Ulusal Siber Güvenliğin Sağlanmasında NATO'nun Olumlu Etkilerinin Artırılması İçin Yaklaşım Modeli

Ü.Bayık, İ.Semiz, S. Sönmez, M.Durak,

***Özet*— NATO 1949 yılında üye ülkelerin, ortak savunma için yeteneklerini geliştirmek, herhangi bir üyenin toprak bütünlüğünün, siyasî bağımsızlığı ve güvenliğinin tehlikede olduğunda bir araya gelmek ve herhangi birine saldırıldığında bu saldırıya hepsine karşı yapılmış bir saldırı olarak kabul ederek ortak hareket etmek maksadıyla kurulmuştur. Günümüzde ülkelere yönelik saldırılar siber uzayda yapılmaktadır. Bu saldırılar devletlerin karşılamayacağı finansal ve fiziksel birçok sonuçlar doğurmaktadır. NATO'da üye ülkelerin siber uzaydaki tecrübe, birikim ve yeteneklerinden etkin bir şekilde faydalanmak için kurumsal olarak bu alanın yönetilmesine yönelik bir model oluşturulmuştur.**

***Terimler*— NATO, Siber savunma, siber güvenlik, Mükemmeliyet Merkezi**

***Abstract*— NATO was established in 1949 in order to develop common security capabilities, to come together and act as a one country in case of any danger in any member states boundary, political sovereignty and security and any attack to one member state. Nowadays attacks are made in cyber space. These attacks cause financial and physical results that countries can not bear themselves. In order to get NATO member states' capabilities and experiences in cyber space, a model is made to manage this space.**

***Key Words*— NATO, Cyber Defense, Cyber Security, Center of Excellence.**

I. GİRİS

BİLISIM teknolojileri, sistemleri ve usullerinin devletlerin kritik alt yapılarına girmesi ile bu altyapıları birbirlerine bağlayan iletişim ortamlarının güvenlikleri stratejik seviyede değerlendirilmesi bir gereklilik haline gelmiştir. Günümüzde akademik ortamda sayısız makale yayınlanmasıyla uluslararası ortamda siber farkındalık üst düzeye çıkmıştır. Askeri unsurların birbirleri ile haberleşmesini kolaylaştırmak maksadıyla ortaya çıkan internet sağladığı faydaların yanında ortaya çıkardığı hassasiyetlerle devletlerin kâbusu haline gelmiştir.

Ülkeler arasındaki konvansiyonel harbin günümüzde ortadan kalkması daha doğru bir ifade ile ülkeler arasında kullanılan enstrümanların değişmesi ile fiziksel dünyanın sınırları genişlemiştir. Bu harp alanının boyutlarının fiziksel dünya ile entegre olan tüm boyutlarının yeniden değerlendirilmesi, her boyutta ortaya çıkabilecek hassasiyetlere tedbirler getirilmesi devletlerinin ulusal güvenliklerinin birinci önceliği haline gelmiştir. Bu maksatla devletler siber güvenliğe yönelik gerek askeri alanda gerekse kamusal alanda teşkilatlanmalara gitmiştir. Ülkemizde ulusal boyutta Ulaştırma, Denizcilik ve Haberleşme Bakanlığının sorumluluğunda yapılanmaya gidilmiştir.

II. ULUSAL SİBER GÜVENLİĞİN DAYANDIĞI PRENSİPLER, TEŞKİLATLANMA SÜRECİ

Ülkemizde siber uzayda yaşanan savaşların (1999 Yılında Kosova Harekâtında NATO Unsurlarına yapılan Siber saldırılar, Estonya-Rusya, Gürcistan-Rusya arasındaki siber savaş) ortaya çıkardığı endişeler, akademisyenlerin, kolluk kuvvetlerinin ve askeri uzmanların bu alandaki çalışmaları ile ulusal bağlamda adımların atılmasını gerektirdiğini ortaya koymuştur. Siber güveliğin dayandığı temel unsurlara bakılacak olursa, Bunlar:

Şekil 1. Siber Güvenliğin Temel Unsurları

- Ulusal politika ve stratejinin geliştirilmesi,
- Yasal çerçevenin oluşturulması,
- Teknik tedbirlerin geliştirilmesi,
- Kurumsal yapılanmanın belirlenmesi,
- Ulusal işbirliği ve koordinasyonun sağlanması,
- Kapasitenin geliştirilmesi,

Ümit Bayık, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: murataltug@gmail.com.

