

Siber Tehdit Ortamında Muharebe Sahasının Sayısallaştırılması

Selçuk DAL, Eşref FIRAT, Serbülen EKEN

Özet—Muharebe sahasının sayısallaştırılması bugün bütün modern ordular tarafından uygulanmaya çalışılan bir faaliyettir. Siber tehdit ortamında muharebe sahasının sayısallaştırılmasının faydalarının yanında çeşitli mahzurları da bulunmaktadır. Muharebe sahası sayısallaştırılırken mahzurları da dikkate alınmalı ve siber tehdidi asgari seviyeye indirecek şekilde planlama yapılmalıdır.

Anahtar Kelimeler—Muharebe Sahasının Sayısallaştırılması, Siber Tehdit

Abstract—Today, battlefield digitization is a concept which has been tried to be applied by all modern armed forces. In a cyber threatened environment, battlefield digitization brings not only advantages but also disadvantages. While digitizing the battlefield, the disadvantages should also be taken into account and planned to minimize the cyber threat.

Index Terms—Battlefield Digitization, Cyber Threat

I. GİRİŞ

Muharebe sahasının sayısallaştırılması ve bilgi teknolojilerinin silahlı kuvvetler tarafından yoğun olarak kullanılmaya başlaması çağımızda olmazsa olmaz bir gereklilik olarak ortaya çıkmaktadır. Öte yandan bilgi teknolojilerindeki ilerlemeler yepyeni bir tehdit kavram meydana getirmiştir: siber tehdit. Bu makale muharebe sahasının sayısallaştırılması ve bilgi teknolojilerindeki ilerlemelerin siber tehdit ortamında kullanımı ve etkinliğini irdelemektedir.

II. SİBER TEHDİT ORTAMINDA MUHAREBE SAHASININ SAYISALLAŞTIRILMASI

A. Çalışmanın Amacı

Muharebe sahasının sayısallaştırılması kavramı ortaya çıktığında bugünkü gibi bir siber tehdit ortamı bulunmamaktaydı. Bugün bilgi teknolojilerindeki gelişmeler ve siber dünyada oluşan tehditler kapsamında muharebe sahasının sayısallaştırılmasının yeniden sorgulanması gerekmektedir. Bu çalışmada muharebe sahasının sayısallaştırılmasının siber tehdit ortamında fayda ve mahzurlarını ortaya koyarak güvenli bir sayısallaştırma için neler yapılabileceğini belirlemeyi amaçlamaktadır.

B. Muharebe Sahasının Sayısallaştırılması

Muharebe sahasındaki gelişmeler teknolojideki gelişmelere paralel olarak ilerlemektedir. Çift yönlü olan bu

ilişkide muharebe sahasının gereksinimleri kimi zaman teknolojiye önderlik etmiş, kimi zamanda muharebe sahası teknolojinin geldiği noktadan süratle istifade etmeye çalışmıştır. Bu yarışta öncülük eden ülkelerin silahlı kuvvetleri, bu sayede çok büyük bir kuvvet çarpanı oluşturmuşlardır. Son çeyrek yüzyılda internetle gelen bilgi aktarımındaki hız ve bilginin bu sayede eş zamanlı ve çok yönlü paylaşımı muharebe sahasının sayısallaştırılması kavramını ortaya çıkarmıştır.

Sayısallaştırma; sinyali bölerek ve ikili sayı sisteminde kod değerleri tahsis ederek herhangi bir bilginin ayrışık veya fasıllı sinyaller şeklinde kodlanmasıdır. Hepimizin sıklıkla duyduğu “0” ve “1” lerden oluşan bu dünyada sinyaller artık daha az karışıklığa maruz, daha uzağa gönderilebilir. Ancak bu özelliklerinin yanında sayısal sinyallerin belki de en önemli özelliği matematiksel algoritma kullanılarak bilgisayarlar tarafından işlenebilir olmasıdır. Bir veri sayısallaştıktan sonra bilgisayar ortamında işlenebilir bir veri haline gelir ve bilgisayarların gücü ve programcının hayal gücüne göre istenilen her şey bu verilerle yapılabilir. Bu nedenle yaşadığımız çağa sayısal bilgi çağı demek mümkündür. Sayısal bilgi; aldığımız tıbbi tedaviyi, banka hesaplarımızın güvenliğini, içtiğimiz suyun, yediğimiz yemeğin kalitesini, birbirimizle iletişim kurma kabiliyetimizi ve evlerimizi kışın sıcak, yazın soğuk tutmak için ihtiyaç duyduğumuz enerjiye erişimimizi kapsayacak kadar hayatın ayrılmaz bir parçası haline gelmiştir [1].

