Uluslararası Siber Güvenlik Strateji ve Doktrinleri Kapsamında Alınabilecek Tedbirler

Uğur Akyazı

***Özet*—Siber uzay artık çoğu ülkede kara, deniz, hava ve uzay gibi bir askeri harekât alanı olarak değerlendirilmektedir. Diğer çatışma alanlarından farklı olarak siber uzay ulusal güç unsurlarının herbirisi üzerinde etkinlik sağlamaktadır. Bu çalışmada siber harekât ortamı tarif edilmiş, NATO'nun siber güvenlik politikası, ülkelerin stratejileri ve ilgili ABD doktrinleri incelenmiştir. Bu kapsamda alınması gereken önlemler ortaya konmuştur.**

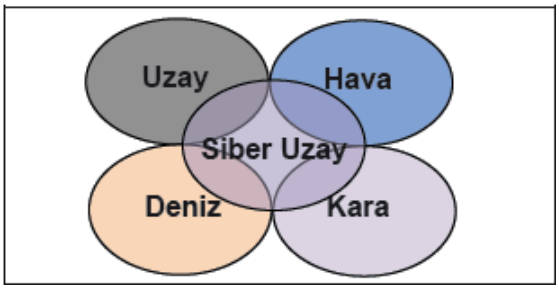
***Anahtar Kelimeler*—Siber güvenlik stratejileri, siber güvenlik doktrinleri**

***Abstract*—Cyber space is considered to be a military operational environment as land, sea, air and space by many countries. Unlike other conflict areas, cyber space affects each one of the elements of the national power. In this study, operational environment of cyber space is described and cyber security policy of NATO, strategies of other developed countries and related U.S. doctrines are examined. In this context, measures to be taken are put forward.**

***Index Terms*—Cyber security policy, strategy and doctrine**

I. GİRİŞ

SİBER güç, tüm harekât alanları ve güç unsurları üzerindeki olayları etkileyerek avantaj sağlamak için siber uzayı kullanma kabiliyetidir. Bu tanımdan da anlaşılacağı gibi siber uzay artık çoğu ülkede kara, deniz, hava ve uzay gibi bir askeri harekât alanı olarak değerlendirilmektedir. Diğer çatışma alanlarından farklı olarak siber uzay ulusal güç unsurlarının herbirisi üzerinde etkinlik sağlamaktadır (Şekil-1).



Şekil-1: Beşinci Harekât Alanı olarak "Siber Uzay"

ABD Hava Kuvvetleri Temel Doktrininde hava gücü artık "stratejik, operasyonel veya taktik hedeflere ulaşmak için hava, uzay ve siber uzayın kullanılması ve kontrolü yoluyla askeri gücü veya etkiyi yöneltme yeteneği" olarak tanımlanmakta ve siber uzay bir savaş alanı olarak algılanmaktadır. Bu tanımın yakın zamanda diğer uluslarla beraber kendi doktrinlerimizde de yer bulacağını tahmin etmek zor değildir. Siber uzay hava, kara, deniz ve uzay olan diğer etki alanları arasında bulunmakta ve saklanan, değiştirilen ya da aktarılan verileri kullanan bilişsel süreçler ile bu fiziksel etki alanlarını birbirine bağlamaktadır.

Uğur Akyazı, Hava Kuvvetleri Komutanlığı, uakyazi99@yahoo.com

İnternet, siber uzayı oluşturan en önemli unsurlardan biri olmakla birlikte, siber uzay sadece internet ile sınırlı değildir. Tanımından da anlaşılacağı üzere, iletişim ağları, dış dünyaya kapalı askeri ağlar, enerji dağıtım ağları, cep telefonları, yazılım tabanlı telsizler, elektronik komuta sistemleri, uydu sistemleri, insansız hava araçları gibi birçok sistem ve donanım siber uzayın elemanlarıdır.

