MARTİN C. LIBICKI'NİN "SİBER CAYDIRICILIK" KAVRAMININ NÜKLEER CAYDIRICILIK OLGUSU İLE KARŞILAŞTIRILMALI ANALİZİ

Uğur Ermiş*, Barış Özdal**

***Özet*—Günümüz uluslararası ilişkilerinde nükleer caydırıcılığa benzer bir şekilde siber caydırıcılığın olup olamayacağı tartışma konusudur. Devletlerin kritik altyapılarını SCADA (Supervisory Control and Data Acquisition) sistemleri ile kontrol ettikleri ve ağ merkezli muharebeye geçtikleri günümüz dünyasında, yapılacak bir siber saldırı ile ciddi zararlar verebilmek mümkündür. İkinci Dünya Savaşı'nın sonunda başlayan nükleer silahların kullanımı ise hatırlanacağı üzere beraberinde nükleer caydırıcılığı getirmiştir. Çalışmada Soğuk Savaş boyunca iki blok arasında dengenin sağlanması noktasında çok önemli bir yer tutan nükleer caydırıcılığın doğurduğu etkiyi, siber uzayda siber caydırıcılığın doğurup doğurmayacağı sorusuna cevap aranmıştır. Bu bağlamda siber caydırıcılık üzerine en yetkin eserleri kaleme alanlardan biri olan Martin C. Libicki'nin görüşlerine yer verilerek siber caydırıcılığın mümkün olup olmadığı tartışılmıştır. Tüm bu etki kapasitesine rağmen siber uzayın kendisine özgü özellikleri nedeniyle nükleer caydırıcılık etkisinde bir siber caydırıcılığın oluşmasının mümkün olmadığı savunulmuştur.**

***Anahtar Kelimeler*— Siber Caydırıcılık, Siber Savaş, Nükleer Caydırıcılık**

***Abstract*—Can we make comparisons of nuclear deterrence and cyberdeterrence in modern era. States conduct their critical infrastructures with SCADA systems. Also states make network centric warfare in our age. Because of all these reasons, cyber-attacks costs high damages. During Cold war, nuclear deterrence provided a diplomatic balance between Soviets and USA. In this article, we are questioning that does cyberdeterrence affect the world as much as nuclear deterrence? Despite all of this capacity, cyberdeterrence isn't effective as much as nuclear deterrence because characteristic of cyber space is very different from our conventional war types and rules.**

***Key Words*—Cyberdeterrence, Cyber War, Nuclear Deterrence**

I. Giriş

BU çalışmada Martin C. Libicki'nin "Cyberdeterrence and Cyberwar" eseri incelenmiş olup siber caydırıcılık ve nükleer caydırıcılık kavramları karşılaştırılmıştır.

Çalışmanın ilk bölümünde nükleer caydırıcılık ele alınmış olup bu çerçevede nükleer silahlanma ve buna bağlı olarak farklı nükleer caydırıcılık stratejileri genel ve soyut olarak incelenmiştir.

Çalışmanın ikinci bölümünde ise siber caydırıcılığın ne olduğu üzerinde durularak siber caydırıcılığın, nükleer caydırıcılıkla benzerlikleri ve farklılıkları Libicki'nin eserinde ortaya koyduğu üç temel ve altı destekleyici soru üzerinden incelenmiştir.

Sonuç bölümünde ise Libicki'nin eserinde verdiği cevaplar doğrultusunda güncel gelişmeler göz önünde bulundurularak, siber uzayda siber caydırıcılığın sağlanıp sağlanamayacağı sorusu analiz edilmiştir.

II. Nükleer Caydırıcılık

Varlığı siyasi oluşumların varlığıyla eş tutulabilecek olan caydırma stratejisi, ilk nükleer silahın 2. Dünya Savaşı'nda Japonya'da kullanılmasıyla farklı bir boyut kazanmıştır. Kısa süre sonra Sovyet Sosyalist Cumhuriyetler Birliği'nin de nükleer stoklara sahip olması caydırıcılık stratejisinin anlamı değişime uğramıştır. Özellikle Soğuk Savaş boyunca nükleer güce sahip devletler bu güçlerini diplomatik müzakerelerde pazarlık güçlerini arttırmak için kullanmışlardır. Diğer bir değişle her iki kutup liderinin de yaşanan tüm gerilime rağmen doğrudan çatışma noktasında karşı karşıya gelmemeleri nükleer silahların sağladığı caydırma işlevine bağlanabilir. Bu bağlamda nükleer güç ve bu gücün sonucu olarak nükleer caydırıcılık bir önleyici diplomasi aracı olarak kullanılmıştır. Kullanılması durumunda eğer bir taraf sahipse karşıdaki ülkeyi, iki taraf birden sahipse çatışan iki devleti ve hatta tüm dünyadaki insan varlığını ortadan kaldırma potansiyeli olan nükleer silahlar, caydırma stratejisinde zirve noktayı temsil etmektedir.