Sayısallaştırmanın getirdiği yeni dünyadan doğal olarak muharebe sahası da etkilenmiştir. Günümüzde gelişmiş bütün ülkelerin savunma sistemleri, ateş gücünü barındıran tank, uçak, gemi gibi sistemlerle; bu sistemlerin üzerindeki veya bu sistemleri destekleyen komuta kontrol, atış kontrol, muhabere, dost düşman tanıma vs. gibi tamamlayıcı savunma sistemleri olarak ikiye ayrılmaktadır. Tamamlayıcı savunma sistemleri sayısal kodlar sayesinde sayısal teknoloji ile geliştirilen ve yazılım kontrolünde çalışan yeni sistemlerle değiştirilmeye başlanmıştır ve buna “muharebe sahasının sayısallaştırılması” denilmiştir [2].

Muharebe sahasının sayısallaştırılması sayesinde bütün komuta kademelerinde taktik resmin elde edilmesi sağlanmış ve muharebe sahasının bilinmeyenleri azaltılmaya çalışılmıştır. ABD silahlı kuvvetlerinde özellikle otomasyon alanında muharebe sahasının sayısallaştırılmasına yönelik bu faaliyetler “Askeri Sistemlerde Çağdaş Devrim (ASÇD) (The contemporary Revolution in Military Affairs) olarak adlandırılmaktadır [3]. ABD Kara Kuvvetleri ASÇD faaliyetlerine ilk olarak 1978’te komuta kontrol sistemlerine yönelik olarak Sigma Star programıyla başlamış ve o günden beri de savaş kabiliyetlerini geliştirmeye devam etmektedir. Bu kapsamda ABD Kara Kuvvetlerinin ilk sayısallaştırılmış birlikleri mekanize birlikler olmuştur. Meskûn mahallere yönelik olarak bazı piyade birliklerinde kısmi sayısallaştırma

Selçuk DAL, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: selcuk2001@gmail.com.
Eşref FIRAT, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: esreffirat2001@gmail.com.
Serbülen EKEN, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: serbulenteken@gmail.com.

faaliyetleri olsa da ABD Kara Kuvvetleri sayısallaştırma konsepti ağır mekanizbirlikler üzerine kurulmuştur.

(I) Sayısallaştırmanın Faydaları (Şekil 1)

Bu tür birliklerde sayısallaştırmanın en önemli faydalarından birisi bazı birliklerin lağvedilmesi, genel olarak da ihtiyaç duyulan personel ve malzeme oranında da ciddi biçimde azalmadır. Buna karşın bir tümenin etki alanı, sayısallaştırmanın kazandırdığı imkân ve kabiliyetlerle 10.000 km² den 24.000 km² ye çıkmıştır [4]. Sayısallaştırma sayesinde askeri literatüre “hassas angaje” kavramı girmiştir. Artık birlikler çok uzak mesafelerden düşmanı hassas olarak ateş altına alabilmekte, hem personel hem de malzeme zayıyatı azalmaktadır. Sayısallaştırmanın bir diğer avantajı da kazandırdığı üstün hız sayesinde kendi içinde çok organize, hızlı hareket eden birliklerle caydırıcı savaşlar yaratmasıdır [3]. Ancak sayısallaştırmanın getirdiği en önemli fayda şüphesiz ki bilgi üstünlüğüdür. Askeri teorisyenlere göre bilgi üstünlüğünün getirdiği üç avantaj [3] bulunmaktadır. Birincisi, düşman, arazi ve kendi kuvvetlerimiz hakkında doğru, tam ve gerçek zamanlı bilgi vererek durumsal farkındalığı artırmaktadır. İkincisi, durumsal farkındalık sayesinde Calusewitz’in bahsettiği “savaşın sis perdesi” [5] büyük ölçüde dağılmakta ve her seviyedeki her asker, savaşın her aşamasında taktik resmi elde edebilmektedir. Üçüncüsü, bu bilgi üstünlüğüne sahip olan kuvvetler düşman kuvvetlerinin ne şekilde hareket edeceğini tahmin edebilmektedirler.