Siber savaş geleneksel savaşa benzemez, ama hava bombardımanı, denizaltı savaşı, özel harekât güçleri ve hatta suikastçıların tarihsel rolü ile bazı özellikleri paylaşır. Özellikle, uzak mesafelerden veya baskın prensibini istismar ederek bir düşmana ciddi düzeyde asimetrik hasar verebilir. Siber saldırıların en azından yakın gelecekte, stratejik bir bombardımandan daha ölümcül olması beklenmemektedir. Ama sonuçta, askeri operasyonların başarısı etki temellidir. Eğer bir hedefi hem bir balistik füze hem de bir bilgisayar solucanı yok edebiliyor veya devre dışı bırakabiliyorsa, doğal seçim solucan olacaktır [1].

II. NATO SİBER GÜVENLİK POLİTİKASI

8 Haziran 2011 tarihinde revize edilen NATO Siber Savunma Politikası, NATO'yu İttifak'ın temel görevleri olan kollektif savunma ve kriz yönetimini gerçekleştirmek amacıyla kendi iletişim ve bilgi sistemlerinin korunmasına odaklamaktadır. Ancak, siber tehditler ittifakın ve devletin sınırlarını aştığı için, İttifak'ın NATO ortağı ülkeler, özel sektör ve akademik çevreler ile işbirliği ihtiyacı da ifade edilmektedir. NATO üyesi devletler uluslararası işbirliğinin önemini Mayıs 2012'deki Chicago Zirvesi Bildirgesi'ndeki şu ifadelerle pekiştirmişlerdir: "Siber güvenlik tehditlerini belirlemek ve ortak güvenliğimizi geliştirmek için somut işbirliğini artırmak amacıyla ilgili ortak ülkelerle ve uluslararası kuruluşlarla beraber çalışmaya kararlıyız." [2]

NATO Siber Savunma Politikası'nın kavramsal temelini oluşturan NATO Siber Savunma Konsepti Mart 2011 tarihinde hazırlandı ve 8 Haziran'da NATO Savunma Bakanları tarafından onaylandı. Konseptle beraber NATO'nun kendi yapıları ve Müttefiklerin savunma kuvvetleri için özel görevler ve faaliyetleri içeren ayrıntılı bir belge olan Eylem Planı yayımlanmıştır. Siber Savunma Politikası'na göre:

a. NATO'nun temel görevleri olan kollektif savunma ve kriz yönetimini gerçekleştirmek için NATO yapılarına ve planlama süreçlerine siber savunma hususları entegre edilecek,

b. NATO ve müttefikleri için kritik olan siber varlıkların korunması ve savunmasına odaklanılacak,

c. Güçlü siber savunma yetenekleri geliştirilecek ve NATO'nun kendi ağlarının korunmasını merkezileştirilecek,

ç. NATO'nun temel görevleri için kritik olan ulusal ağların siber savunması için minimum gereksinimler geliştirilecek,

d. Ulusal kritik altyapılarının güvenlik açıklarını azaltmak için Müttefiklere yardım sağlanacak,

e. Ortaklar, uluslararası kuruluşlar, özel sektör ve akademik çevreler ile birlikte çalışılacak,

f. İlgili siber savunma gereksinimlerinin tespit edilerek NDPP (NATO Defence Planning Process) yoluyla öncelik verilecek,

g. NATO Askeri Yetkilileri siber savunmanın NATO'nun temel görevleri yerine getirmesini, askeri görevler için planlamayı ve bu görevlerin yürütülmesini nasıl desteklediğini değerlendirecek,

ğ. Farkındalık programları geliştirilecek ve NATO tatbikatlarına siber bileşenler eklenecek,

h. NATO ve müttefikleri Tallinn'deki Kooperatif Siber Savunma Mükemmeliyet Merkezi'nden uzmanlık ve destek almak için teşvik edilecektir [3].

NATO ülkeleri Ulusal Siber Güvenlik ve (kollektif) siber savunmanın yakın bağlantı içerisinde olması gerektiği görüşünde olduklarını giderek daha açıkça ifade etmektedirler. Bu durumu en doğrudan açıklayan Beyaz Saray olmuştur: "Bütün devletler doğal olarak kendini savunma hakkına sahiptirler ve siber uzay yoluyla yapılan bazı düşmanca eylemler askeri ortaklarımız ile olan taahhütlerimiz gereği olan eylemleri mecbur kılabilir." "Müttefikler arasındaki güçlü ilişkiler etkili bir siber savunma politikasının temelini oluşturmaktadır" şeklinde olan Fransız Ulusal Siber Güvenlik Stratejisinde olduğu gibi diğer bazı ulusal stratejiler doğrudan kollektif savunmayı değil ama NATO taahhütlerini öne çıkarmaktadır. "Kollektif siber savunma"nın tam olarak ne gerektirdiği açık değildir ve çok geniş bir aralıktaki siber eylemleri kapsayabilir. Bunlar:

