SİBER GÜVENLİK TEMELİNDE KRİTİK ALTYAPILAR VE HAZAR HAVZASI

Article · December 2016

DOI: 10.17719/jisr.2016.1373

CITATIONS
0

READS
191

1 author:

Hülya Kınık
Karadeniz Technical University
2 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Uluslararası Sosyal Araştırmalar Dergisi
The Journal of International Social Research
Cilt: 9 Sayı: 47 Volume: 9 Issue: 47
Aralık 2016 December 2016
www.sosyalarastirmalar.com Issn: 1307-9581

SİBER GÜVENLİK TEMELİNDE KRİTİK ALTYAPILAR VE HAZAR HAVZASI

CRITICAL INFRASTRUCTURES AND CASPIAN BASIN WITH THE SUBJECT OF CYBER SECURITY

Hülya KINIK*
Vahit GÜNTAY**

Öz

Bölgesel çalışmalar ve uluslararası ilişkiler temelindeki yaklaşımlar, gelişen alan çalışmalarını farklı düzeyleriyle karşımıza çıkarmaktadır. Bu düzeyler adına önemli bir temeli oluşturan siber güvenlik ve özelindeki kritik altyapılar, devletler arası politik girişimlerde tartışılagelen bir husus haline gelmiştir. Bunun en temel noktalarından birisi siber alana artan bağımlılık ve enerji nakil hatlarının bir dizi veriyle çıkar mücadelesine konu olmasıdır. Hazar Havzası özelinde değişen dengeler, uluslararası ilişkiler adına hukuksal bazı gelişmeleri karşımıza çıkarırken, bu gelişmeler siber alandaki mücadeleyi de gözler önüne sermiştir. Bu durumun en önemli göstergesi, bölgenin enerji nakil hatlarındaki önemi ve bu hatların siber alanda teknolojik altyapılara entegresi olmuştur. Bu gelişmeler dahilinde uluslararası güvenliğin önemli ayağını oluşturan siber güvenlik çerçevesinde kritik altyapılar ve bu altyapılar üzerinden çıkar mücadelesi, bölge devletlerinin ilgi alanını bu düzeye kaydırmaya başlamıştır. Bölgesel çekişmeler de bunun en önemli ispatıdır. Çalışma dahilinde Hazar'ın hukuksal statüsü uluslararası güvenlik açısından analiz edilerek siber güvenlik yaklaşımı açısından bir kurgu oluşturulmuştur. Bu analizin boyutu teorik ve kavramsal bir temelle desteklenerek yaklaşımın anlaşılabilirliği yönünde çaba sarfedilmiştir. Siber alanın artan yoğunluğu dahilinde, çalışma içerisinde oluşturulmak istenilen farkındalık açıklayıcı bir şekilde ele alınmıştır.

Anahtar Kelimeler: Uluslararası İlişkiler, Siber Güvenlik, Kritik Altyapılar, Hazar Havzası.

Abstract

Regional studies and approaches with the subject of international relaitons have some developments with different levels at area studies. Cyber security and its sub-title critical infrastructures which is the main basis of these levels, has become a discussion subject at political initiatives within inter states. One of the main point of this issue is dependency to cyber area and interest conflict of energy transmission line with a range of data. Changing balances at Caspian Basin have some developments at international relations with its legal effect and these developments have revealed a conflict at cyber area. The most important indicator is region's importance at energy transmission lines and integration of these lines to technological infrastructures at cyber area. With these developments, cyber security as an important subject at international relations with the frame of critical infrastructures and interest conflict, have attracted region states' interest to this level. One of the best proof is current regional developments. In this study, Caspian Region's legal status is analysed with the respect of international security and constituted a frame with cyber security approach. The dimension of the analysis is supported with theoretical and conceptual base for understanding the frame. Within the increasing intensity of cyber area, main theme is evaluated with explanatory way.

Keywords: International Relations, Cyber Security, Critical Infrastructures, Caspian Basin.

Giriş

Uluslararası ilişkiler temelindeki çok boyutlulukla birlikte "*siber politikalar*" adı altında çalışma aritmetiği bulan siber güvenlik, siber saldırılar ile birlikte yeni bir çalışma alanını karşımıza çıkarmıştır. Ulus devletlerin veya bu düzeyde tartışma niteliği gösteren güncel çalışmalar siber güvenlik konseptine ve özüne atıflarda bulunmaktadır. *Askeri işlerde ve gelişmelerde devrim* olarak adlandırılan bu durum elektronik, ileri teknolojik savaş unsurlarının ortaya çıkmasıyla çok boyutlu bir paradoks haline dönüşmüştür.

Teknolojik değişim ve algısal boyutu kritik altyapıların, iletişim sistemlerinin ya da özelde hava savunma sistemleri gibi birçok unsurun tehlikede olması ve caydırıcı bir özellik kazanması, siber güvenliği önemli bir analiz düzeyine taşımaktadır. Bu düzeyin getirmiş olduğu farklılık özellikle hukuksal bütünlük dahilinde tartışılması ve ele alınması zor bir alanı da karşımıza çıkarmaktadır. Siber savaş kavramı ve bu savaş türü etrafında tartışılan konular enerji koridorları, enerji nakil hatları ve araştırma sonuçlarında elde edilen verilerin istihbaratı konusunda genişlemeye devam etmektedir. Her ne kadar siber savaş belli yönleriyle asimetrik çatışmalara benzetilse de bu durumun güçleştiği noktalar Hazar Havzası gibi bölgelerde hem enerji boyutunda, hem de hukuksal statülere ilişkin süreçlerde tartışılagelmektedir. Siber savaş sadece saldırı unsurlarıyla ele alınan ve bu durumun tartışıldığı bir boyut değildir. Aynı zamanda kritik altyapıların tehdidi ve bu tehdidin oluşturduğu caydırıcılık ile ilgilidir.

* Arş. Gör., KTÜ, İİBF, Uluslararası İlişkiler Bölümü, Trabzon. E-posta: hulya.ercan@ktu.edu.tr
** Arş. Gör., KTÜ, İİBF, Uluslararası İlişkiler Bölümü, Trabzon. E-posta: vahitguntay@gmail.com

Siber güvenliğin getirmiş olduğu ve kritik altyapılarla birlikte oluşan tehditsel süreç farkındalık oluşturulmasında önemli bir basamaktır. Siber alanda gelişen ya da gelişme arzusu içinde olan devletlerin çevre ülkelerle olan ilişkileri, belli farkındalıkların oluşturulmasıyla güvenlik stratejilerinin uygulanmasına dönük olarak da işleyecektir. Bu stratejilerin seçiminde ve bir yaklaşıma dönüştürülmesinde uluslararası hukuk kuralları geçerli olacaktır. Hazar'ın temelde kimi zaman statüsel sorunları, kimi zaman enerji koridorlarındaki varlığı ve çıkar mücadelesi siber güvenlik alanında, uluslararası hukuk bütünlüğünde değerlendirilecektir.