Şekil 1. Muharebe Sahasının Sayısallaştırılmasının Faydaları

(II) Siber Tehdit

Bilgi teknolojilerindeki gelişmeler bugün neredeyse her bireyi en az bir, hatta birden fazla bilgisayar sahibi yapmıştır. Yapılan araştırmalara göre dünya üzerinde iki milyardan fazla kişiye pek çoğu internete bağlı kişisel bilgisayar bulunmaktadır [6]. Küçük birer kişisel bilgisayar olan ve hemen hemen onların yaptığı her şeyi yapan cep telefonlarının sayısı ise yaklaşık 6 milyardır [7]. Bütün devlet kurumları da bir şekilde çevrim içi yapılarla sistemlerini internete bağlamaktadırlar. Bu sayede birbirine bağlı bu yapıda, sınırlar kaybolmakta ya da belirsizleşmekte, bu okyanusun içinde ada olarak kalan bilgisayarların sayısı ise çok azalmaktadır [8].

2007 yılında Baltık ülkelerinden birinde yaşanan siber taarruz [9], 2008 yılında Karadeniz ülkelerinden ikisi arasında yaşanan savaş öncesi yapılan siber taarruz [9] ve bir ülkenin nükleer araştırma merkezlerinde ortaya çıkan “stuxnet” virüsü [10] bize bilgi teknolojilerindeki

gelişmelerin aynı zamanda nasıl bir siber tehdit dünyası oluşturduğu hakkında da fikir vermektedir. Çağımızda bilgisayarların vazgeçilmez unsurlar olarak –çamaşır makinelerinden nükleer başlıklara kadar- her türlü sistemin içinde bir şekilde yer alıyor olması hayatımızı kolaylaştırdığı kadar aynı zamanda yanlış emellerle kullanıldığında bunların birer tehdit olarak kullanılması olasılığını da gündeme getirmiştir.

2007 yılında bir Baltık ülkesinin yaşadığı da tam olarak siber bir kâbustur. Yurt çapında bedava sınırsız internetin olduğu, dünya çapında e-devlet sistemine ilk geçen ve ekonomisini internet ve bilgi sistemleri üzerine oturtmuş olan bu ülke, bir alışveriş merkezi önüne konan işgalci bir ülke döneminden kalma bir anıtın kaldırılması üzerine haftalar süren bir siber taarruza maruz kalmıştır. Bu taarruzda ilk önce devlet kurumlarının haber sistemleri, sonra bütün medya sonra da bankalar hedef alınmıştır. Büyük bir panik havası yaşayan servis sağlayıcılar sistemlerini yeniden başlatmak zorunda kalmış ve ülkenin bilgi teknolojilerindeki ünü bir anda yerle bir olmuştur [11]. Çevrimiçi sistemlerin ne kadar güvensiz olduğu böylece anlaşılmıştır.

Çevrimdışı sistemlerin çevrim içi olmaması yönüyle güvenli oldukları söylenebilir mi? Bu konuda verilebilecek en iyi cevap meşhur “stuxnet” virüsüdür. Nükleer geliştirme merkezlerindeki trafoların aşırı derecede ısınmasını sağlayarak patlamalarını sağlayan bu virüs hiçbir ağa bağlı olmayan bu sisteme bir şekilde sızmış ve siber taarruz bakımından harika bir iş çıkararak yeni bir çağır açmıştır [12]. Peki çevrimdışı bir sisteme nasıl oldu da bir virüs bulaşabilir? Cevabı tam olarak bilinmese de virüsün bir taşınabilir bellek vasıtasıyla bulaştığı tahmin ediliyor. Şayet durum böyleyse çevrimdışı olduğu için güvende olduğu düşünülen pek çok sistemin aslında o kadar da güvenilir olmadığı, istenildiği takdirde bir şekilde saldırıya maruz kalabileceği söylenebilir.