Stratejistler tarafından nükleer caydırıcılık stratejisi minimum caydırma stratejisi ve nihai caydırma stratejisi olarak ikiye ayrılmaktadır. Minimum caydırma stratejisi, rakibin kaldıramayacağı ölçüde bir misilleme saldırısına yetecek kadar nükleer silaha sahip olmayı öngörmektedir. Nihai caydırma stratejisinde ise rakibin misilleme kapasitesini de yok etme amaçladığından, ilk vuruşta rakibin tüm nükleer cephaneliğini ortadan kaldırmaya yetecek kadar silahlanmayı gerektirmektedir. Bu bağlamda nihai caydırma stratejisi nitelik ve nicelik olarak çok daha fazla silaha sahip olmayı gerektirmektedir. Minimum caydırmada ise stratejik dengeyi sağlayacak kadar silaha sahip olmak yeterlidir. [6]

NATO konseptleri içinde "Esnek Karşılık" ve "Topyekûn Karşılık" doktrinlerini genel ve soyut olarak ele almak gerekirse örgüt 1949 yılında kurulduğunda temel stratejilerin oluşturulması büyük ölçüde ABD'nin kontrolünü altında olmuştur. 1953 yılında ABD Genelkurmay Başkanı Oramiral Redford'un hazırlanmasına katkı verdiği yeni bakış olarak bilinen NSC(National Security Council) 162[1] isimli rapor, kitlesel topyekûn karşılık doktrininin temellerini oluşturmaktadır. Topyekûn karşılık doktrini temelde Batı Bloğu olarak lanse edilen bölgeye olası Komünist saldırı karşısında Amerikan Stratejik Hava Kuvvetlerine bağlı

* Araştırma Görevlisi, Uludağ Üniversitesi, Uluslararası İlişkiler Bölümü, Siyasi Tarih A.B.D.
** Doçent Doktor, Uludağ Üniversitesi, Uluslararası İlişkiler Bölümü, Siyasi Tarih A.B.D.

uçakların Sovyetler ve Çin Halk Cumhuriyeti'nin stratejik endüstri merkezleri ve şehirlerine nükleer silahlarla saldırılmasını öngörmektedir. Bu örnekten de anlaşıldığı üzere Topyekûn Karşılık doktrini iki noktaya dayanmaktadır:

1. Nükleer silahlarla karşılık yeteneği düşmanı hem sınırlı hem de topyekûn bir savaştan caydıracaktır
2. Nükleer silahlar durum gerektiğinde kullanılacaktır. Bu nedenlerle, Avrupa Müttefik Kuvvetleri Başkomutanlığı'na askeri savunmasını taktik nükleer silahları kullanabilecek biçimde yeniden düzenlemesi yetkisi verilmiştir.

Genel olarak bakıldığında ise nükleer silahlar üzerinden oluşturulan bu yapı hem Sovyetleri girişeceği olası bir savaştan caydırmış hem de Batı Bloğu üyesi Avrupa devletlerini ve ABD'yi büyük kara orduları oluşturma masrafından kurtarmıştır.

1949 yılında Sovyetlerin ilk denemesini yaptığı nükleer silah her ne kadar ABD'nin nükleer tekelini kırmışsa da ABD'yi stratejisini değiştirmeye asıl iten olay 1957 yılında Sovyetlerin Sputnik isimli yapay uyduyu başarılı bir şekilde uzayda yörüngeye yerleştirmesi olmuştur. Diğer bir deyişle Sputnik'in uzaya yerleştirilmesi iki okyanus tarafından coğrafi olarak korunun ABD'nin tarihte ilk defa kendi topraklarında vurulma ihtimalini ortaya çıkarmıştır.

Bu gelişmenin arından sınırlı savaş kavramı ABD tarafından kabul edilmeye başlamıştır. ABD artık havadan filolar üzerinden yapılarak nükleer saldırılar yerine, yerlerinin saptanması çok güç olan ve Polaris tipi güdümlü füzelerle yüklü nükleer denizaltıları ve ICBM (Inter-Continental Ballistic Missile)'leri geliştirmeye başlamıştır. ABD tarafından bu strateji uyarınca, tam anlamıyla yaşamsal çıkarlarının olduğu durumlarda güvenliğini nükleer silahlarla koruyacağı, diğer durumlarda ise savunmanın geleneksel silahlarla yapılacağı anlayışına dayanan bir doktrin geliştirilmiştir. Esnek karşılık stratejisinin sonucu olarak NATO'nun kara kuvvetlerinde bir artışı gerçekleşmiştir. [5]