Çalışmanın konseptini oluştururken dikkat edilen husus, uluslararası hukuk ve Hazar Havzası'nın hukuksal statüsünün yer aldığı bir bakış açısıyla uluslararası güvenlik sorunsallarından biri olan siber güvenlik ve onun özelindeki kritik altyapıları incelemek olmuştur. Siber savaş temelinde anlaşılması gereken en önemli nokta, yürütülen harekat biçiminin sadece veri trafiğini engelleme ya da kötücül yazılımlarla zarara uğratma noktasında bir eylem olmadığı gerçeğidir. Bu gerçekliği uluslararası ilişkilerin çatışmalı olduğu bir çok noktada görmekteyiz. Kimi zaman veri trafiğinin yönetildiği ve siber alana bağlı olan enerji nakil hatlarının işleyemez hale getirilişi ya da kalıcı zararlar bırakılması, kimi zaman bu hatların tamamen yok edildiği ve örneklerinin görüldüğü uluslararası sistem kendi dinamiklerini Hazar Havzası adına hissettirmektedir.

Hazar Havzası ve kritik altyapılarının değerlendirilmeye çalışıldığı araştırmalar bütünü, uluslarası ilişkiler yaklaşımında aktörlerin sadece bölge devletleri olmadığını da göstermektedir. Sınırı ve ticari bir boyutta ilişkisi olmayan devletler, uluslararası şirketler konunun her ayağında yer almak istemektedirler ve farklı çalışmalar, raporlarla bölgeye ilişkin analizler sunmaktadır. Gerek teorik, gerekse pratik boyutun tarıtışıldığı Hazar Havzası bu yönüyle yakın gelecekte ciddi bir çekişme alanı olacağını ispatlamıştır. Dünyada sadece belirli ve özel birtakım bölgelerin bu türden raporlarla değerlendirildiği uluslararası sistem adına Hazar Havzası, siber alandaki mücadele adına önemli bir merkez haline dönüşmüştür ve bu konuda farkındalığın artırılması gerekmektedir.

Enerji koridorunun Avrupa ve Orta Doğu ayağında, Hazar Havzası'na yakınlığıyla önemli birtakım göstergelere sahip olan Türkiye için de konunun önemi ortadadır. Çalışmanın konsepti ve yaklaşımsal olarak kritik altyapılara ilişkin tespitler Türkiye gibi ülkeleri doğrudan ilgilendirmektedir. Siber alanda gelişim gösteren bölge coğrafyası için *siber savaş* kavramı Hazar Havzası gibi bölgeler adına hem hukuksal olarak, hem de siber savaş gibi konularda ciddi bir mücadele alanıdır ve bu alanın dışında kalan ülkeler kritik altyapılar açısından, enerji nakil hatları bağlamında ciddi sorunlar yaşamaktadır.

Çalışma kapsamında açıklayıcı bir analiz yapılarak siber güvenlik ve kritik altyapılar ile igili kavramsal bir çerçeve çizilmiş, uluslararası güvenliğin yükselen bir temasına ilişkin tespitler yapılmıştır. Daha sonra Hazar Havzası'nın hukuki statüsü değerlendirilerek uluslararası güvenlik açısından bir yaklaşım sergilenmiştir. Son olarak bölgeye ilişkin enerji özelinde ve siber alanda tespitler yapılarak kritik altyapılara yönelik değerlendirmeler yapılmıştır.

1. Uluslararası Güvenlik Açısından Siber Güvenlik ve Kritik Altyapılar

Uluslararası ilişkilerin doğası temel olarak uluslararası alandaki olayların ortaya çıkış şekilleri ve sebepleri üzerinde durmaktadır. Pek çok teorisyen egemen devletlerarasındaki ilişkiler hakkında fikirler öne sürmüşlerdir. Temel olarak amaçları, devletlerarasındaki ve içindeki siyasi etkileşimin modellerini anlayabilmek olmuştur. Bu teorisyenlerden bazıları geçmiş olayları açıklama ve gelecekle ilgili öngörülerde bulunarak teorik modellemeler üretme ve bu modeller vasıtasıyla genel ilkeler çıkarma çabası içine girmiştir.

Bu modellemeler tartışılırken savaş ve barış, sınırlar ile güç ilişkileri temel paradigmalar halinde belli başlı sorular olarak uluslararası ilişkilerin doğasını yoğurmuştur. Teknolojideki hızlı değişme, devletlerarası ilişkilerde büyük gelişmelere yol açmıştır. Uluslararası alanda savaş ve siyaset biçimlerinin de değişmesine neden olmuştur (Knutsen, 2006:346). Bu değişimle birlikte, *"Digital-age Security"* kavramının kendiliğinden tartışıldığı yeni dönemde özel bir etkinin olduğu ve yeni yaklaşımlara ihtiyaç olduğu kaçınılmaz bir gerçeklik haline dönüşmüştür (Dunn, 2007:86).

Uluslararası ilişkilerin kalbinde yer alan devletler siber uzayın aktörü haline gelmesiyle devletlerarası çıkarlar, var olan güç potansiyelini siber güvenlik alanına kaydırmış ve ayrıca bir parantez açmıştır. Devletlerin siber uzayın bir aktörü haline gelmesi, siber suçların etki alanının genişlemesine ve yarattığı tehdit potansiyelinin artmasına neden olmaktadır. Bu durum uluslararası ilişkiler içerisinde devletlerin siber güvenlik kavramını daha ciddi bir şekilde ele almaları zorunluluğunu getirmiştir. Siber güvenlik, iki büyük dünya savaşında olduğu gibi askeri ve jeopolitik üstünlüğü ön plana çıkaran taarruzlar yerine bilgi sistemleri üzerinden yapılan, siber uzayın sunduğu sınırsız özgürlük ortamı içinde daha kolay ve kısa sürede gerçekleştirilebilen saldırıları mümkün kılmıştır (Bayraktar, 2015:24).

Kamu ve özel sektörü ilgilendiren, belli bir alana ilişkin temel parametreler sunan siber politikalar, uluslararası ilişkiler temelinde kimi zaman dünyayı salt saldırı-savunma ikileminde görmekte; kimi zaman

da teknik durumları kavramada başarısız olan bir tablo karşımıza çıkarmaya başlamıştır (Stone, 2012:102). Siber güvenliğe ilişkin sosyal bilimler temelinde ve uluslararası ilişkiler temelindeki çalışmaları doğru anlama adına *sibernetik, siber toplum, siber terörizm, siber tehdit, siber caydırıcılık, siber savaş, siber istihbarat* gibi kavramların doğru anlaşılması gerekmektedir.