(III) Siber Tehdit Ortamında Bilgi Teknolojilerindeki Gelişmelerin ve Muharebe Sahasının Sayısallaştırılmasının Mahzurları

Muharebe sahasının sayısallaştırılmasının daha önce bahsedilen pek çok avantajının yanında çeşitli mahzurları da olduğu görülmektedir. Bu mahzurları; sayısallaştırmanın tahakkuku ve idamesi için çok sayıda yüklenici veya taşeron sivil firmadan faydalanma zorunluluğu, bazı komuta kademelerinin kaybolması ve karar verme zaafiyeti, ağ yönetiminde ortak bir doktrin oluşturma gerekliliği, asimetrik tehdide sebebiyet vermesi, iletişimin sekteye uğraması ya da istismar edilmesi ve sayısal sistemlerin ele geçirilmesi olarak sıralamak mümkündür [3] (Şekil 2).

Muharebe sahasının sayısallaştırılması adına yapılan bütün faaliyetler ancak ve ancak çok daha fazla sayıda sivil firmanın eliyle yapılabilmektedir. Örneğin, bugün TSK'nin iletişim alt yapısını oluşturan TAFICS sistemi ASEL SAN firmasının ana yükleniciliği altında 3 firmanın katılımıyla gerçekleştirilmiştir. Sivil firmalara olan bu derece bir bağımlılık harp zamanında değişik komplikasyonların oluşmasına sebebiyet verebilecektir. Her ne kadar sivil de olsalar askeri sistemlere verecekleri destek bu kişileri savaş zamanında savaş hukuku bakımından hedef haline getirebilecektir. Bu nedenle gerçek bir savaş zamanında bu kişilerin nasıl

davranacağını, kesintisiz bir biçimde hizmet vermeye devam edip edemeyeceği tam olarak belli değildir. Bu da mevcut yapıda bütün sayısallaştırma faaliyetlerinin üzerine bina edildiği TAFICS iletişim alt yapısı adına ciddi bir zafiyet olarak önümüze çıkmaktadır.



Şekil 2. Muharebe Sahasının Sayısallaştırılmasının Mahzurları

Sayısallaştırmanın bir başka mahzuru da taktik resmin her kademe tarafından rahatlıkla görülebilmesi sayesinde ara kademe komuta ihtiyaçlarını ortadan kaldırmasıdır. İlk bakışta olumlu gibi görünen bu merkezileşmenin, dikkatli bakıldığında karar verme yetisine sahip komutanların yetişmesi adına büyük bir zafiyet olduğu görülecektir. Çünkü komutanlar ancak her kademede görev yaptıktan sonra bulunduğu konumun gereğini yerine getirecek bilgi ve tecrübeye sahip olurlar. Hâlbuki muharebe sahasının sayısallaştırılması ile küçük birlik komutanları daha fazla önlerindeki ekranlara bağımlı, dış çevredeki ipuçlarını daha az değerlendirebilir hale gelmektedirler [3]. Ara komuta kademelerinin de kaybolmasıyla bu imkân bile yeterince sahip olamayan komutanlar ileride daha büyük sorunları çözmek ve daha zor kararlar vermek gerektiren komuta kademelerine gelerek bir karar zafiyeti oluşturabileceklerdir.

Silahlı kuvvetlerin çok daha fazla müşterek ve birleşik harekâtı icra etmeye yönelik ortaya çıkan ihtiyaçlar kapsamında, sayısallaştırmanın karşılaşılabilecek bazı problemler olacağı aşikârdır. Çünkü bütün kuvvetlerin gerek personel gerek malzeme gerekse kurumsal kültür bakımından çeşitli farklılıkları bulunmaktadır. Bu nedenle daha fazla sayısallaştırma daha fazla aynı dili konuşmaya ve ortak doktrine ihtiyaç manasına gelmektedir. Gerek mevcut yapının gerekse gelecekte inşa edilecek yapıların mutlaka bu kapsamda ele alınması gerekecektir.

