombi bilgisayarlardan oluşan ve botnet olarak adlandırılan saldırı ağları, birileri tarafından çeşitli kötücül yazılımlar kullanılarak oluşturulmaktadır. Oluşturulan bu ağlar sonrasında, başta DDOS saldırılarında ve spam e-posta gönderiminde kullanılmak üzere kiralanmakta veya satılmaktadır [13]. İnternet ortamında, belirli bir şirketin veya kurumun web servislerini 24 saatliğine ulaşılamaz hale getirmek üzere botnet kiralama bedeli, hedef sitenin korunma gücüne bağlı olarak 50 dolar ile birkaç bin dolar arasında değişmektedir. Shadowserver tarafından verilen bilgilere göre sadece 2008 yılı içinde 190 000 DDOS saldırısı gerçekleştirilmiş ve bu yıl için oluşan botnet ticaret hacmi 20 milyon dolar seviyesine ulaşmıştır [14].

Botnet oluşumu sırasında kullanılan kötücül yazılımın hangi vasıtalarla yayıldığına bağlı olarak belirli bir bot ağına takılan bilgisayarın çoğunlukla belirli bir ülkeden olmasını beklemek mümkün görünebilir. Ancak bir takım özel bot ağları bir yana bırakılırsa, büyük bot ağlarında tüm ülkelerden kurban bilgisayarların olması olası bir sonuçtur. Bu yönüyle, bir ülkedeki internet kullanıcılarının dünya genelindeki toplam kullanıcı sayısına nispetince zombi bilgisayarı olabileceği beklenebilir. Dolayısıyla, sayı itibariyle yurtdışı bağlantılardan gelecek saldırılarından ülke içinden gelebilecek saldırılara oranla çok yüksek olacağı varsayımı birçok durum için yapılabilir.

## VI. ZOMBİLER ÜZERİNDEN SİBER SAVAŞ VE İNTERNET DEĞİŞİM NOKTALARI

Ülkeler arası bir siber savaş, özellikle oluşturacağı ekonomik ve sosyal neticeler bakımından konvansiyonel kinetik savaşları aratmayacak sonuçların ve maliyetlerin meydana gelmesine sebebiyet verebilir. Bu bakımdan, taraflardan hangisinin özel anlamda interneti genel anlamda ise bilişim ve iletişim teknolojileri ekonomik ve kamusal altyapılarında daha çok kullanıyorsa böyle bir savaştan daha fazla etkilenebileceği söylenebilir. Ancak saldırıyı bertaraf etmenin yolu da muhakkak ki teknik imkanlarının ve kapasitenin iyi yönetilmesiyle mümkün olacaktır.

2007 Mayıs ve Temmuz aylarında Estonya 'ya ve 2008 Haziran ayında Gürcistan'a yönelik siber saldırılar bir çok kesimce siber savaş olarak nitelendirilmiştir. Her iki ülkenin bu saldırılar karşısında durumunun incelenmesi, benzer çapta bir saldırının örneğin Türkiye'ye de yönelmesi öncesinde neler yapılabileceğinin tespiti açısından önem taşınmaktadır.

Estonya örneği incelendiğinde karşılaşılan saldırıya sadece web servislerin önünde alınacak güvenlik tedbirleriyle karşı konulamayacağı açıkça görülmektedir. Zira, Estonya saldırıya uğradığı tarih itibariyle, dünyada sayıları toplamda 300'ü aşan ve genellikle gelişmiş ülkelerde bulunan İnternet Değişim Noktalarının (IXP: Internet Exchange Point) herhangi birine ülke içinde sahip olmadığından ve bu nedenle kendi İnternet Servis Sağlayıcıları arasında dönmesi gereken iç internet trafiğini dahi yurtdışı internet değişim noktaları üzerinden gerçekleştirmesi nedeniyle uğradığı siber saldırı karşısındaki zafiyete uğramıştır [15].