Siber terörizm kavramının beslendiği nokta ve harekat bulma süreci *siber tehditlerle* ilgilidir ve kaynaklandığı noktalar da bu kavrama dahildir. *Siber tehditler;* internete bağlanmayı sağlayan ve çevrimiçi saldırılara maruz kalmayı olanaklı kılan araçların oluşturduğu unsurlardır. Siber tehdit yöntemleri ve ortaya çıkış süreci sanal bir ortamda gerçekleşince maddi ve manevi, fiziksel sonuçlar doğurmaktadır ve bu sonuçların geri dönüşü olmayabilir. Bu suçların etkileyici olmaları bireysel olmalarına, kurumsal bir etki oluşturmasına ya da devlet gibi uluslararası aktörlere etki edişine göre farklılaşmaktadır. Özellikle bireysel anlamda işlenen bilişim suçları ve bunların etki düzeyleri, istihbarat alanına ilişkin tehditsel unsurlar ve devlete yönelik siber saldırı ya da devlete siber destekli kinetik saldırılar aynı derecede değildir ve bir etki alanına sahiptir. Devletlerin çoğu zaman müdahil olduğu siber olaylar organizasyonel suçlardan daha etkili sonuçlar doğurabilmektedir. Kimi zaman kritik altyapılara ve devletlerin nüfuzunun olduğu coğrafyalarda bu tehditler kritik altyapı bütünlüklerinde daha fazla hissedilmektedir ve bir tehdit bütünlüğü oluşturmaktadır.

Siber güvenlik perspektifinde, operasyonel unsurların oluşturulması ve hedeflerin belirlenmesi aşamalarıyla birlikte savunma hattındaki en büyük zafiyet kritik altyapıların korunmasında baş göstermektedir. Yapılan saldırılar ve müdaheleler çıkar elde etme amacıyla gerçekleşeceği için misilleme karşı tarafı caydırma adına fiziksel unsurlara yönelecektir ve gözetilecek karşı ataklarda konvansiyonel unsurlara başvurulmayacaktır.

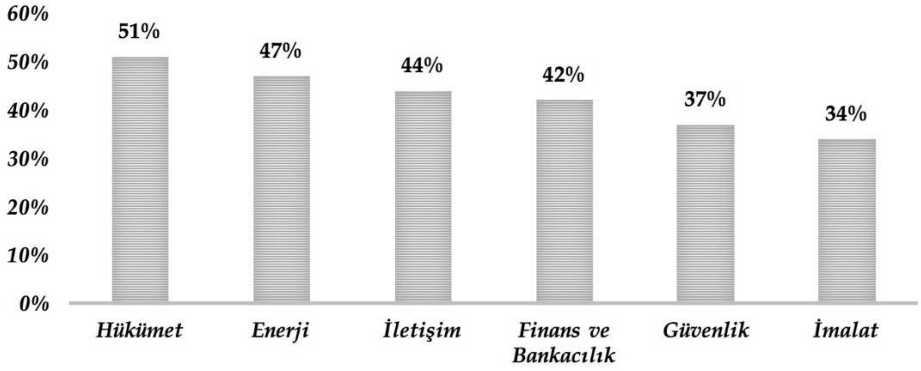
Kritik altyapılar, muhtelif sivil ve askeri tehditlere maruz kaldığından, ulusal düzeyde korunması gereken stratejik sistemler kapsamında değerlendirildiği için hassas nokta olarak yer almaktadır. Siber ittifaklar açısından, siber savunma kapsamında korunması gereken kritik altyapı ve sistemleri şu şekilde ifade edebiliriz:

- *Savunma sanayii,*
- *Tüm iletişim sistemleri,*
- *Bilgi sistemleri,*
- *Lojistik sistemler,*
- *Hava savunma ve komuta kontrol sistemleri,*
- *Kripto sistemleri,*
- *Seyrüsefer, yaklaşma, iniş, konumlama ve yön bulma sistemleri,*
- *Uydu ve yer sistemleri,*
- *Uzay sistemleri,*
- *İnsanlı ve insansız hava aracı sistemleri.*

Tüm bu sistemlerin bağlı olduğu bir uluslararası arenada siber saldırıları kullanarak devletlerin kritik altyapılarını çökertmek ve karşılıklı bağımlılık ilişkisine dayanan bir sistemin işleyişini çalışmaz hale getirmek günümüz siber savaş ortamında mümkün gözükmektedir. Operasyonel alanı hedef alan ve fiziksel dünyada çeşitli sonuçlar doğurabilecek saldırıların çoğu da IT sistemlerinin delinmesiyle başlamaktadır (Hemme, 2015:25). Bu noktada özellikle kritik altyapılar, operasyonel teknolojiler ve bilgi teknolojileri dallarında çalışan ciddi bir uzman altyapısıyla siber güvenlik kültürü inşa etmenin gerekliliği kendini hissettirmektedir.

Grafik 1'de, organizasyon yapısına göre veri kaybına uğrayan kuruluşların ABD özelinde, 2015 yılı etkilenme oranları gösterilmektedir. Oranların temel olarak veri kaybı açısından işaret ettiği alanların başında hükümet, enerji, iletişim, finans, güvenlik ve imalat gelmektedir. Özellikle enerji ve iletişim özelinde gerek veri kaybı, gerekse veri kayıplarından oluşturulabilecek riskler, siber saldırıların kritik altyapılar üzerinde yoğunlaştığının ispatıdır. Gelişmekte olan ülkeler açısından enerji nakil hatlarının önemi düşünüldüğünde, fiziki olarak bu hatların korunması temel öncelik olarak ön plana çıkmaktadır. Karşı taraf açısından amaçlanılan unsur, verilerin ele geçirilmesi yanında fiziki zararlar olabilir. Hazar coğrafyası da enerji koridoru oluşu ve sahip olduğu önem itibariyle ciddi bir tehdit alanını oluşturmaktadır.

Grafik 1. Organizasyon Yapısına Göre Veri Kaybına Uğrayan Kuruluşların Genel Etkilenme Oranları



Kaynak: Report on Cybersecurity Critical Infrastructure in the Americas, 2015:25

Enerji, telekomünikasyon, ulaşım ve su sistemleri gibi kritik altyapı sistemleri bilgi sistem otomasyonu ile idame ettirilmektedir. Bu sistemlerin bir ülke için stratejik öneme sahip olduğu düşünüldüğünde doğal hedefler haline dönüşmeleri kabul edilebilir bir durumdur. Bir ülkeye zarar vermek, kaos yaratmak ya da ekonomisini alt üst etmek için sistemlere gerçekleştirilecek bir siber saldırı yeterli olabilir (Yılmaz ve Sağıroğlu, 2013:324). Bu hedefler arasında basınç sistemiyle çalışan enerji nakil hatları sistemleri, besleyici birim olarak ciddi tehlike altındadır. Genel olarak eğilim, özellikle bu hatların siber alana bağlı olması yönündedir. Hazar özelinde geçiş koridoru olarak sahip olduğu nitelik ve coğrafi anlamdaki zenginlik bu altyapının oluştuğu süreçle birlikte tehlike oluşturmaktadır.