Öte yandan muharebe sahasının sayısallaştırılmasını başarıyla ifa eden birlikler karşısında, hiç bir düşman kuvveti bulunmak istemeyecektir. Kilometrelerce öteden hassas angaje ile ateş altına alma kabiliyeti olan bir güce karşı kim konvansiyel bir şekilde açık arazide karşı koymak ister? İşte bu nedenle muharebe sahasını sayısallaştırabilmiş güçler karşısında ya en az onların kadar sayısallaştırmayı başarabilmiş ya da asimetrik bir güç karşı koyabileceklerdir. Bu bakış açısıyla sivil kıyafetler içinde bir zırhlı taşıyıcıya 5 m. uzaklıkta bulunan bir düşman askeri 1000 m. deki bir tanktan daha zararlı olabilir. Özellikle meskun mahallerdeki muharebeler sayısallaştırma konseptinin çok uzağında cereyan etmektedir. Böylece sayısallaştırılmış birlikler bu tür muharebelerde etkinliklerini yeterince gösterememektedirler.

Bu tür bir asimetrik muharebe anlayışı ise sayısallaştırmadan beklenen hemen hemen her şeyi boşa çıkarabilecek kadar tehlikelidir [3].

Muharebe sahasının sayısallaştırılması çerçevesinde en önemli unsur iletişim olarak karşımıza çıkmaktadır. Sayısallaştırılmış birliklerde taktik resmin elde edilmesi, emirlerin iletilmesi, ihtiyaçların tespit edilmesi, ikmal faaliyetlerinin icra edilmesi gibi pek çok hayati önemi haiz faaliyet hep iletişim kanalları üzerinden gerçekleştirilmektedir. Dolayısıyla bu iletişim kanallarının çalışması sekteye uğradığında ya da uğratıldığında sonuç bu tür birlikler için bir faciaya dönüşmektedir [13]. İletişim kanallarının sekteye uğraması doğal koşullar nedeniyle (kötü hava koşulları, arazideki engeller vs.) olabileceği gibi suni nedenlerle (elektromanyetik yayım, karıştırma vs.) de olabilmektedir. Her iki halde de sayısallaştırılmış bilgiye tabi olan dost unsurlar böyle bir durumda çok yakınına kadar gelen bir düşman unsurunu göremeyecek veya bu nedenle dost ateşine maruz kalma ihtimali artabilecektir. Ancak tek endişe edilen şey iletişim kanallarının sekteye uğraması değildir. İletişimin ele geçirilerek yanlış bilgi üretilmesi ise şüphesiz daha büyük bir tehlikedir.

Bütün bir harekâtı icra ederken dost birliklerin güvendiği en önemli şey eldeki bilgilerin doğruluğudur. Muharebe sahasının sayısallaştırılması da daha önce ifade edildiği gibi zaten düşman, arazi ve mevcut kuvvetler hakkındaki bilgilerin doğruluğunu artırmak için ortaya konulmuş bir sistemdir. Peki ya elimizdeki bilgiler doğru değilse? O zaman en iyi senaryo ile hiç kuvvet ayırmamanız gereken yere kuvvet ayırırsınız en kötü senaryo ile de hiç düşman ateşine maruz kalmaksızın ekranınızda dost unsurların düşman olarak görünmesiyle dost ateşleriyle birlikleriniz imha olur. Peki bu nasıl mümkün olabilir? Sayısallaştırma işleminin her aşamasında mutlaka bir takım algoritmalar, bilgisayarlar veya işlemcisi, belleği olan bilgisayar benzeri yapılar kullanılmaktadır. Bu nedenle bu tür yapıların gerek çevrimiçi gerekse çevrimdışı yollarla (virüs, truva atı, sniffer, kötücül yazılımlar vs.) ele geçirilmesi ihtimali bulunmaktadır.