## VII. SİBER SUÇLARLA MÜCADELE VE TÜRKİYE'DE SİBER GÜVENLİK TATBİKATLARI

Toplam 43 ülkenin imzaladığı *Avrupa Konseyi Siber Suçlar Sözleşmesi'ni* Türkiye de Kasım 2010 tarihi itibariyle imzalamış bulunmaktadır. Sözleşmede, bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve kullanıma açık bulunmasına yönelik suçlar, "Yasadışı erişim, yasadışı müdahale, verilere müdahale, sistemlere müdahale, cihazların kötüye kullanımı" olarak sıralanmaktadır [16].

Her ne kadar siber suçlara yönelik uluslararası böyle bir sözleşme imza altına alınsa ve beraberinde işbirliği meydana gelecek olsa da burada bir savaş durumuna yönelik maddeler bulunmamaktadır. Dolayısıyla bu sözleşme siber savaşın engellemesi açısından çok anlam ifade etmemekte olup sadece fert veya toplulukların işleyeceği siber suçlarla ilgili bir sözleşmedir. Bu haliyle, özellikle yurtdışı bir kaynaktan ferdi veya dar bir toplulukça yapılan siber suçlarla mücadele katkı sağlayacak olsa da bu sözleşmeyi imzalamış veya imzalamamış ülkeler arasında çıkabilecek siber bir savaşı engelleme veya politik bir saldırı tespit etme yönünden başarı sağlanabileceği mümkün görünmemektedir.

Ülkemizde şu ana kadar *BOME 2008* ve *USGT 2011* gibi siber savaş ve savunmaya yönelik olarak iki ayrı tatbikat gerçekleştirilirken Dünyada da, *Dark Screen, CyberStorm, Cyber Europe, APCERT Drill* ve *NATO Cyber Coalition* gibi çeşitli siber tatbikatlar gerçekleştirilmiştir [17], [18].

Ulusal Siber Güvenlik Tatbikatı 2011'e, enerji, finans, telekom, savunma, sağlık ve sosyal güvenlik gibi alanlarda faaliyet gösteren 41 kamu ve özel sektör kurum ve kuruluşun katılımıyla gerçek saldırı benzeri saldırılar ve yazılı senaryoların değerlendirilmesi gerçekleştirilmiştir [18]. Bu tür tatbikatların muhakkak ki siber güvenlik farkındalığının ve bilicinin, başta katılımcı kurum kuruluşlar olmak üzere tüm ülke genelinde oluşmasına ve gelişmesine katkısı olacaktır.

Ancak önümüzdeki yıllarda devam edecek bu tür tatbikatlarda, sadece web türü servislerin değil kritik fiziki altyapıların otomasyonu dahil her türlü sistemin dikkate alındığı ve her kurum/ kuruluşun kendi İnternet Servis Sağlayıcısıyla birlikte rol aldığı ortak çalışmaların da yapılmasının gerekli olduğu değerlendirilmektedir.

## VIII. SONUÇ VE ÖNERİLER

Bin yıllardır yapılmakta olan konvansiyonel kinetik savaşlara ilişkin savunma ve saldırı prensipleri tanımlanmış durumdadır. Öte yandan, siber savaş konsepti, tanım, kapsam ve genel prensipleri itibariyle henüz tam olarak şekillenmemiş ve üzerinde fazlaca tartışmaya muhtaç bir şekilde beklemektedir. Bu çalışmada, bu tartışmalara katkı sağlamak maksadıyla siber savaşların unsurları ve kapsamı üzerine bazı değerlendirmelerde bulunulmuştur. Bu değerlendirmeler maddeler halinde sunulmuştur.