İnan Semiz, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: inansemiz@gmail.com.

Selçuk Sönmez, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: selcoksonmez@gmail.com.

Melih Durak, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: melihdurak@gmail.com.

- Farkındalığın artırılması,
- Uluslararası işbirliği ve uyumun sağlanmasıdır[1].

Belirtilen temel unsurlara yönelik olarak ulusal alanda birçok adımlar atılmıştır. Gerek kamu kurum ve kuruluşlarının gerekse özel sektördeki kuruluşlarının siber güvenliğe yönelik farkındalıkları artırılmıştır. Ulusal ve uluslararası alanda birçok siber tatbikatlara icra edilmiş, özel kurum, kuruluşlar ve kamu kurum, kuruluşları tatbikata katılmıştır. Bu tatbikatlarda özellikle kritik alt yapıların korunmasına yönelik senaryolar denenmiştir. Siber güvenlik yönelik birçok çalışma ve araştırma yapılmış ve yapılmaya devam edilmekle birlikte daha atılacak birçok adım bulunmaktadır. Yapılan çalışmalar aşağıdaki başlıklar altında toplanmaktadır.

- Yasal çalışmalar,
- Ulusal bilgi güvenliği kapısı,
- TR-BOME Bilgisayar Olaylarına Müdahale Ekibi,
- Bilgi Toplumu Stratejisi Eylem Planı (2006 - 2010),
- Kişisel Verilerin Korunması Kanunu Tasarısı,
- Ulusal Sanal Ortam Güvenlik Politikasının oluşturulması,
- Siber Güvenlik Tatbikatları,
- Siber Güvenlik Çalıştay ve Konferansları,
- TSK'nın Yürüttüğü Faaliyetler.

Türkiye'de siber güvenlik kapsamında ele alınacak olan bilgi toplumuna dönüşüm çalışmaları 2000'li yılların başlarında başlamıştır. Ülkemizdeki siber güvenlik tatbikatlarının ilki olan BOME 2008 Tatbikatı TÜBİTAK UEKAE bünyesinde faaliyet gösteren TR-BOME koordinatörlüğünde, 20-21 Kasım 2008 tarihlerinde icra edilmiştir.

Daha geniş katılımlı ikinci tatbikat Ulusal Siber Güvenlik Tatbikatı 2011, TÜBİTAK BİLGEM ve Bilgi Teknolojileri ve İletişim Kurumu (BTK) koordinatörlüğünde Ocak 2011'de düzenlenmiş, 41 kamu ve özel sektör kurum ve kuruluşunun katıldığı tatbikat gerçek saldırılar ve gerçekçi senaryolar denenmiştir. [2]

Ocak 2013'te Ulaştırma, Denizcilik ve Haberleşme Bakanlığı koordinatörlüğünde Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı yayımlanmıştır. Eylem planının temel amacı; Kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan hizmet, işlem ve bunların sunumlarında kullanılan sistemlerin güvenliğinin sağlanması, kritik altyapılara ait bilişim sistemlerinin güvenliklerinin sağlanması olarak belirlenmiştir. Siber güvenliğe ait riskler ortaya konulmuş ve bu risklerin etkin bir risk yönetimi ile ortadan kaldırılması hedeflenmiştir [3].