a. Etkilenen bir ülkedeki kritik altyapıların savunmasına yardımcı olması için asker ya da sivillerin kullanılması,

b. Kayıt tutma ve çağrı yönetimi gibi en kolay işlerden, olaylara müdahaleyi yönetme gibi profesyonel görevlere kadar askerlerin ya da sivillerin kriz yönetim görevlerinde kullanılması,

c. Soruşturmalara yardımcı olmaları için adli müfettişlerin görevlendirilmesi,

ç. NATO ya da diğer ülkeler veya sektörlerle koordinasyona yardımcı olmaları için ekiplerin görevlendirilmesi. Örneğin, finans sektörüne yapılan bir saldırı üzerine bilgi akışında yardımcı olmak için ilgili ülkeye bir finans temsilcisi gidebilir, ya da askeri bir irtibat ekibi aynı şeyleri askeri koordinasyon için yapabilir.

d. İnternet Servis Sağlayıcılarına, saldırı altındaki ülkeye giden saldırı trafiğini engellemeleri direktifinin verilmesi (veya ikna edilmesi),

e. İnternet Servis Sağlayıcılarına, saldırıları sona erdirmede yardımcı olmak için işbirliğinde bulunana kadar saldırının arkasında olduğundan şüphelenilen ülkenin trafiğini kısma direktifinin verilmesi (veya ikna edilmesi),

f. Saldırının arkasındaki Komuta Kontrol altyapısını bozmaya yönelik seçici aktif savunmanın yapılması,

g. Saldırıları kurutmak ve savunma seçeneklerini artırmak için ilave yerel Internet Değişim Noktaları ve diğer yerel altyapıların kurulması,

ğ. Saldırı altındaki ülkenin ek kapasite geliştirmesine yardım etmek için ağ teknolojisi üreticilerinin sipariş önceliğini bu ülkeye vermelerinin sağlanması,

h. İttifak üyesi bir ülkenin kendi siber saldırı kuvvetlerini İttifak adına karşı atak yapmak için konuşlandırması [2].

III. ULUSAL SİBER GÜVENLİK STRATEJİLERİ

Yüzden fazla ülkenin devlete ait siber yetenekleri bulunmakta olup bunların en az elli tanesi gelecekteki ulusal ve ekonomik güvenlik girişimleri için siber güvenliğin önemini vurgulayan bir çeşit siber strateji yayınlamıştır. Bu ülkelerden öne çıkanlar Tablo-1'de görülmektedir. Türkiye'nin "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" Ulaştırma, Denizcilik ve Haberleşme Bakanlığı koordinesinde 20 Haziran 2013 tarihinde yayınlanmıştır.

ABD Ulusal Siber uzay Güvenliği Stratejisi beş ulusal önceliği dile getirmektedir:

a. Ulusal Siber Uzay Güvenliği Yanıt Sistemi;

b. Ulusal Siber Uzay Güvenliği Tehdit ve Güvenlik Açığı Azaltma Programı;

c. Ulusal Siber Uzay Güvenliği Farkındalığı ve Eğitim Programı;

ç. Devletin Siber Uzay Güvenliğini sağlamak ve

d. Ulusal Güvenlik ve Uluslararası Siber Uzay Güvenlik İşbirliği.

İlk öncelik siber olaylara karşı verilecek tepkileri geliştirmeye ve bu tür olaylardan gelecek potansiyel zararı azaltmaya odaklanır. Ikinci, üçüncü ve dördüncü önceliklerin amacı siber saldırılardan gelecek tehditleri ve kendi güvenlik açıklarını azaltmaktır. Beşinci öncelik ise, ulusal güvenlik varlıklarını etkileyebilecek siber saldırıları önlemek ve bu tür saldırılara karşı uluslararası tepkiler geliştirmek ve yönetmektir [5].