1. Dar ölçekli ve çoğunlukla ticari nedenlerle şirketler arasında meydana gelen siber saldırılardan farklı olarak, 2007 Estonya ve 2008 Gürcistan'da yaşanan siber saldırı vakaları kimi araştırmacı ve uzmanlarca bir çeşit siber savaş olarak değerlendirilmiştir. Bu nedenle anılan her iki ülkede de yaşanan vakaları ve bu vakaların yaşanmasına sebebiyet veren açıklık ve zafiyetlerin neler olduğunun anlaşılması ve irdelenmesi oldukça önem arz etmektedir.

2. Günümüzde birçok bilgi varlığı, ekonomik ve sosyal açıdan birçok fiziki varlıktan daha değerli duruma gelmiştir. Bu yönüyle, bir ülkenin bilgi varlıklarına veya fiziki tesislerinin yönetiminde kullandıkları bilgi ve iletişim altyapılarına yönelik siber saldırılar sonuçları itibariyle fiziki saldırılardan daha yıkıcı ve vahim gelişmelere neden olabilmesi muhtemeldir.

3. Siber savaşların, boyutları ve sonuçları itibariyle çeşitli şirket, kurum veya kuruluşları hedef alan küçük çapta ve yerel saldırılardan farklı olarak ele alınması gerekir. Zira politik motivasyonlu bir savaşta, kamu hizmeti veren kurum ve kuruluşların tek başlarına saldırıya karşı koyabilme imkanları sınırlı olacaktır. Bu noktada, gerçekleşebilecek bir siber savaşa karşı, kimlerin hangi rolü üstleneceğinin pozisyonlarına, imkan ve kabiliyetlerine göre önceden tayini gerekecektir. Örneğin, internet servis sağlayıcıların üstleneceği rol ile içerik sağlayıcıların yükleneceği rolün farklı olması ve bu farka göre sorumluklarının tanımlanması gerekecektir. Bu anlamda, Türkiye özelinde, siber savaş öncesinde rol ve sorumlulukların tanımlanması önem arz etmektedir.

4. Ülkemizde, bankacılık ve altyapı hizmetleri de dahil olmak üzere kamuya hizmet veren kurum ve kuruluşların tümünü kapsayacak bir siber savunma planının hazırlanmasına ihtiyaç duyulmaktadır. Bu kapsamda, ilgili her kurum ve kuruluşun kendi bilgi varlıklarına ve tesislerine yönelik risk analizini yapması ve kendi karşı koyma yöntemlerini belirlemesi gerekir. Risk analizi ve karşı koyma yöntemlerinin belirlenmesi süreçlerinde, bu iş için ihtisaslaşmış bir kamu merkezinin kurulması be bu merkezden destek almaları kurum ve kuruluşlar bazında yapılacak çalışmalarının başarı oranını yükselteceği değerlendirilmektedir. Zira kamusal hizmet veren işletme ve kuruluşların büyük bir çoğunluğunun kendi ihtisasları dışındaki böyle bir alanda tek başlarına etkin bir savunma yöntemi geliştirememeleri beklenmedik bir durum olmayacaktır. Bu itibarla, ilgili kurum ve kuruluşlara destek verecek bir siber savunma koordinasyon merkezinin varlığı olabilecek bir saldırıya karşı koyma başarını ve toplam savunma kabiliyetini attıracaktır.

5. Siber savunma için ulusal eylem planının hazırlanması ve bu planının belirli periyotlarla gözden geçirilerek geliştirilmesine ve oluşturulacak siber savunma koordinasyon merkezinin ilgili kurum ve kuruluşlarının bu plana uygun davranıp davranmadıklarının denetlenmesiyle siber savunma hattının iç cephelerinin oluşmasını sağlayacağı değerlendirilmektedir.