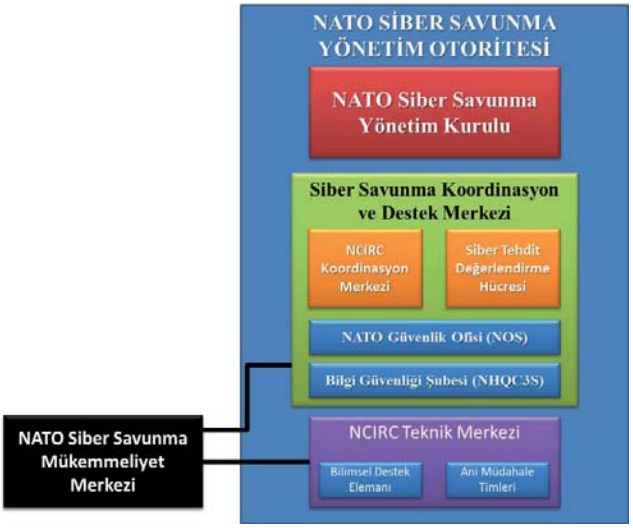
2013-2014 dönemi içerisinde yedi başlık altında hedef belirlenmiştir. Her belirlenen hedef yapbozun parçaları gibi eş güdüm halinde yürütüldüğünde bir anlam ifade etmektedir. Bu hedeflerden; yasal mevzuatın oluşturulması, Ulusal Siber Olaylara Müdahale Merkezi oluşturulması, altyapının güçlendirilmesi, siber güvenlik alanında insan kaynağının yetiştirilmesi öne çıkmaktadır. Tüm belirlenen bu hedefler stratejik seviyede farkındalığın artığını ve operatif seviyede icraya geçildiğinin bir göstergesidir.

III. NATO'NUN SİBER GÜVENLİĞE YÖNELİK ATTIĞI ADIMLAR VE HİZMETLERİ

NATO 1949 yılında üyelerinin savunma yeteneklerini geliştirmek ve doğu bloğuna karşı bir caydırıcılık sağlamak maksadıyla kurulmuştur. 21'inci yüzyılda güvenlik parametreleri soğuk savaştan sonra değişmiş üyelerinin öncelikle enerji güvenlikleri, kritik altyapılarının iletişim alt yapıları ile birbirlerine bağlanması ile bu alt yapıların oluşturduğu siber alanın güvenliği birinci önceliği haline gelmiştir. Bu küresel tehditlere karşı özellikle 2007 yazında Rusya tarafından Estonya'ya yapılan siber saldırılardan sonra yeni savunma stratejileri geliştirilmesi gerektiğinin bir delili olmuştur. Kamu güvenliği ve devletlerin istikrarı karşısındaki giderek büyüyen bu tehdit NATO'nun elektronik iletişime bağımlı üyelerinin siber cephede son derece zayıf olduklarını ortaya çıkarmıştır [4].

NATO Estonya'ya yapılan bu saldırılardan sonra Estonya'da Siber Savunma Mükemmeliyet Merkezi kurmuştur. NATO'nun 2010 stratejik konseptinde Siber Güvenliğe yönelik olarak " … siber saldırılara karşı yeteneğimizi geliştirerek saldırıları tespit etme, koruma ve engelleme alanlarında çalışmalar yapma…" ifadeleri yer almıştır. Bu stratejik vizyonla 8 Haziran 2011 tarihinde NATO Savunma Bakanlarının onayı ile Siber Savunma Politikası yürürlüğe girmiştir [5].

NATO Siber Savunma Teşkilatı, Siber Savunma Yönetim Otoritesine bağlı olarak çalışan Siber Savunma Yönetim Kurulu, Siber Savunma Koordinasyon ve Destek Merkezi ve Bilgisayar Olaylarına Müdahale Yeteneği (NCIRC) Teknik Merkezinden oluşmaktadır. Ayrıca, NATO çapında siber güvenliğe ilişkin farkındalık sağlamak ve standart oluşturmak maksadıyla Estonya'da teşkil edilen Siber Savunma Mükemmeliyet merkezi ile koordineli olarak bu alanda birçok eğitim faaliyeti icra edilmektedir.



Şekil 2. NATO Siber Savunma Yönetim Otoritesi

Bu teşkilatın bağlılarına ilişkin detaylı bilgiler aşağıdadır [6].

A. NATO Siber Savunma Yönetim Sistemi:

NATO çapında siber savunma olaylarının yönetimi ile ilgili tek otoritedir. İhtiyaç olduğunda, süratli ve etkili bir siber savunma için her türlü faaliyetin başlatılması ve koordinasyonun yapılmasından, ittifakın kendisinin veya İttifak üyesi bir ülkenin, siber saldırıya maruz kalması durumunda, talep edilmesi hâlinde yardım sağlanmasından sorumludur.