III. SONUÇ

Bilgi teknolojilerindeki gelişmeler kapsamında muharebe sahası daha fazla sayısallaşmaya başlamıştır. Muharebe sahasının sayısallaştırılması karar vericilere tüm komuta kademelerinde taktik resmin sağlanması, yüksek bir hız ve hassas angaje imkanını kazandırmıştır. Bu tür sayısallaştırılmış bir birlik için etki alanı artmış ve muharebe sahasının bilinmeyenleri azalmıştır. Ancak bu faydaların yanında muharebe sahasının sayısallaştırılmasının siber tehdit ortamını da dikkate alarak getirdiği bir takım mahzurlar da bulunmaktadır. Bu mahzurları, sayısallaştırmanın tahakkuku ve idamesi için çok sayıda sivil firmadan faydalanma zorunluluğu, bazı komuta kademelerinin kaybolması ve karar verme zaafiyeti, ağ yönetiminde ortak bir doktrin oluşturma gerekliliği, asimetrik tehdide sebebiyet vermesi, iletişimin istismar edilmesi ve sayısal sistemlerin ele geçirilmesi olarak sıralamak mümkündür.

Gelişmiş ülkelerin silahlı kuvvetleri artan bir hızla muharebe sahasını sayısallaştırma faaliyetlerine devam etmektedirler. Günümüzde teknolojinin imkânlarını

kullanmayan bir ordunun muharebelerde başarılı olmasını düşünmek imkânsızdır. Adeta bütün doktrinler, elde edilen sayısallaştırma faaliyetleri ölçüsünde bir değişim göstermektedir. Ancak siber tehdit göz önünde bulundurulmadan sarf edilen muharebe sahasını sayısallaştırma çabaları getirdiği faydadan daha fazla mahzur doğuracaktır.

KAYNAKLAR

- [1] <http://www.northropgrumman.com/MediaResources/Presentations/2013/Pages/052113MikePapayCyberThreatsandSecuritySolutions.aspx> erişim tarihi 11.07.2013.
- [2] TÜBİTAK Savunma Havacılık ve Uzay Sanayi Panel Raporu 2003, s.6.
- [3] Mitchell, Elizabeth a. Stanley, Technology's Double-Edged Sword:The Case of US Army Battlefield Digitization, Defense Analysis Vol.17, No.3, 2001, s.267-280.
- [4] Battlefield Automation, United States General Accounting Office, 2000 s.15.
- [5] Clausewitz, Carl von, Savaş Üzerine, Çev. Şiar Yalçın, İstanbul, Spartaküs Yayınları, 1997, Kitap II, Bölüm 2, Altbölüm 24.
- [6] State of the Future 2012 Report, (Executive Summary) <http://www.millennium-project.org/millennium/SOF2012-English.pdf> erişim tarihi 11.07.2013.
- [7] <https://www.cia.gov/library/publications/the-world-factbook/geos/xx.html> erişim tarihi 10.01.2013.
- [8] Libicki, Martin C., Cyberdeterrence and cyberwar, RAND, 2009, s.4.
- [9] Moore, Ryan J., Prospects For Cyber Deterrence, NPS, Monterey, 2008, s.27, 54.
- [10] Shanker Tom, Sanger David, U.S. Suspects Iran Was Behind a Wave of Cyberattacks, New York Times, Washington, 13 Ekim 2011.
- [11] Mansfield, Steve, Estonia:What doesn't kill you make you stronger., Network security,2012, s.12.
- [12] Farwell, James P.-Rohozinski Rafael, Stuxnet and the Future of Cyber War, Survival vol.53. no.1,2011, s.24.
- [13] Finley, Dorothy, Handling degraded communications, Military Review,2001, s. 33.

Selçuk Dal Kara Harp Okulundan 2001 yılında Sistem Mühendisi diploması aldı. 2004-2006 yılları arasında Naval Postgraduate School Monterey, California ABD'de Manpower Systems Analysis bölümünde yüksek lisans eğitimini tamamladı. Halen Kara Harp Akademisinde eğitim görmektedir.

Eşref Fırat Kara Harp Okulundan 2001 yılında Sistem Mühendisi diploması aldı. 2005-2007 yılları arasında Konya Selçuk Üniversitesinde Halkla İlişkiler Bölümünde yüksek lisan eğitimini tamamladı. Halen Kara Harp Akademisinde eğitim görmektedir.

Serbülent Eken Kara Harp Okulundan 1997 yılında Sistem Mühendisi diploması aldı. Kara Harp Akademisinde yüksek lisans eğitimine müteakip halen Kara Harp Akademisinde öğretim elemanı olarak görevine devam etmektedir.