Tablo-1: Siber Güvenlik Stratejisi sahibi ülkeler [4]

Ulusal Siber Güvenlik Stratejileri	
ABD	Savunma Bakanlığı, "Siber Uzayda Harekât Stratejisi" (2011)
	Beyaz Saray, "Uluslararası Siber Uzay Stratejisi: Ağlarla Birleştirilmiş Dünyada Refah, Güvenlik ve Şeffaflık" (2011)
	İç Güvenlik Bakanlığı, "Güvenli Siber Gelecek Planı: İç Güvenlik Kuruluşları Siber Güvenlik Stratejisi" (2011)
İngiltere	"İngiltere Siber Güvenlik Stratejisi: Dijital Dünyada İngiltereyi Korumak ve Yükseltmek" (2011)
Fransa	İç İşleri Bakanlığı, "Fransa Stratejisi: Bilişim Sistemlerinin Güvenliği ve Savunması" (2011)
Almanya	Federal İç İşleri Bakanlığı, "Almanya Siber Güvenlik Stratejisi" (2011)
Hollanda	"Ulusal Siber Güvenlik Stratejisi: İşbirliği ile Başarı" (2011)
Hindistan	Bilişim Teknolojileri Bakanlığı, "Siber Güvenlik Stratejisi" (2011)
Türkiye	Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, "Ulusal Siber Güvenlik Stratejisi" (2013)

IV. ABD DOKTRİNLERİ

ABD Hava Kuvvetleri Temel Doktrininde [6] hava gücü artık "stratejik, operatif veya taktik hedeflere ulaşmak için hava, uzay ve siber uzayın kullanılması ve kontrolü yoluyla askeri gücü veya etkiyi yöneltme yeteneği" olarak tanımlanmaktadır. Hava Kuvvetleri temel fonksiyonlarından olan Siber Uzay Üstünlüğü ise "engelleyici bir müdahale olmaksızın belirlenen zaman ve etki alanında harekât icra edebilmek amacıyla siber uzaydaki harekât avantajı" olarak ifade edilmektedir [7]. Bu işlevin alt öğeleri: Siber uzay Kuvvetlerini Kullanma, Siber uzay Savunması, Siber uzay Desteğidir.

ABD Savunma Bakanlığı, "Siber Uzay Harekâtları için Ulusal Askeri Stratejisi"ni yayınlayarak siber uzayı bir savaş alanı olarak algıladığını resmen belirtmiştir. Bu belgede, siber uzay veri saklamak, değiştirmek, ağ sistemleri ve ilgili fiziksel altyapılar sayesinde veri akışını sağlamak için elektronik ve elektromanyetik spektrumun kullanıldığı bir alan olarak tanımlanmaktadır. Bu tanıma göre, siber uzay elektronik ve elektromanyetik enerji kullanan ağ sistemlerinden oluşan gerçek bir fiziksel etki alanıdır.

ABD Silahlı Kuvvetlerin siber uzay tanımı, siber uzayın bilgisayar ağlarından daha fazla şeyler içerdiğini göstermektedir. Daha da önemlisi, ağ sistemlerinin elektromanyetik enerji kullanılarak oluşturulmuş olmasından dolayı, siber uzaydaki savaşlar hâlihazırda elektronik harp olarak kabul edilen yetenekleri de içerecektir. Elektromanyetik enerji kullanarak bir ağın elektronik bileşenlerini sorgulamak veya bozmak için doğrudan internete bağlı olmayan ağlara bile erişilebilinecek veya saldırılabilinecektir. Bu silahlı kuvvetler için önemli bir tehdittir.