6. Kurum ve kuruluşlar seviyesinde, kullanılan yazılımların, işletim sistemlerinin güvenliği kadar güvenlik duvarı, saldırı tespit sistemi gibi güvenlik bileşenlerinin güvenilebilir ve takip edilebilir olmaları da ayrıca önem teşkil etmektedir. Özellikle milli olmayan güvenlik yazılımı ve donanımlarının bir siber savaş durumunda, savaşın taraflarına bağlı olarak olağandışı bir pozisyon alması etik olmasa da tamamen ihtimal dışı bir durum değildir. Bu nedenle tıpkı milli tank, helikopter vb. konvansiyonel savaş araçlarında olduğu gibi siber savaşın müdafaa unsurlarından güvenlik duvarı, saldırı tespit sistemi gibi sistemlerinde yerli üretim için ilave teşvik programlarının uygulanmasına ihtiyaç olduğu değerlendirilmektedir.

7. Ülke siber hattının dış cephe savunmasında rol sahibi olan işletmeler internet servis sağlayıcılarıdır. Bu yönüyle ISS'lerin ülke siber savunmasında farklı ve özel bir rolü olduğu muhakkaktır. Özelikle, Türkiye'de birkaç çok başarılı olmayan girişim olsa da Batı Avrupa ülkeleri ve Amerika Birleşik Devletlerinde olduğu gibi ülke içi ISS trafiğinin değiştirildiği bir internet değişim noktasının (IXP) Türkiye içinde hala mevcut olmaması dış siber savunma cephesi kurulmasının önündeki en büyük engel olarak görülmelidir. Bugün itibariyle Türkiye'de, pazarın serbestleşmesi ve rekabete açılması açısından olumsuz bir tablo olarak nitelendirilse de siber savunma açısından internet trafiğinin büyük bir çoğunluğunun hala tek bir işletmede olması şans olarak değerlendirilebilir.

Ancak başta mobil internet kullanıcıları ve alternatif genişbant abonelerinin trafik miktarlarının artmasıyla birlikte, nüfusu birkaç milyonun üzerinde olan tüm şehirlerde IXP kurulması ülkenin siber savunması açısında büyük önem taşımaktadır. Estonya örneğinde olduğu gibi Türkiye'deki ISS'lerin maliyet ve rekabet gibi nedenlerle yurtdışı değişim noktaları üzerinden arabağlantı yapmaları Türkiye açısından kaynak israfına ve maddi kayıplara yol açacağı gibi dış siber savunma hattının da kurulamamasına sebebiyet verecektir. Bu nedenle, Türkiye içindeki birkaç milyon nüfusa sahip tüm şehirlerde IXP kurulması, mevcut kurulum girişimlerin desteklenmesi ve yurtiçi internet trafiğinin yurtdışı IXP noktalarından değişimine izin verilmemesi ülke siber güvenliğinin en önemli halkasını teşkil edecektir.

8. Yurtdışı internet giriş ve çıkışlarının topolojik olarak belirli noktalarda tutulması, kurulması önerilen siber savunma koordinasyon merkezine bu noktalara ait güncel bilgilerinin devamlı ulaştırılması, kritik kurum ve kuruluşlara yapılabilecek yurtdışı menşei botnet saldırılara karşı hedef ve kaynak bazında filtrelerin hazır bulundurulması, özellikle yurtdışı botnetlerden gelecek DDOS saldırıları için etkin bir dış savunma hattı oluşturulmasına imkan sağlaması bakınından önemlidir. İnternet için yurtiçi- yurtdışı trafik ayrımı yapmak genel anlamda tartışmalı bir yaklaşım olarak görülebilir. Zira bir internet servisi sadece Türk vatandaşlarına yönelik olarak verilse dahi yurtdışındaki Türk vatandaşlarının da bu servislere ulaşabilmesini temin etmek gerekecektir. Ancak, belirli sürelerde yapılacak yoğun botnet saldırıları için internet trafiğini yurtdışı ve yurtiçi olarak ayrıma tabi tutmak ve yurtdışından saldırıya uğrayan sistemlere gelen talebi yine belirli ve nispeten kısa bir zaman aralığı için kesmek, yaratabileceği istisnai bazı problemler dışında, servislerin tamamen durmasını engellemesi bakımından ciddi faydalar getireceği mütalaa edilmektedir. Bu bağlamda, böyle bir dış siber savunma hattının kurulabilmesi için önerilen siber savunma koordinasyon merkezinin tüm ISS'lerin yurtdışı giriş çıkış trafiklerinin yönetildiği operasyon merkezleriyle irtibatlı olması ve yasal düzenlemelerle siber saldırı ve savaş hallerinde filtre talep edebilme hakkına sahip olmalarına ihtiyaç vardır.