Başta enerji olmak üzere, nükleer alanda faaliyet gösteren tesislere etki eden ve literatüre *"Blended Attacks"* olarak geçen saldırıların fiziksel dünyada yıkıcı sonuçlar doğurabileceği, 2010 yılındaki Stuxnet olayıyla ispatlanmıştır. 2015 Aralık ayında Ukrayna'da siber silahları kullanarak ülkeyi karanlığa gömen etki bu olaylardan sadece birkaçıdır. Oluşan ittfakların amaçları geçici olsa da, birlikteliğin sürdüğü süre zarfında bu tür olaylara müdahil olunabilmesi anlık veri alışverişi bakımından ve tehdidin karşılıklı olarak tespiti açısından önemli bir yere sahiptir. Savunma kısmında kritik altyapıların kapsadığı fiziksel çevre bireylerin, iletişim ağlarının, cihazların ve uygulama alanlarının devamlılığında üst bir niteliktir.

2. Hazar'ın Hukuki Statü Sorunu ve Uluslararası Güvenlik Açısından Hazar Havzası[1]

Sovyetler Birliği'nin (SSCB) dağılması ile birlikte Hazar coğrafyasında yeni kıyı devletlerin ortaya çıkmasıyla oluşan yeni jeopolitik düzende, Hazar'ın hukuki statüsünün belirsizliği önemli tartışma konularından biri olmuştur. Bağımsızlıklarını kazanmalarının ardından bir yandan ulusal kimliklerini inşa etmeye, diğer taraftan kalkınmalarını sağlamaya çalışan Kazakistan, Azerbaycan ve Türkmenistan'ın yeni kıyı devletleri olarak bölgede söz sahibi olmaları, Rusya ve İran'ın eski anlaşmalara dayandırdığı Hazar'daki tarihi paylaşımın sorun teşkil etmesine yol açmıştır. İki yüzyılı aşkın bir süre boyunca sadece Rusya ve İran arasında siyasi-ekonomik bir ilgi alanı olan Hazar Denizi, bu aşamadan sonra beş devletin ilgi alanına dönüşmüştür. Kıyı devletlerinin her biri, artık hidrokarbon kaynaklarıyla zengin olan ve jeopolitik önem taşıyan güzergahlar üzerinde stratejik bir konumda bulunan bu büyük su havzasından yararlanmak ve kendi payına düşeni fazlasıyla almak istemektedirler (Oğan, 2015). Değişen dünyanın getirmiş olduğu yeni boyutla birlikte oluşan teknolojik altyapı, enerji nakil hatlarının özellikleriyle birlikte siber güvenliğin temelinde kritik altyapıların incelenmesi hususunda temel değişkenler ortaya çıkmıştır.

Hazar'ın hukuki statü sorunu ve etkileşimde olduğu kritik altyapılara ilişkin süreç incelenirken öncelikle statü sorununu doğrudan etkileyen coğrafi özelliklerinden bahsetmek gerekmektedir. Hazar çeşitli kaynaklarda, *"dünyanın en büyük (tuzlu su) gölü"* olarak tanımlansa da, tarih boyunca hep bir *"deniz"* olarak algılanmış ve bu şekilde isimlendirilmiştir. Güneydoğu Avrupa ile Asya'nın birleştiği bölgede, 47.07-36.33 kuzey paralelleri, 45.43-54.20 doğu meridyenleri arasında yerleşen Hazar Denizi batıda Azerbaycan, kuzeybatıda Rusya, kuzey ve kuzeydoğuda Kazakistan, doğuda Türkmenistan ve güneyde İran ile çevrilidir. Hazar Denizi'nin toplam sahası 376 bin km^2 ve su hacmi ise 76700 km^3'tür. Kuzeyden güneye 1200 km uzunluğunda ve batıdan doğuya 320 km genişliğindedir ve Hazar'da ortalama derinlik 184 metredir. Suyun en derin noktası Azerbaycan'a ait Lenkeran bölgesinde 1.200 metre ve en sığ noktası ise kuzeyde Volga (İdil) Nehri'nin döküldüğü alanda 5 metre civarındadır. Hazar'ın en geniş yeri 554 km ve en dar yeri ise Apşeron Burnu-Tarta arasında 200 km'dir. Hazar sahillerinin toplam uzunluğu 7010 km'dir.

[1] "Hazar'ın Hukuki Statü Sorunu ve Uluslararası Güvenlik Açısından Hazar Havzası" alt başlığı yazar Hülya Kınık'ın KTÜ, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalı yüksek lisans programında hazırlamış olduğu "Kıyıdaş Devletlerin Talepleri Çerçevesinde Hazar'ın Hukuki Statü Sorunu" adlı tezden kurgulanmıştır.

Kazakistan'ın 2340 km, Rusya Federasyonu'nun 1930 km, Türkmenistan'ın 1200 km, Azerbaycan'ın 800 km ve İran'ın 740 km uzunluğunda Hazar'a kıyısı bulunmaktadır (Oğan, 2001:146). Bütün bu özellikler göz önünde bulundurulduğunda, Hazar Havzası çok büyük bir alanın değerli ve stratejik ulaşım ve iletişim noktasıdır. Başka bir ifadeyle Hazar Havzası'nın jeopolitik yeri ve konumu bölgenin değerini artırmaktadır. Bu bütünlük içinde bölgeye ilişkin siber güvenlik temelli bir yaklaşım da sergilenebilmektedir.

Coğrafya ile beraber bahsedilmesi gereken önemli noktalardan biri bölgenin sahip olduğu zengin hidrokarbon kaynaklarıdır. Hazar Havzası, "*Yeni Basra Körfezi*" olarak adlandırılmakla birlikte şu anki veriler bu tespitin ne kadar doğru olduğu konusunda kesin bir kanıt sunmamakta, mevcut kaynaklar Hazar devletlerinin ekonomileri dikkate alındığında kayda değer bir yer tutmaktadır. Zira bu kaynaklar, söz konusu cumhuriyetlerde kalkınmayı hızlandırabilir ve dışa bağımlılıklarını -özellikle Rusya'ya- azaltabilir (Laçiner, 2006:37). ABD Enerji Enformasyon İdaresi (U.S Energy Information Administration-EIA), Hazar havzası adına muhtemel petrol rezervlerinin 48 milyar varil, doğal gaz rezervlerinin ise 292 milyar metreküp olduğunu tahmin etmektedir. Petrolün neredeyse yüzde 75'i ve doğal gaz rezervlerinin yüzde 67'si Hazar kıyılarının 100 km uzaklığında bulunmaktadır (EIA, 2013:8). Bu tahminler açıkça devletlerin siyasi ve ekonomik çıkarları üzerinde etkiye sahip olmuştur. Gelişen ve değişen uluslararası sistemin getirmiş olduğu teknolojik altyapı ve sistemler mücadelenin alanını çok boyutlu bir alana yaymıştır.