B. NATO Siber Savunma Yönetim Kurulu:

Üst düzey yönetim ve karar organıdır. NATO Siber Savunma Politikasının hayata geçirilmesi ve NATO ve/veya NATO ülkelerinden herhangi birine ciddi bir siber saldırı yapılması veya siber saldırı tehdidinin ortaya çıkması durumunda, uygun önlemlerin alınmasından sorumludur.

C. NATO Siber Savunma Koordinasyon ve Destek Merkezi:

Üye ülkeler ve haricî organizasyonlar ile birlikte NATO'nun siber savunma faaliyetlerinin koordinasyonu bu merkezde yerine getirilir. Kriz yönetimi ve acil müdahale konularında bilgi değişimini sağlamaktan ve gerekli bağlantıları kurmaktan sorumludur.

Ç. NATO Bilgisayar Olaylarına Müdahale Yeteneği (NCIRC) Teknik Merkezi:

NATO çapında siber savunma hizmetlerinin geliştirilmesi, uygulanması ve idamesinin sağlanmasından sorumludur. Uygulamada Bilgisayar Olaylarına Müdahale Ekibi (BOME) (Computer Events Response Team, CERT®) fonksiyonunu yerine getirir.

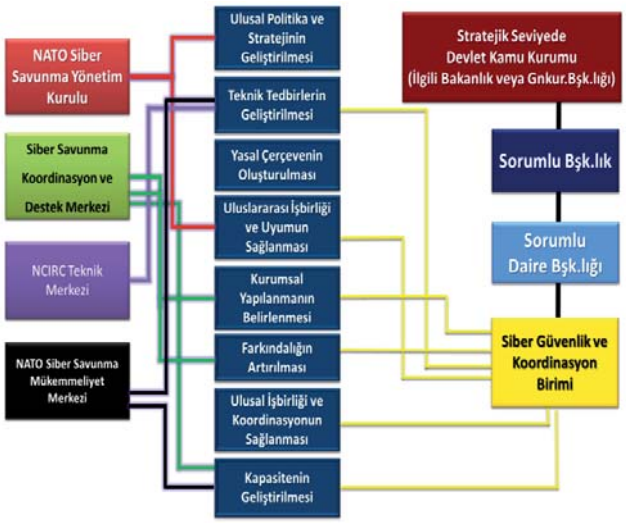
D. NATO Siber Savunma Mükemmeliyet Merkezi:

Üye ülkelerden çalışanların oluşturduğu bu merkez bir ARGE alanı gibi faaliyet göstermektedir. Gerek Siber Savunma Koordinasyon ve Destek Merkezi gerekse Bilgisayar Olaylarına Müdahale Yeteneği ve Teknik Merkezi ile koordinasyon halinde çalışmaktadır. Yeni siber savunma konseptlerin ve yeteneklerin geliştirileceği bir merkezdir.

NATO'da siber güvenliğe yönelik olarak yaklaşımlar pro-aktif bir tutumdan ziyade re-aktif bir tutum izlemektedir. Tehditlerin belirmesine müteakip tedbirler geliştirilmektedir. BU hassasiyet oluşturulan yapının en zayıf alanı olarak görülmektedir. Bu hassasiyettin giderilmesi için her yıl icra edilen Siber Tatbikatlar önem arz etmektedir.

IV. NATO'DAN ULUSAL OLARAK YARARLANILACAK SİBER GÜVENLİK UNSURLARI VE YAKLAŞIM MODELİ

NATO yukarıda da ifade edildiği gibi üyelerin güvenliklerini sağlamak maksadıyla kurulmuştur. Uluslararası alanda siber güvenlik bağlamında tecrübe kazanmış bir örgüttür. Burada kazılan yeteneklerin, tecrübelerin, üye ülkelerin yetenek ve tecrübelerinin uzman bir bakış açısı ile yönetilmesi gerekmektedir. Akademik alanda siber güvenliğe yönelik belirlenen temel unsurların NATO'da oluşturulan teşkilatın içerisinde hangi birimler tarafından yönetildiği Şekil-3'te belirtilmiştir.