9. Siber saldırı denildiğinde akla ilk olarak web tabanlı servislere yönelik saldırılar gelmektedir. Ancak ilerde doğabilecek bir siber savaşın boyutlarının sadece internete açık web servisleri olarak varsaymak savunma konseptinin yanlış kurgulanmasına sebebiyet verebilir. Bu itibarla, ülke içinde hizmet veren su, elektrik, havalimanları, gaz iletim ve dağıtım tesisleri de olmak üzere her türlü kritik fiziki altyapıyı da kapsayan bir siber savunma hattının ve anlayışının geliştirilmesi gerekmektedir. Otomasyon sistemlerinin gelişmesi ve giderek IP protokolünün haberleşme platformu olarak kullanılmaya başlanması ile siber saldırılara maruz kalma riskleri de artacaktır.

10. Alan Adı Sunucuları (DNS), kullanıcıların neye nereden bağlanacağını söyleyen yol rehberleri olduğundan siber savaş ve savunma açısından özel öneme sahiptirler. Genel anlamda ülke içindeki tüm DNS sunucularının ve özellikle ISS'lere ait olan geniş kullanıcı kesimlerince kullanılan DNS'lerin güvenliği internet kullanıcılarının güvenliğiyle neredeyse eşdeğer bir konumdadır. DNS konusu bu yönüyle ele alındığında, ISS'lere ait DNS sunucularının gerekirse önerilen siber savunma koordinasyon merkezince denetlenmesi, belirli bir güvenlik standardına bağlanması ve hatta sertifikalandırılmasıyla internet kullanıcılarının güvenliğini arttırıcı önemli tedbirler arasında sayılabilir.

11. Farklı nedenlere yurtiçindeki kullanıcılarının bir bölümünün yurtdışı DNS'leri kullanması ve arama motorlarının kullanım pratikliği gibi nedenlerle artık URL yazmamak içinde kullanılmaya başlanması, siber savaş durumunda kullanıcıların adres çözümleme güvenliğini riski sokan durumlar arasındadır. Bu konularda yapılabileceklerin doğrudan son kullanıcıya bağımlı olması nedeniyle çok daha uzun vadeli ve problemli görünmektedir.

## IX. KAYNAKLAR

[1] "Uçaklara korsan telsiz oyunu", http://gundem.milliyet.com.tr/ucaklara-korsan-telsiz-oyunu/gundem/gundemdetay/08.06.2011/1399782/default.htm , (Erişim 06 Ağustos 2011)
[2] "Merkez Bankası EFT Sistemi Yazılım Güncellemesi Sırasında Çöktü", http://www.turk.internet.com/portal/yazigoster.php?yaziid=32659 (Erişim 07 Ağustos 2011)
[3] R. C. Parks, D. P. Duggan, "Principles of Cyber-warfare", Proceedings of the 2001 IEEE, Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 5-6 June, 2001
[4] Sun Tzu, "Savaş Sanatı", Anahtar Kitaplar Yayınevi, Eylül 2001
[5] R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Qiuming Zhu; P. Laplante, ,"Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political", IEEE Technology and Society Magazine, Volume: 30 Issue:1, On page(s): 28 - 38, Spring 2011
[6] A. Özbilen, "Fiziki Altyapı Ve Endüstriyel Tesisler İçin Siber Güvenlik", http://ceng.gazi.edu.tr/secure/yazilardetay.aspx?yaziid=6 (Erişim 07 Ağustos 2011)
[7] USA Homeland Security, "Critical Infrastructure Identification, Prioritization, and Protection, Homeland