Rusya Federasyonu ve İran'ın, tarihi antlaşmalara dayandırdığı düzeni devam ettirme istekleri ile bağımsızlıklarını kazanan kıyı devletlerin kendi çıkarları doğrultusundaki istekleri, Hazar'ın hukuki statü sorununu, 1991 sonrasındaki yeni düzende temel tartışma konularından biri haline getirmiştir. Kıyıdaş ülkelerin her biri bu konuda kendi tezlerini ortaya koyarken bu tezlerine paralel olarak zengin petrol ve doğal gaz kaynaklarının paylaşım kavgasına da girişmişlerdir. Hazar'ın statü sorununun ortaya çıkışının bazı temel nedenleri vardır. Öncelikle, Hazar'ın statüsü, SSCB ve İran arasında yapılan anlaşmalarla kesin olarak belirlenmemiştir. Söz konusu antlaşmalar daha çok gemicilik, balıkçılık ile ilgili olmasının yanında bazen de tek taraflı -Rus tarafı lehine- askeri güç bulundurma konularını düzenlemiştir. Bu gün için SSCB ve İran arasında geçmişte yapılan anlaşmalar sorunun çözümünde yetersiz kalmaktadır. Dolayısıyla, geçerliğini günümüzde de koruyan bu anlaşmalar Hazar'a kıyısı olan eski SSCB'ye bağlı devletleri bir çıkmaza sürüklemiştir (Aydın, 2012:211). Eski geleneksel yapı, başta Rusya ve İran olmak üzere yeni kıyı devletlerinin de siyasi ve ekonomik çıkarlarına uygun gözükmemektedir (Bayraktar, 2007:86). Bunun yanında sorun üzerindeki tartışmalar, Hazar'ın coğrafi olarak isimlendirilmesi boyutundan çıkarak onun ne şekilde paylaşılıp kullanılacağı üzerine yoğunlaşmıştır.

Hazar Havzası'nın jeolojik açıdan incelenmesinin zor olması ile birlikte ilgili uluslararası hukuk kuralları çerçevesinde farklı yorumlara açık yapısı havzanın hukuki statüsünün belirlenmesini zorlaştıran faktörler arasındadır (Karagöl ve diğerleri, 2016:14). Bu hukuki çerçeve siber alanda altyapıların oluşturulması ve bölgesel bir siber gücün ortaya çıkışını da engellemektedir. Bu bağlamda, Hazar'ın statüsünü belirleme noktasında üç farklı yaklaşım söz konusudur. Birinci görüşe göre Hazar, diğer göllere ve denizlere benzemeyen kapalı bir su havzasıdır; bu sebepten onun özellikleri mevcut uluslararası yasal normlar ve uygulamalara konu olamaz. Dolayısıyla Hazar'ın yasal statüsünü ayrıntılı bir şekilde düzenleme sürecinde, gelenek dışı yaklaşımlara başvurulmalıdır (Kephanov, 1997:2). İkinci bir görüş olarak, Hazar'ın bir göl olduğu üzerinde durulmaktadır; ancak uluslararası göllerin kullanımına ve paylaşılmasına dair genel geçerliliği olan uluslararası hukuk kurallarının varlığından söz edilemediği için Hazar'ın bir göl olarak kabul edilmesi durumunda paylaşımına ilişkin iki görüş öne çıkmaktadır. Bunlardan ilki "*ortak yönetim" (Condominium)*; ikincisi ise "*ulusal sektörlere bölünmesi"* görüşüdür (Abdullayev, 1999:268). Bunlardan ilkine göre kıyıdaş ülkeler, Hazar kıyısındaki kıyı uzunluklarına göre pay alabilecek ve ek olarak kıyı çizgisinden itibaren 20 deniz mili mesafede bir sahaya sahip olacaklardır. Bu durumda 20 deniz mili mesafenin dışında kalan alanın arama ve işletme hakları kıyıdaş devletler tarafından oluşturulacak bir yönetime verilecek ve kararlar oy birliği de ile alınacaktır (Oruç, 2013:87-88). Bu yaklaşım bölgede kritik altyapıların oluşturulmasında ve bunun siber alana entegresinde de önemli bir çerçeveyi oluşturmaktadır.

İkinci görüşün kabul edilmesi halinde ise uluslararası hukuka göre devletler anlaşarak istedikleri düzenlemeye gitmekte serbesttirler. Özellikle Azerbaycan tarafından desteklenen bu rejime göre Hazar'ın beş kıyı devleti arasında bölünerek her bir kıyı devletinin tıpkı kendi kara alanındaki egemen haklara sahip olması gerekmektedir (Kapyshev, 2012:26). Bu esasa göre ise kıyı devletlerinin sahillerinden eşit uzaklıkta orta hattıyla ve bu merkez hattı üzerindeki kara sınırlarının son noktasından çizilen bir dikey hatla ulusal sektörler oluşturulacaktır. Böylece her devlet kendi sınırları içerisindeki alanda doğal kaynakları çıkarma ve işletme hakkına sahip olmaktadır. Orta noktanın belirlenmesinin ardından alanı bölerek sınırların oluşturulması anlamına gelen bu ilkeye göre tüm kıyı devletleri biyolojik ve doğal kaynaklar, su yüzeyi ve tüm ulusal bölgelerde ulaştırma konusunda münhasır hâkimiyet sahibi olmaktadır (Shafiyev, 2001). Bu paylaşımı Kazakistan, Rusya ve Azerbaycan kabul ederken güney kıyıdaşlar olan İran ve Türkmenistan karşı çıkmaktadır. Çünkü böyle bir paylaşım kıyı uzunlukları fazla olan Rusya, Kazakistan ve Azerbaycan'ın

paylarının fazla olmasını sağlamaktadır (Deniz, 2014:34). Göllerin bölünmesinin birçok yöntemi olmasına rağmen Hazar'a kıyısı bulunan devletlerin sınır çizgisi veya diğer bölünme yöntemleri üzerinde anlaşamadıkları bilinmektedir. Aslında sorun, Hazar'ın hangi yöntemle veya nasıl bölüneceğinin yanında bölünmesi durumunda ortaya çıkacak egemenlik kaybı ve bunun devletlerin ekonomik çıkarlarına vereceği zarardır.