Çoğu askeri komuta ve kontrol ağları ve hava savunma sistemleri silahlı kuvvetler dışındakilerce doğrudan erişilemeyen izole ya da kapalı ağlardır. Siber uzay elektromanyetik ortamda fiziksel bir etki alanı olarak tanımlandığından dolayı, siber uzayda fiziksel harekât ile savaşılacaktır. Bu, sanal etkiler yaratmak veya düşmanlara sanal gerçeklik ortamında saldırmak değildir. Bu nedenle, siber uzaya bir harekât alanı olarak yaklaşmak, bu etki alanının sürekli kullanılabilmesini sağlamak için bazı yetenekleri geliştirmek gerekmektedir. Dokümanda, etkiler oluşturmak için siber yeteneklerden bazılarını geçmişte kullandıkları belirtilirken, bu kabiliyetlerin siber uzayda eylem özgürlüğünü sağlamak için henüz kullanılmadıkları ifade edilmektedir. Siber uzayda hareket serbestîsi elde ettikten sonra müşterek kuvvet komutanının stratejik, operasyonel ve taktik hedeflerine ulaşmak için diğer işlemleri gerçekleştirebileceği anlatılmaktadır.

Hava Kuvvetleri'nin yeteneklerinden yararlanmak için siber uzayda harekât icra edebilmek amacıyla ABD Hava Kuvvetleri Siber Komutanlığı kurulmuştur. Hava Kuvvetleri, müşterek savaşta düşmanın kuvvetlerini yönlendirme, komuta ve kontrol etme, hatta silahlarını ateşleme kabiliyetini etkileyecek şekilde siber uzayda gerçek etkiler oluşturma imkânı sağlamayı hedeflemektedir. Bu etkiler kolayca düşmanın zihninde oluşacak etkiler değildir. Diğer bir deyişle, bunlar sanal ya da hayali etkiler değildir - düşman siber uzaydaki savaşta gerçekten ölebilir veya zarar görebilir [8].

Siber uzay, insan yapımı bir harekât alanıdır ve doğal harekât alanları olan kara, deniz, hava ve uzaya benzememektedir. Siber uzayın düğümleri fiziksel olarak diğer harekât alanlarının içerisinde bulunur. Siber uzaydaki etkinlikler diğer harekât alanlarındaki faaliyetler için hareket serbestîsi sağlayabilirken diğer harekât alanlarındaki faaliyetler de siber uzay içerisinde etkiler oluşturabilir. Siber uzay fiziki altyapı, elektronik sistemler ve elektromanyetik spektrumun (EMS) bölümleri ile desteklenmektedir. Yeni sistemler ve altyapılar geliştirildikçe, yüksek EMS frekanslarını kullanabilir, daha yüksek veri işleme kapasitesi ve hızına sahip olabilir ve daha büyük bant genişliği kullanabilir. Sistemler verileri değiştirdiği gibi aynı zamanda frekansları değiştirmek için de tasarlanmış olabilir. Bu nedenle, siber uzayda fiziksel manevra alanı bulunmaktadır.

Siber uzayda mantıksal manevra kabiliyeti genellikle konakçı bilgisayar sistemleri tarafından kullanılan güvenlik protokollerinin bir fonksiyonudur. İstenmeyen sistemlerin girişine karşı savunma, konakçı bilgisayar sisteminin kodunda ya da mantığında yer almaktadır. Sistemler arasında

bir bağlantı kurulduktan sonra, potansiyel bir saldırganın sisteme girmesi için mantıksal bir hatadan faydalanması gerekir. Bu nedenle, siber uzayda mantıksal manevra biçimi kod yazmadır.

Saldırgan, hedeflenen sistemlere karşı manevra kabiliyeti kazanmak için kötü amaçlı kod yazar. Sistem içinde istenmeyen bir varlığın farkına varıldığında, savunma sistemi girişi engellemek için sistemin kodunu değiştirecektir. Hedef sistem içinde kalmak isteyen saldırgan, kötü amaçlı kodunu buna göre uyarlar. Bu süreç geleneksel hava, kara, uzay ve deniz alanlarında avantajlı pozisyonlar elde etmek için manevra yapan güçlere eşdeğerdir. Mantıksal ve fiziksel manevra alanlarının her ikisi de gereklidir – genelde biri olmadan diğeri işe yaramaz. Tablo-2'de ABD Doktrinlerinde yer alan Harp Prensiplerinin Siber uzay Harekâtında uygulamalarına örnekler verilmiştir.

ABD'nin Siber Güvenlik Ulusal Stratejisi kapsamlı bir stratejidir. Üç adet stratejik önceliği vardır:

a. Amerika'nın kritik altyapılarına karşı siber saldırıları önlemek,

b. Siber saldırılara karşı ulusal güvenlik açıklarını azaltmak,

c. Siber saldırılardan gelecek zararı ve toparlanma süresini en aza indirmek.