Şekil 3. NATO'dan Ulusal Olarak Yararlanılacak Siber Güvenlik Unsurları ve Yaklaşım Modeli

V. SONUÇ

Olası bir siber savaşta etkin savunma yapılabilmesi için siber güvenlik konusunun iyi kavranması ve değerlendirilmesi gerekmektedir. Bu bağlamda Ulusal Siber güvenlik Strateji ve 2013-2014 Eylem planında da belirtildiği gibi yasal düzenlemelerin yapılması, uluslararası hukuktan kaynaklanan hakların kullanılabilmesi için hazırlık yapılması, ulusal bilgisayar olaylarına müdahale organizasyonunun oluşturulması, ulusal siber güvenlik altyapısının güçlendirilmesi, siber güvenlik alanında insan kaynağı yetiştirilmesi ve milli teknolojilerin kullanılması hayati öneme sahiptir [7].

Siber güvenlikte uluslararası alanda oluşturulacak işbirliği ve koordinasyon devletlerin kendi güvenliklerini sağlanmasında öncelikli alması gereken tedbirlerdendir. Bu bağlamda siber alandaki güvenliğini en üst seviyeye çıkarmak için üye ülkelerin yetenek, kabiliyet ve tecrübelerinin, yönetim alanında deneyim kazanmış personel ve teşkilatla yürütülmesi ulusal siber güvenliğimize daha fazla katkı sağlayacaktır. Söz konusu koordinasyon biriminin yetenekleri geliştirilerek özel sektördeki kurum ve kuruluşlara etkin deneyim ve bilgi paylaşımı yapabilecektir. Söz konusu yaklaşım modeli ile aşağıda belirtilen faydaların sağlanacağı değerlendirilmektedir.

- Uluslararası geliştirilen politikalar ile ulusal politika dinamik bir yapıta tutulacak, yaşayan bir siber güvenlik politikası izlenebilecek,

- NATO bünyesinde icra edilen tatbikatlardan elde edilen tecrübeler ve bilgi birikimleri ile gerek özel gerekse kamu kurum ve kuruluşlarına yol gösterilerek sistemlerinin güvenlikleri bir canlı haline gelecek,

- Bu tatbikatlardan elde edilen tecrübeler ile ulusal olarak icra edilecek tatbikatlar hedefleri gerçekçi, güncel tehditlerin değerlendirildiği, siber saldırı imkân ve kabiliyetlerinin nasıl olabileceğinin kıymetlendirildiği tatbikatlar icra edebilecek,

- Siber güvenlik, siber savunma ve gelecekte ortaya çıkması muhtemel tehditlere karşı düzenlenen akademik

çalışmalarda rol almasın için personel teşvik edilecek ve kurumsal olarak siber dünyaya yönelik akademik bir birikim oluşturulabilecek,

- Üye ülkeler tarafından siber güvenliğe yönelik izlenen politika, teknoloji ve yasal mevzuattan istifade ile ulusal alanda düzenlemeler yapılabilecek,

- Kamu kurum, kuruluşları ile özel kurum ve kuruluşların siber tehdit ve saldırılar ile güvenlik önlemleri konusunda sürekli bilgilendirici ve bilinçlendirici mekanizma tesis edileceği değerlendirilmiştir.

KAYNAKLAR

[1] Mustafa ÜNVER, Cafer CANBAY, Ayşe Gül MİRZAOĞLU "Uluslararası Kuruluşların Siber Güvenlik Faaliyetleri" Konulu makale 2009, S. 10

[2] Bilim ve Teknik Dergisi, Emre BAKIR "Türkiye'de Siber Güvenlik" konulu makale Kasım 2012, S. 12

[3] Ulaştırma, Denizcilik ve Haberleşme Bakanlığı "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" konulu çalışma, Ocak 2013, S. 14-19

[4] http://www.nato.int/docu/review/2011/11-september/Cyber-threads/TR/, Yeni Tehditler; Siber Boyut, Erişim Tarihi: 10 Temmuz 2013

[5] İstanbul Bilgi Üniversitesi, Bilişim ve Teknoloji Enstitüsü "Siber Güvenlik Raporu" konulu çalışma Mayıs 2012, S. 43

[6] Rex Huges, "NATO and Cyber Defence" NATO Review, April 2009 S. 2

[7] Bilim ve Teknik Dergisi, Emre BAKIR "Türkiye'de Siber Güvenlik" konulu makale Kasım 2012, S. 15