Son olarak, Hazar'ın hukuki statüsünün bir deniz olarak kabul edilmesi halinde, BM Deniz Hukuku Sözleşmesi'nin doğrudan uygulanması gerekecektir. Bu durumda 12 millik karasuları, 200 mili aşmayan münhasır ekonomik bölge ve kıta sahanlığı prensiplerine göre çizilecek bir sınır söz konusu olacaktır. Ancak Hazar ülkeleri arasında bu tür bir uygulamaya izin verecek uzaklık zaten mevcut değildir. Bu durumda BM Denizler Hukuku Sözleşmesi'nin 15'inci maddesi gereği devletlerin, karşılıklı kıyılara sahiplerse orta noktayı esas kabul ederek, sınırın o çizgiyi aşmaması ilkesi uygulanacaktır (Szalkai, 2013:38). Özellikle oluşturulacak enerji nakil hatlarında ve bağlı sistemsel altyapı bu durumdan açık bir şekilde etkilenecektir.

Hazar'da beş taraflı bir antlaşmanın varlığından bahsedilemese de görece işbirliği, ihtilafları da tetiklemekle birlikte kıyıdaş devletlerin aralarında imzaladığı ikili ve çok taraflı anlaşmalarla sağlanmıştır. 1998 Kazakistan-Rusya, 2001 Rusya-Azerbaycan ve 2001 Azerbaycan- Kazakistan Antlaşmaları ve daha sonraki 2003 Rusya-Kazakistan-Azerbaycan Antlaşmasından sonra, kuzey kıyıdaşları aralarında bir uzlaşmaya varılmıştır. Deniz yatağından *"orta hat"* esasına göre yararlanmayı öngören bu rejime, güney kıyıdaşlar olan İran ve Türkmenistan karşı çıkmaktadır. Güneyde Türkmenistan, denizin paylaşılması ilkesini benimsemekle birlikte, bunun yöntemi konusunda fikir ayrılığına düşmüştür. Özellikle Azerbaycan ile orta bir hat boyunca aralarında Hazar'ı bölme konusunda anlaşmalarına rağmen bu hattın sınırlarının nereden çizileceği konusunda uzlaşamamışlardır. İran ise her bir kıyı devletinin Hazar'ın %20'sine sahip olması gerektiğini savunmaktadır ve beş eşit parçaya taksiminden yanadır (Mohsenin, 2001:170).

Bütün bu görüşlerin farklılığından da anlaşıldığı gibi hem uluslararası deniz hukuku hem de uluslararası teamül hukuku ilkelerinin uygulanabilirliği Hazar'ın sınırlarının belirlenmesi ve statü sorununa çözüm bulması noktasında tartışılabilir niteliktedir. Bu bağlamda, üzerinde durulan esas nokta, bütün kıyı devletleri arasında özel bir antlaşmanın yapılmasının gerekli olduğudur. Hazar bir deniz veya göl de olsa, su üzerindeki sınırlarını belirlemek beş kıyı devletinin inisiyatifindedir (Lee, 2005:39).

3. Hazar ve Çevre Ülkeler Özelinde Kritik Altyapılar ve Siber Güvenlik Temelli Bir Yaklaşım

Uluslararası hukukun Hazar Havzası adına bütünlük oluşturamadığı husus, güç mücadelesi ve sorunsalında önemli bir çerçeveyi oluşturmaktadır. Bu sorunsal siber güvenlik temelinde kritik altyapıların oluşturduğu temelde de hissedilmektedir. Çevre ülkelerin bölgede etkinliği hususunda veri trafiği ve bu konuda yakın dönemde yaşanan bir dizi olay yaklaşımın geçerliliğini ortaya koymaktadır. En temelde Rusya'nın baskın bir şekilde başını çektiği bu alan siber güvenlik temelli yaklaşımları karşımıza çıkarmaktadır.

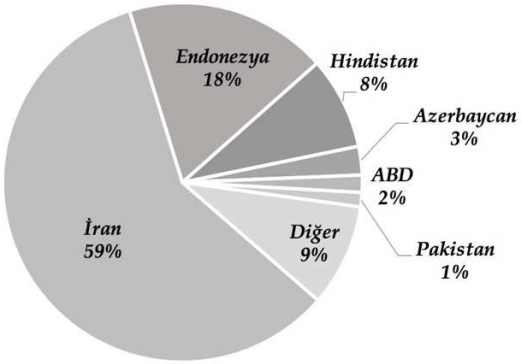
Enerjide büyük ölçüde dışa bağımlı olan küresel aktörlerin, ekonomilerindeki gelişmelere paralel olarak gelecekte enerjiye olan talepleri daha da artacağından, ABD gibi süper, Çin ve Hindistan gibi yükselen güçler, Rusya, Türkiye ve AB gibi bölgesel güçler, enerji taşımacılığı konusunu güvenlik sorunu olarak görmektedirler. Aynı zamanda, gerek enerji kaynaklarının üretimi gerekse nakil hatları projeleri, bölgesel devletler ve enerji talebindeki küresel aktörler adına önemli bir rekabet aracı haline gelmiştir. Bu rekabetin en yoğun olarak yaşandığı Hazar bölgesinin ham petrol dış satım potansiyelinin giderek artacağı düşünüldüğünde, enerji ihtiyacı her geçen gün artan devletlerin, dikkatlerini Hazar bölgesine çevirmelerinin sebebi anlaşılmaktadır (Turan, 2010:44). Bu nedenle, petrol ve doğalgaz arzının karşılanmasında Hazar havzası küresel ve bölgesel güç çatışmalarının odağında bulunan bölgelerin başında gelmektedir. Bu devletlerin dış politika araçları farklılık gösterse de temel amaçları, enerji güvenliğini sağlamak ve ulaşım hatları üzerinde hak sahibi olmaktır (Bayraç, 2009:136). Bu ulaşım hatları üzerinde verilere sahip olma ve yeri geldiğinde bu verileri manipüle edebilme ya da hatlar üzerinde fiziki zararlar oluşturma bir dizi amaçlar arasında yer almaktadır.

Enerji sektörünün doğası gereği bünyesinde barındırdığı riskler politika yapıcıların mutlaka üzerinde durması gereken konuların başında gelmektedir. Zira boru hatlarındaki enerji nakil faaliyetlerinde ortaya çıkabilecek aksaklıklardan kaynaklanan operasyon maliyeti, bakım ve tamirat masrafları, milli ekonomiye bedeli oldukça ağır tahribatlar yaratmakta, ayrıca siyasal anlamda uluslararası sistemde çok ciddi prestij ve itibar kayıplarını içeren ağır faturaların ortaya çıkmasına neden olabilmektedir (Caşın ve Kısacık, 2014:15). Enerji güvenliğinde savaş hali dışında ortaya çıkan söz konusu yeni tehdit ve riskler karşısında boru hatlarının sorunsuz, kesintisiz olarak çalıştırılması ve arz güvenliğinin sağlanmasının, ülke milli güvenliği, ekonomik kalkınma ve siyasal istikrar politikaları açısından hayati önem taşıdığı kuşkusuzdur (Caşın ve diğerleri, 2015:7).