Siber uzay Harekâtları için Ulusal Askeri Strateji (NMS-CO) siber uzayda ABD üstünlüğünü sağlamak amacıyla ABD Silahlı Kuvvetleri için hazırlanmış olan kapsamlı bir stratejidir. NMS-CO'nun dört stratejik önceliği bulunmaktadır:

a. Düşman karar döngüleri içinde harekât icra edebilmek için inisiyatif kazanmak ve korumak,

b. Askeri harekâtlar arasındaki siber yetenekleri entegre etmek,

c. Siber uzay harekâtları için yetenek geliştirmek,

ç. Siber uzay harekâtlarındaki riski yönetmek.

Halkın bilgi ve becerisi ile birlikte taarruzi ve müdafi siber harekâtların entegrasyonu, bu yaklaşım için temel esastır.

Siber harekâtlar stratejik, operasyonel ve taktik seviyedeki birden çok etki alanında aynı anda etkiler oluşturabildiği için devam eden harekâtlar için bile stratejik düzeyde planlama yapmak zorunludur. Plancıların kamu kuruluşları ve ortak ülkelerdeki uygun istihbarat ve hedefleme kuruluşlarına girdi sağlamaları ve geri bildirim almaları gerekmektedir. Siber uzayın benzersiz özellikleri ve hız potansiyeli hızla değişen durumlara tepki verme yeteneği gerektirir.

Tablo-2: Harp Prensiplerinin Siber Harekât Uygulamaları

PRENSİP	AMAÇ	ÖRNEK SİBER UZAY HAREKÂTI
Hedef	Her askeri operasyonu açık bir şekilde tanımlanmış, kararlı, ulaşılabilir bir hedefe doğru yöneltmek	Müşterek Komutanın yönettiği siber uzay saldırıları ile düşmanın önemli enerji ağlarının elektrik gücünü kapatmak
Taarruz	Bozmak, zayıflatmak, engel olmak, caydırmak, ele geçirmek, korumak ve istismar etmek	2007 yılında yapılan Dağıtık Hizmetin Engellenmesi Saldırısı ile Estonya ağ sistemine aşırı yüklenme olmuştur
Sıklet Merkezi	Etkileri en avantajlı yer ve zamanda yoğunlaştırmak	2008 işgali sırasında Rus aktörlerin Gürcistan güçlerinin koordinasyonu bozmak için Gürcü ağlarda önleyici siber saldırı yapması
Kuvvet Tasarrufu	İkincil çabalara minimum gerekli güç tahsis etmek	"Kinetik" varlıkları diğer harekâtlar için serbest bırakabilmek amacıyla düşmanın önemli düğüm noktalarına siber saldırı yapılması
Manevra	Düşmanı dezavantajlı bir konuma sokmak	Bir siber saldırı sırasında çok sayıda IP kullanarak kimliğinin belirlenmesini önlemek
Emir ve Komuta Birliği	Bir sorumlu komutan altında kuvvet birliğini sağlamak	24'üncü Hava Kuvveti ile Hava Kuvvetleri küresel bilgi şebekesinin kontrolü
Emniyet	Müdahalesiz erişim sağlamak	Katmanlı savunma, kendi kendini düzeltme ve yeniden yapılandırılmalarla Komuta Kontrol ağlarının işlerliğini sağlamak ve korumak
Baskın	Düşmanı hazırlıksız olduğu bir zamanda, yerde veya şekilde vurmak	Savunmasız veya önceden ele geçirilmiş sistemlere habersiz yapılan siber saldırılar
Sadelik	Anlaşılmayı sağlamak için açık ve öz yönlendirme yapmak	Kuvvetin her düzeydeki veri ve ağ yapılarına kullanıcı dostu erişim sağlamak
Sınırlama	Gereksiz güç kullanımını önlemek, yan hasarı sınırlamak	Hedefleri yok etmeden etki oluşturarak, komutanlara tek başına icra edilebilen, kinetik olmayan seçenekler sağlamak
Sebat	Ulusal stratejik nihai durumu gerçekleştirene kadar savaşa devam etmek	Sistemlerin sürekli güvende çalışmasını sağlamak; ortak ülkelerde güçlü siber yetenekler oluşturmak
Meşruiyet	Hedef toplum ve ortakların gözünde, eylemlerin yasal, ve meşru göründüğünden emin olmak	Kinetik saldırıların avantajlı olmadığı şartlarda düşmana karşı istenilen etkiyi elde etmek için kinetik olmayan siber yetenekleri kullanmak

