BİLGİ TEKNOLOJİLERİ VE İLETİŞİM DERGİSİ (BTK DERGİ)
CİLT: 1 SAYI: 1 TARİH: TEMMUZ - EYLÜL 2023 ISSN: 2980-1311

KİTAP İNCELEMESİ
ALİ BURAK DARICILI, "SİBER UZAY VE SİBER GÜVENLİK: ABD VE RUSYA FEDERASYONU'NUN SİBER GÜVENLİK STRATEJİLERİNİN KARŞILAŞTIRMALI ANALİZİ", 2017, 320 SAYFA, DORA YAYINCILIK: BURSA

Arş.Gör.Erva KARADAĞ[1]

Yaklaşık on beş yıl boyunca Millî İstihbarat Teşkilatı çatısı altında çeşitli yurt içi ve yurtdışı görevler üstlenen, şu an Bursa Teknik Üniversitesi'nde görev yapan Doç. Dr. Ali Burak Darıcılı, 2017 yılında Uludağ Üniversitesi'nde hazırladığı doktora tezini, aynı yıl *"Siber Uzay ve Siber Güvenlik: ABD ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi"* başlığıyla kitaplaştırarak akademi dışı okuyucunun da ilgisine sunmuştur. Darıcılı, siber uzay ve siber güvenlik çalışmalarının bilgi/bilişim teknolojilerinin sınırları içerisinde kalan salt "teknik" bir alan olduğuna yönelik dar kapsamlı değerlendirmelerden farklılaşarak, bu alanda meydana gelen değişim, dönüşüm ve gelişmelerin birey-kurum-devlet-uluslararası sistem olmak üzere farklı analiz düzeyinin güvenliğine yönelik dikkat çekici etkisine vurgu yapmaktadır. Bu bağlamda çalışma, geleneksel savaş ve çatışma alanlarının yanı sıra siber uzayda da birbirleriyle rekabet halinde olan ve çatışan, siber uzayın başat aktörleri olan Rusya ve Amerika Birleşik Devletleri'nin siber güvenlik stratejilerini neo-realist perspektiften mercek altına almaktadır.

Dört bölümden oluşan çalışmanın "Reel Politik Paradigmanın Uluslararası İlişkiler Disiplininde Kurumsallaştırılması" başlığını taşıyan ilk bölümünde, çalışmanın kavramsal ve teorik altyapısı inşa edilmiştir. Uluslarası İlişkiler'in başat teorilerinden klasik realizm ve neo-realizmin disiplin içerisindeki yeri, temelleri

[1] Arş.Gör.Erva KARADAĞ, Milli Savunma Üniversitesi, Alparslan Savunma Bilimleri ve Milli Güvenlik Enstitüsü, Güvenlik Araştırmaları Anabilim Dalı, ekaradag@kho.msu.edu.tr, ORCID: 0000-0001-5901-9572

ve savları, bu teorilerin güvenlik kavramına bakışları değerlendirilmiş, siber uzay ve siber güvenliğin kavramsal çerçevesi çizildikten sonra, Joseph Nye'nin güç tipolojisi ve güç difüzyonu yaklaşımları bağlamında ele alınmıştır., Bu bölümde ortaya konan argüman, siber uzayda yaşanan gelişmelere paralel olarak tehditlerin çeşitlendiği ve belirsizleştiği; bu durumun uluslararası sistemi hiç olmadığı kadar anarşik, güvensiz bir hale dönüştürdüğü ve siber uzayın getirdikleriyle devletlerin bu alanda da tehditleri bertaraf etmeye muktedir başat aktörler olarak rol ve sorumluluklarının pekiştiğidir.

"Amerika Birleşik Devletleri'nin Siber Güvenlik Stratejisinin Analizi" başlıklı ikinci bölümde bu stratejinin inşasında önemli rol oynayan başta ABD Savunma Bakanlığı, ABD İç Güvenlik Bakanlığı ve ABD istihbarat topluluğunda yer alan Federal Araştırma Bürosu (FBI) ile Merkezi Haber Alma Örgütü (CIA) olmak üzere ilgili kurum/kuruluşlar, federal ve eyalet seviyesinde hazırlanan başta yasalar olmak üzere çeşitli yasal düzenlemelerden müteşekkil hukuki altyapı ve stratejiyi ortaya koyan başkanlık emirleri, direktifler, resmi belge, doktrin ve planlar detaylı bir biçimde ele alınmıştır. Ek olarak Edward Snowden vakası, Wikileaks sızıntısı ve 2016 ABD Başkanlık Seçimlerini etkilemeye yönelik Rusya Federasyonunca düzenlendiği iddia edilen siber faaliyetler gibi örnekler incelenmiştir.