Security Presidential Directive 7", December 17 2003, www.dhs.gov/xabout/laws/gc_1214597989952.shtm (Erişim 03 Ağustos 2009)
[8] "Critical Infrastructure Protection in The Fight Against Terrorism", Commission Of The European Communities COM(2004) 702 Final, Brussels, October 10 2004, eur-lex.europa.eu/LexUriServ/LexUriServ.do (Erişim 03 Ağustos 2009 )
[9] "Communication From The Commission on a European Programme for Critical Infrastructure Protection 786 Final", COMMISSION OF THE EUROPEAN COMMUNITIES, Brussels, December 12 2006, eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf (Erişim 03 Ağustos 2009)
[10] James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", Center for Strategic and International Studies, December 2002
[11] "Anonymous Adalet Bakanlığı'na saldırdı, 'Zombi' uyarısı geldi", http://www.hurriyet.com.tr/ekonomi/18033225.asp , (Erişim 07 Ağustos 2011)
[12] 'Anonymous sizi de yakabilir', http://www.dha.com.tr/anonymous-sizi-de-yakabilir-son-dakika-haberi_174617.html (Erişim 07 Ağustos 2011)
[13] Z. Li, Q Liao, A. Striegel, "Botnet Economics: Uncertainty Matters", Managing Information Risk and the Economics of Security, 2009, 245-267, DOI: 10.1007/978-0-387-09762-6_12
[14] Y. Namestnikov, "The economics of Botnets", Kaspersky Lab. http://www.securelist.com/en/analysis/204792068/The_economics_of_Botnets (Erişim 02 Ağustos 2011)
[15] R. Stapleton-Gray, W. Woodcock, "National Internet Defense—Small States on the Skirmish Line", Communications of the acm vol. 54 no. 3, 2011
[16] "Nihayet Türkiye'de Sanal Suçlar Sözleşmesi'ni İmzaladı", http://www.bilisimdergisi.org/s127/pdf/10-13.pdf (Erişim 02 Ağustos 2011)
[17] Ünal TATAR "Dünyada ve Türkiye'de Siber Güvenlik Tatbikatları", Ankara, Haziran 2011, http://www.bilgiguvenligi.gov.tr/dokuman-yukle/6.-kamu-kurumlari-bilgi-teknolojileri-guv.-konf./unal-tatar-tatbikatlar/download.html (Erişim 08 Ağustos 2011)
[18] "Basın Bülteni : Ulusal Siber Güvenlik Tatbikatı 25-28 Ocak 2011 tarihlerinde gerçekleştiriliyor, Ankara, 25.01.2011 http://www.btk.gov.tr/eski/Basin_Duyurular/Bulten/2011/25012011_siberguvenlik.pdf (Erişim 08 Ağustos 2011)

**A. ÖZBİLEN**
1980 Antakya doğumludur. Gazi Üniversitesi Elektrik-Elektronik Mühendisliğinde lisans ve yüksek lisans eğitimini tamamladı. Gazi Üniversitesi Elektrik Eğitimi A.B.D 'de doktora öğrenimine devam etmektedir. Türk Telekom A.Ş Ankara Bilişim Ağları Müdürlüğü, Türk Telekom A.Ş Genel Müdürlüğü Uluslararası İlişkiler Dairesi Başkanlığında Telekom Uzman Yardımcısı unvanıyla görevler aldı, halen Bilgi Teknolojiler ve İletişim Kurumu'nda uzman olarak görevini sürdürmektedir.
"Denetim Sistemleri ve Kritik Altyapı Güvenliği" üzerine akademik çalışmalarına devam eden yazarın bu konular üzerine çeşitli dergilerde yayınlanmış makaleleri ve konferans bildirileri bulunmaktadır.