Plancılar siber uzayda artan güvenliğin harekâtlar üzerindeki etkisini göz önünde bulundurmalıdır. Bilgi harekâtlarının koşullarını değiştirmek veya ağları analiz etmek için ek araçlar kullanmak düşük ağ çalışma hızına

neden olabilir. Bant genişliği sınırlı olan veya kuvvetlerin çok dağınık olduğu bir ortamda, plancılar siber savunma geliştirmek için alınan önlemlerin aslında harekâtları engelleyebileceği veya uyumlarını bozabileceğini dikkate almalıdırlar.

Askeri operasyonların yürütülmesi aşamasında, Harekât Merkezi içindeki siber uzay operatörleri siber etkileri komutanın niyeti, istenilen etkiler, dost ve düşman kuvvetlerin yetenekleri temelindeki zaman aşamalı manevra ve vuruş düzeni içine entegre edecektir.

Görev döngüsünün önemli bir ürünü olan Hava Kuvvetleri Siber Görev Emri (CTO), siber uzay kuvvetlerinin görevlerini alması ve uygulaması için kullanılır. Hava görev döngüsünü temel alan siber görev döngüsü, siber uzay harekâtlarının etkinliğinin planlaması, koordinasyonu, uygulanması ve değerlendirilmesi için kullanılan iteratif bir süreçtir. Krizleri desteklemek için döngünün süresi savaş temposuna göre uzatılabilir veya kısaltılabilir. Durumsal farkındalık ve çakışmaların önlenmesi amacıyla siber harekâtların tamamı CTO'da yer almalıdır. Planlama aşamasında, 624'üncü Harekât Merkezi CTO'yu tamamlamak için COMAFFOR / JFACC direktifini, angajman kurallarını (ROE), müşterek öncelikli hedef listesini, aday hedef listesini ve onaylı ana hava taarruz planını (MAAP) kullanır.

Yasal hususlar ve uluslararası yasal yükümlülükler siber yeteneklerin kullanılmasında da geçerlidir. Uluslararası hukuk, iç hukuk ve politika kararları, silahlı çatışma hukuku, angajman kuralları harekât faaliyetlerinin değerlendirildiği yasal çerçeveyi oluşturmaktadır. Genellikle, komutanın karargâhındaki askeri hukukçu siber uzay harekâtlarını hukuka uygun olarak yapması konusunda, Askeri Harekâtlara Hukuki Destek (JP 1-04) [9] dokümanına göre ilgili komutana tavsiyelerde bulunur. Hukuki destek personelinin siber uzay harekâtlarında kullanılan bilgi, süreç ve programlara erişimi ve temel siber teknolojilerine hâkimiyeti olmalıdır [7].

V. SONUÇ

Günümüzde belli bir artış trendi izlese de hayatın akışını çok ciddi biçimde olumsuz etkileyecek siber saldırılar henüz gerçekleşmemiştir. Ancak gelecek yıllarda, dünyamız büyük oranda e-dünyaya dönüştüğünde gerçekleştirilecek siber saldırıların hayal dahi edilemeyecek boyutta cana ve mala zarar vermesi kuvvetli bir olasılık olarak görülmektedir. Bu itibarla, gelecekte kıyamet senaryosu benzeri kötü durumlarla karşılaşmamak için bugünden siber güvenlik konusunda tedbirlerin alınmasında yarar görülmektedir.