"Rusya Federasyonu'nun Siber Güvenlik Stratejisinin Analizi" başlıklı üçüncü bölümde, bir önceki bölüm ile paralel olarak Rusya Federasyonu'nun siber güvenlik konseptinin kavranabilmesi açısından Rus siber alanının temel özellikleri, başta Rus Askeri İstihbarat Direktörlüğü (GRU), Rus İstihbarat Servisi (SVR) ve Rus Federal Güvenlik Servisi (FSB) gibi istihbarat kuruluşları başta olmak üzere ilgili kurum/kuruluşların siber kapasitesi, çeşitli güvenlik doktrinleri, prensip ve konseptler, stratejik güvenlik belgeleri ile resmi dokümanlar detaylı bir incelemeye tabi tutulmuştur. İç politikada ortaya konan yol gösterici mahiyetteki bu belgelerin yanı sıra Rusya Federasyonu'nun siber güvenlik temelli işbirliği hedefleri kapsamında attığı adımlar, Birleşmiş Milletler'den Şangay İşbirliği Örgütü'ne kadar çeşitli uluslararası ortamda yürütülen diplomasi faaliyetleri ve başta Çin Halk Cumhuriyeti ile olmak üzere diğer devletlerle ortaya konan girişimler değerlendirilmiştir. Ayrıca Rus istihbarat servislerince gerçekleştiği iddia edilen çeşitli ülkeler, şirketler ve kritik altyapıların hedef alındığı siber saldırı ve espiyonaj vakalarının yanı sıra da yakın mercek altına alınmıştır. Bu bölümün temel argümanı, Rusya Federasyonu'nun siber uzayda hukuki, bürokratik ve teknolojik ge-

lişmelere paralel olarak sahip olduğu siber kapasite ve gücü alaka ve menfaatleri çerçevesinde, legal veya illegal yollar aracılığıyla, enformasyon savaşı ile destekli bir baskı ve zorlama aracı olarak kullandığıdır.

"Amerika Birleşik Devletleri'nin ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırılması" başlıklı dördüncü ve son bölüm ile, Soğuk Savaş'tan günümüze kadar Amerika Birleşik Devletleri'nin ve Rusya Federasyonu'nun siber alandaki rekabeti gerek pratik, gerek kurumsal, gerekse bağlamsal olarak ortaya konulmuştur. Pratik boyutta çalışma, Sputnik II'den ARPA-ARPANET-MILNET ağ projesine, Rus Askeri İşlerde Devrim (RMA) projesinden Amerikan Yıldız Savaşları Projesi'ne ve Soğuk Savaş'ın sona ermesinin ardından yürütülen siber saldırılar, siber operasyonlar ve enformasyon savaşına değin iki ülke arasındaki rekabet karşılaştırmalı olarak ele alınmıştır. Bağlamsal boyutta çalışma, Amerika Birleşik Devletleri'nin ve Rusya Federasyonu'nun siber alandaki rekabetinin resmi doküman, strateji ve doktrinlerin içerik analizini ortaya koymaktadır. Söz konusu analiz neticesinde her iki ülkenin siber uzay ve siber güvenlik stratejilerinin benzeşen, farklılaşan, çatışan ve uyuşan tarafları değerlendirilmiştir. Kurumsal boyutta ise Amerika Birleşik Devletleri'nin başta ABD Savunma Bakanlığı, ABD İç Güvenlik Bakanlığı ve ABD istihbarat topluluğunda yer alan Federal Araştırma Bürosu (FBI) ile Merkezi Haber Alma Örgütü (CIA) ve Rusya Federasyonu'nun Rus Askeri İstihbarat Direktörlüğü (GRU), Rus İstihbarat Servisi (SVR) ve Rus Federal Güvenlik Servisi (FSB) gibi siber güvenlik organizasyon yapıları karşılaştırmalı olarak mercek altına alınmıştır.

Sonuç olarak, siber uzay ve siber güvenlik düzlemlerini uluslararası güvenlik ve dış politika ekseninde inceleyen; bu alanları Rusya Federasyonu ve Amerika Birleşik Devletleri vakaları üzerinden ele alan bu çalışma, uluslararası ilişkiler ve bilgi/bilişim teknolojileri perspektiflerini bir araya getiren interdisipliner yönüyle dikkat çekmektedir. Bu yönü ile çalışmanın teknik bilimlerden sosyal bilimlere, akademik çevrelerden popüler/akademi dışı çevrelere, geniş bir okuyucu kitlesine hitap etmesine olanak sağladığı değerlendirilmektedir.

KAYNAK:

DARICILI A. B. (2017). Siber Uzay ve Siber Güvenlik: ABD ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi. Dora Yayıncılık, Bursa