Hazar'a kıyıdaş devletlerarasında fiziksel güvenliği garanti altına alan ve özellikle devletlerin birbirlerine karşı saldırmazlık beyanlarını içeren çeşitli ikili anlaşmalar imzalanmıştır. Ancak Hazar'ın kıyı

devletlerinin yanı sıra onlarla işbirliği içerisinde olan küresel petrol ve doğalgaz yatırımcıları, yalnızca fiziksel güvenlik konusununun yanında bir siber saldırı potansiyelini de dikkate almalıdırlar. Haziran 2010'da, İran'ın nükleer tesislerine yönelik gerçekleştirilen Stuxnet saldırısı ile tehlikeli bir siber dünyanın ortaya çıkması, Hazar'daki güvenlik olgusunun geleneksel tanımlama ve beklentilerin ötesine geçmesi gerektiğini göstermektedir (Cottone, 2015). Grafik 2'de görüleceği üzere fiziksel tahribatlara da neden olabilecek bir genel kaygıyı oluşturan Stuxnet sahip olduğu etki düzeyiyle birçok farklı ülkeyi etkilemiştir. Sadece Hazar Havzası özelinde düşünülmemesi gereken örnek olayda bölgenin ciddi bir tehlike içerisinde olduğu ortadadır.

Grafik 2. Stuxnet'ten Etkilenen Ülkeler



Kaynak: Çifçi, 2012:174

Hazar Havzası özelinde düşünülen siber tehdit ve kritik altyapılara yönelik boyut sadece uluslararası ilişkilerin doğasındaki çatışma ruhuyla ve çıkar mücadelesiyle bağdaştırılmamalıdır. Özellikle yapılacak projelerde gelecek vizyonu açısından kurgusal ortam sıkıntıya girebilecektir. Enerji sistemlerinin bilgisayarlar tarafından yönetildiği düşünülürse bu kurgu içinde devletlerin uğrayacağı zarar anlık gerçekleşmeyecek ve Hazar adına, özellikle enerji alanında bir karamsarlık da gözlenebilecektir.

Hazar Bölgesi ve aynı derecede bir uzantı dahilinde yer alan Karadeniz Havzaları farklı ekonomik temeller üzerine kurulu olduğu için uluslararası güvenlik politikalarının siber yönünde enerji kaynaklarıyla birlikte çıkar mücadelesi yer almaktadır. Bölgesel bir çekişmenin sadece bölge aktörleriyle açıklanamayacağı alan, Rusya baskınlığında kendisini hissettirmektedir. Hazar petrollerinin Avrupa'ya taşınması ayağında önemli bir politika trafiğinin olduğu bölgesel gelişmeler ve kritik süreç, bir dizi siber olayın bölgede yaşanması ile derinleşmiştir.

Sonuç ve Öneriler

Uluslararası sistem yeni teknolojik gelişmelerle birlikte, güvenlik anlamında evrimini sürdürecektir. Güvenlik olarak bu türden gelişmeler iki yönlü bir değişimi beraberinde getirecektir. Bunlardan ilki nükleer ve konvansiyonel silahların sahip oldukları kalitenin ve etkinin gelişimidir. Gelişen imkanlarla birlikte bu tür silahların etki alanı ve düzeyi, caydırıcılık rolü uzun bir dönemde, yine en üst seviyede sınırları zorlayacak ve devletleri karşı karşıya getirecektir. İkinci değişim ise siber anlamda yaşanacak olan çekişmelerdir. Bilgiye erişim ve bu bilginin karşı bir güç olarak tekrar kullanılması, devletlerin yönetimsel ve askeri anlamda, sistemleri üzerinde olan etkisini ve önemini daha da artıracaktır. Öyle ki bu düzeyin etki olarak nükleer ve konvansiyonel caydırıcılık düzeyine ulaşması bile beklenildiği göz ardı edilmemelidir.

Siber güvenlik temelli politik yaklaşımlarda güvenlik stratejileri oluşturma ve bunu alana uygulayabilme Hazar Havzası adına temel bir hassasiyeti gerektirmektedir ve siber tehditler boyutunda ele alınmalıdır. Karadeniz ve Hazar temelinde gözetilecek siber politakalar doğru bir şekilde yönlendirilmezse uluslararası hukuktan doğacak yaptırımlarla birlikte daha geniş sorunsallara dönüşebilir. Hazar ve Karadeniz'deki enerji kaynaklarının ve koridorlarının hayati öneme sahip olması, sorunların doğuşunda ve siber güvenlik temelinde önemli hususlardır. Rusya ile Gürcistan arasında yaşanan çekişme, Rusya'nın Batı ile yaşadığı sıkıntılar, Ukrayna Krizi ve Türkiye'nin önemli bir aktör olduğu bu bölgedeki çıkar savaşı yaşanılan problemlerden bazılarıdır ve istikrarı olumsuz yönde etkileyerek çok yönlü bir sorunsalı siber güvenlik alanına da taşımaktadır.

Bölgede uzun süredir yaşanan sınır çekişmeleri, insani ve ekonomik boyutta bazı kalıcı sorunları beraberinde getirebilir nitelikle birlikte siber alandaki sorunlarla evrim geçirecektir. Dağlık Karabağ Sorunu, Gürcistan'daki yerel sorunlar ve sınır güvenliği, Ukrayna'nın bölgede Rusya ile olan çekişmesi, Rusya'nın her fırsatta Sovyetlere duyduğu özlem nedeni ile bölgeye müdahale etmesi ve Avrupa'nın genel olarak Rusya ile olan çekişmesi, uzun vadeli sorunlar olarak Karadeniz ve Hazar çevresinde çıkış noktalarını oluşturacaktır.

Hazar havzası özelinde caydırma amaçlı olarak, siber alanda saldırı niteliğinin kritik altyapılara yönelmesi önemli bir gelecek kurgusunu gerektirmektedir. Enerji koridorları adına bölgesel bağlılık ve reaksiyon, Rusya baskınlığında saldırgan bir yaklaşıma dönüştüğü anda, uluslararası hukuktan doğan bir dizi yaptırımlar söz konusu olduğunda konvansiyonel unsurların devreye girdiği savaş durumunu ortaya çıkarabilir. Devletlerin çıkarlarını maksimize etme algısı ve arzusu bu türden tartışmaları politik düzeyde sert bir şekilde hissettirecektir.

Siber güvenlik dünyası açısından, tehditlerin büyük kısmı birden fazla değişkenle meydana gelmektedir ve tehdidin çok boyutluluğu, savunma içinde benzer bir yaklaşımı zorunlu kılmaktadır. Hamlelerin gizliliği yanında, gelişmiş ağ güvenlik çözümleri ile ortaklıkların kurulmasına ihtiyaç duyulmaktadır. Karadeniz ve Hazar ülkeleri bağlamında, gizliliğin yanında saldırı odaklı ve enformasyon kaynaklarının çökertilmesi amaçlı saldırılar daha sık görülmekte ve ülkeler bu konuda daha bireysel politikalar izlemektedir. Bu gelişmeler ışığında, siber anlamda terörizm boyutuna varan saldırıların, Karadeniz ve Hazar'da çıkar ve caydırma amaçlı olduğu göze çarpmaktadır.