Alınacak tedbirlerin başarılı olabilmesi için bunların küresel çapta olması gerekmektedir. Küresel çapta işbirliği ve koordinasyon sağlanarak ortak algı, anlayış ve kabullerin oluşturulması, sorunların önlenmesi, önlenemese dahi ortaya çıktıktan sonra hızla ve asgari zararla çözülebilmesi noktasında büyük önem arz etmektedir. Bu itibarla, tüm ülkelerin taraf olacağı sözleşmeler marifetiyle küresel bir hukuki çerçeve geliştirilmesi, bu hukuki çerçeve içinde yargı ve kolluk birimlerinin hızlı ve etkin çalışabilmelerinin temin edilmesi hayati önem taşımaktadır. Bunların yanında, siber alan da diğer alanlarda olduğu gibi silahlı çatışma hukukuna uygun davranış standartlarına sahip olması gerekmektedir. Uluslararası siber uzay düzenlemeleri için diğer ortak alan düzenlemeleri örnek alınabilir. 150 ülkenin katkısıyla 14 yılda ancak oluşturulabilen BM Deniz Hukuku Sözleşmesi'nde olduğu gibi, eğer ülkeler ısrarla takip etmezse kapsamlı bir çerçevenin geliştirilmesi çok zordur.

NATO Siber Savunma Politikasında yer aldığı gibi Silahlı Kuvvetler yapımıza ve planlama süreçlerine siber savunma hususları entegre edilmeli, farkındalık programları geliştirilerek tüm tatbikatlara siber bileşenler eklenmelidir. Siber uzay harekâtlarının planlaması, koordinasyonu, uygulanması ve değerlendirilmesi için hava görev döngüsünü temel alan bir siber görev döngüsü kullanılabilir. Harekât merkezlerine siber güvenlik hücreleri eklenmeli ve harekâtı destekleyen siber harekât merkezleri kurulmalıdır. Siber güvenlik teşkilatı içerisinde bilgi sistemleri güvenliği, iletişim ağı güvenliği, adli analiz gibi teknik unsurlara ilave olarak; istihbarat, harekât ve adli konularda görev yapacak icracı veya danışman statüsünde personelin görevlendirilmesi sağlanmalıdır.

KAYNAKLAR

1. K. Geers, "Strategic Cyber Security", NATO Cooperative Cyber Defence Centre of Excellence, 2011
2. *National Cyber Security Framework Manual*, Talinn, NATO CCDCOE Publication, 2012
3. *Defending the Networks, The NATO Policy on Cyber Defence*, 2011
4. M.D. Cavelty, "The Militarizatin of Cyber Security as a source of global tension", Strategic Trends 2012, Chapter 5, Center for Security Studies, Zurich
5. E. Tıkk, "Frameworks for International Cyber Security", NATO Cooperative Cyber Defence Centre of Excellence, Talinn, 2011
6. *Air Force Doctrine Document (AFDD)-1, Hava Kuvvetleri Temel Doktrini*, ABD Hava Kuvvetleri, 2011
7. *Air Force Doctrine Document (AFDD) 3-12, Siber Uzay Operasyonları*, ABD Hava Kuvvetleri, 2011
8. D.T. Fahrenkrug, "Cyberspace Defined", The Wright Stuff, Air University, 17 Mayıs 2007
9. *Joint Publication (JP) 1-04, Legal Support to Military Operations*, ABD Genelkurmay Başkanlığı, 2011

Uğur AKYAZI. 1978 yılında Çankırı'da dünyaya gelmiştir. İlk ve ortaokulu Kırıkkale'de, liseyi Kuleli Askeri Lisesi'nde okumuş ve Hava Harp Okulundan 1999 yılında mezun olmuştur. 1999-2011 yılları arasında Hava Harp Okulu Dekanlığı Bilgisayar Mühendisliği Bölümü Yazılım A.B.D. Bşk.lığı Öğretim Elemanlığı görevini yapmıştır. 2011-2013 yılları arasında Hava Harp Akademisi öğrenimini tamamlamıştır. 2002 yılında ABD Hava Kuvvetleri Teknoloji Enstitüsü'nde (AFIT) Sistem Mühendisliği dalında yüksek lisans, 2011 yılında İstanbul Teknik Üniversitesi'nde Bilgisayar Mühendisliği dalında doktora eğitimi almış olup 2008-2011 yılları arasında yayımlanmış 3 adet uluslararası konferans makalesi ve 1 adet uluslararası dergi makalesi bulunmaktadır.