Siber savaşların kendi dinamikleri içerisinde tartışıldığı boyut kritik altyapıların tehditsel niteliğiyle enerji nakil hatları özelinde hassas bir içeriğe sahiptir. Bunun temelinde yatan sebep siber tehditlerin fiziksel etkiler doğurabilecek niteliklere ulaşabilmesi ve özellikle sektörel anlamda bazı düzeylerde dinamiklere sahip olmasıdır.

KAYNAKÇA

ABDULLAYEV, Cavid (1999), "Uluslararası Hukuk Çerçevesinde Hazar'ın Statüsü ve Doğal Kaynakların İşletilmesi Sorunu", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, S.48(1-4), s.256-290.

AYDIN, Nermin Zahide (2012), "Hazar'da Enerji Kaynakları ve Siyaset", *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi*, S.9(2), s.207-224.

BAYRAÇ, H. Naci (2009), "Küresel Enerji Politikaları Ve Türkiye: Petrol Ve Doğal Gaz Kaynakları Açısından Bir Karşılaştırma", *Eskişehir Osmangazi Üniversitesi Sosyal Bilimler Dergisi*, S.10(1), s.115-142.

BAYRAKTAR, Gökhan (2007), "Hazar'daki Jeopolitik Mücadelenin Türkiye'nin Enerji Güvenliğine Etkileri", *Stratejik Araştırmalar Dergisi*, S.11, s.83-93.

BAYRAKTAR, Gökhan (2015), *Siber Savaş ve Ulusal Güvenlik Stratejisi*, İstanbul: Yeniyüzyıl Yayınları.

CAŞIN, Mesut Hakkı ve KISACIK, Sina (2014), *Kritik Enerji Altyapı Güvenliği*, İstanbul: Hazar Strateji Enstitüsü.

CAŞIN, Mesut Hakkı ve diğerleri (2015), *Kritik Enerji Altyapı Güvenliği El Kitabı*, İstanbul: Hazar Strateji Enstitüsü.

ÇİFÇİ, Hasan (2012), *Her Yönüyle Siber Savaş*, Ankara: TÜBİTAK Bilim Kitapları.

DENİZ, Taşkın (2014), Enerji Diplomasisi Açısından Siyasallaşan Mekan, *Türk Coğrafya Dergisi*, S.62, s.29-37.

DUNN, Myriam A. (2007), "Securing The Digital Age: The Challenges of Complexity for Critical Infrastructure Protection and IR Theory", Johan Eriksson and Giampiero Giacomello (Ed.), *International Relations and Security in the Digital Age*, 1. Baskı *içinde* (85-106), New York: Routledge Publishing.

HEMME, Kris (2015), Critical Infrastructure Protection: Maintenance is National Security, *Journal of Strategic Security*, N.5(8), p.25-39.

KAPYSHEV, Ardak (2012), Legal Status of the Caspian Sea: History and Present, *European Journal of Business and Economics*, N.6, p.25-28.

KARAGÖL, Erdal Tanas ve diğerleri (2016), Statü Sorunu İkileminde Hazar'da Enerji Denklemi, *Analiz Dergisi*, S.155, s.14.

KEPHANOV, Yolbars A. (1997-1998), The New Legal Status of the Caspian Sea is the Basis of Regional Co-operation and Stability, *Perceptions: Journal of International Affairs*, N.2(4), s.1-5.

KNUTSEN, Torbjon L. (2006), *Uluslararası İlişkiler Teorisi Tarihi*, İstanbul: Açılım Kitap.

KOTTONE, Stacey (2015), *A Legal & Cyber Minefield: An Overview of the Caspian Region*, http://moderndiplomacy.eu/index.php?option=com_k2&view=item&id=883:a-legal-cyber-minefield-an-overview-of-the-caspianregion&Itemid=488, (30.05.2016)

LAÇİNER, Sedat (2006), Hazar Enerji Kaynakları ve Enerji Siyaset İlişkisi, *Orta Asya ve Kafkasya Araştırmaları Dergisi (OAKA)*, S.1(1), s.36-66.

LEE, Yusin (2005), Toward a New International Regime for the Caspian Sea, *Problems of Post-Communism*, N.52(3), p.37-48.

MOHSENIN, Mehrdad M. (2001), The Evolving Security Role of Iran in the Caspian Region, Gennady Chufrin (Ed.), *The Security of the Caspian Sea Region*, 1. Baskı *içinde* (166-177), Oxford: Oxford University Press.

OĞAN, Sinan (2001), Hazar'da Tehlikeli Oyunlar: Statü Sorunu, Paylaşılamayan Kaynaklar ve Silahlanma Yarışı, *Avrasya Dosyası*, N.7(2), s.143-177.

OĞAN, Sinan (2005), *Yeni Global Oyun ve Hazar'ın Statüsü*, Türkiye Uluslararası İlişkiler ve Stratejik Araştırmalar Merkezi (TÜRKSAM), http://www.turksam.org/tr/makale-detay/601-yeni-global-oyun-ve-hazar-in-statusu, (05.04.2014)

ORUÇ, Tarık Çağrı (2013), Kıyıdaş Devletlerin Talepleri Çerçevesinde Hazar'ın Hukuki Statüsü ve Paylaşılması Sorunu, R. Kutay Karaca (Ed.), *Asya'da Güvenlik Sorunları ve Yansımaları*, 1. Baskı *içinde* (82-102), İstanbul: Bilgesam Yayınları.

Report on Cybersecurity and Critical Infrastructure in the Americas, Trend Micro Incorporated, 2015.

SHAFIYEV, Farid Raufoğlu (2001), The Legal Regime of the Caspian Sea: Views of the Littoral States, *Prism*, N.7(6), http://www.jamestown.org/single/?tx_ttnew s%5Btt_news% 5D=28012&tx_ttnews%5BbackPid% 5D=223 #.VXmb2Pntmko, (16.06.2016).

STONE, John (2012), Cyber War will Take Place, *Journal of Strategic Studies*, N.36(1), p.101-108.

SZALKAI, Kinga (2013), A Sea or A Lake- What Difference Does It Make? Queations of the Delimination of the Caspian Sea, *Security Policy Review*, N.6(2), p.33-49.

TURAN, Aslıhan P. (2010), Hazar Havzası'nda Enerji Diplomasisi, *Bilge Strateji*, S.2(2), s.44.

U.S Energy Information Administration (EIA), "Overview of Oil and Natural Gas in the Caspian Sea Region", 2013, s.8, http://www.eia.gov/countries/analysisbriefs/Caspian_Sea/caspian_sea.pdf, 16.10.2014.