III. Siber Caydırıcılık

Caydırıcılık teorisinde amaç saldırının maliyetini ve sonuçlarını beklenen yarardan daha fazla hale getirerek saldırının önünü kesmektir. Bu stratejinin yerine getirilebilmesi noktasında da iki önemli unsur vardır. Bu unsurlardan ilki sağlam bir savunma kapasitesine sahip olmaktır. Eğer bir devletin savunması, olası bir saldırıyı son derece zor hale getiriyorsa, saldırma potansiyelini barındıran devlet durmayı seçebilir. Siber uzayda, bu durumu sağlayabilmek saldırıların büyük birçoğu için çözüm sunmaktadır. Caydırıcılıkta ikinci önemli unsur ise misillemenin önem kazanmasıdır. Eğer başarılı saldırganlar, eylemleri neticesinde misilleme ile yüzleşirse, bu durum diğer saldırganları saldırıdan vazgeçirebilmektedir.

Siber caydırıcılığın klasik caydırıcılıktan ayıran en önemli unsuru, saldırının kaynağının tespit edilmesidir. Siber uzayda, dijital dünyanın doğası gereği sağladığı anonimlik, misillemenin doğru kaynağa yapılması noktasında engeldir. Bu durum bizi siber caydırıcılığın üçüncü unsuru olan Tespit/İsnata götürmektedir. [2]

Nükleer caydırıcılık ise tekil ve simetriktir. Bu noktada nükleer caydırıcılığın tekil olması nükleer silaha sahip olan devletin yapabileceği saldırının sonuçları neticesinde kimsenin bu devleti tahrik etmek istememesidir. Eğer nükleer misilleme meydana gelirse ki bu durum misilleme ve karşı misillemeyi de içerebilir, caydırıcılığın altında yatan koşulları fazlasıyla değiştirebilir. Zira misillemeyi yapan taraf ya da her iki taraf birden ortadan kalkabilir, hareket kabiliyetlerini yok olabilir yada güçsüz kalabilirler. Aynı durum ağır konvansiyonel caydırıcılık içinde geçerlidir. Eğer misilleme başlarsa bu daha büyük bir savaşa yola açacaktır ki bu durumda taraflardan birinin varlığı ortadan kalkabilecektir. [4]

Siber caydırıcılık ise tekrarlanabilir olmalıdır. Çünkü yapılacak olası siber misilleme ne saldırgan devleti devre dışı bırakabilir, ne hükümetlerin değişmesine yol açabilir ne de silahsızlandırabilir. Böylelikle devlet saldırabilir, misillemeden zarar görür ve başka bir zaman saldırmak için varlığını devam ettirebilir. Fakat siber caydırıcılıkta simetriktir çünkü eşitler arasında gerçekleşir. Hedef devlet (potansiyel misillemeci) saldıran devletten daha üstün bir ahlaki zemine sahip değildir. Aynı zamanda hedefin çatışmanın ilerlemesi durumunda kazanacağına inanmak için herhangi bir neden yoktur. Bu yüzden misillemeci daimi karşı misillemeden endişelenmelidir. [4]

Siber caydırıcılık tekrarlanabilmesi ve simetrik olması noktasında eşsiz değildir. Bu tür caydırıcılık genelde çekişme içinde bulunan ve birbirleri karşısında sürekli savunmada olan iki devlet ya da bazı durumlarda grup arasında gerçekleşmektedir. Anarşik sistem içinde, şiddetin salgın gibi yayıldığı böyle durumlarda ise caydırıcılık barışı koruma noktasında yeterli değildir. [4]

Daha somut bir biçimde vurgularsak sahip olduğu konvansiyonel güç, ABD'nin karşısındakinin tepkisini önemsemeden küresel bir polis gibi davranmasına müsaade etmektedir. Lakin bu durum siber uzayda geçerli değildir. ABD üstün saldırı kabiliyetine sahip olmak için bu alana büyük miktarlarda yatırım yapmaktadır. Devletin sistemleri en iyiler tarafından yazılmakta ve yazılım noktasında ABD dünyanın tek ithalatçısı konumundadır. Tüm bu durumuna karşın ABD hala saldırıya açıktır. Zira Amerikan toplumunun özellikle de ağ merkezli muharebe yapan ordusunun büyük ölçüde bilgi sistemlerine bağlı olduğu bilinmektedir. Oluşan bu bağlılık daha az gelişen ve daha az demokratik olan ülkelere karşın ABD'yi özel ve kamusal alanda saldırıya daha açık hale getirmektedir. Ayrıca Amerikan kurumları arasında güvenlik politikaları noktasında çok az benzerlik bulunmaktadır. Bu durum toplumu daha güçlü hale getirse de kurumların bağlantılarına zarar vermeyi kolaylaştırmaktadır. Ayrıca çatışmadan konvansiyonel olarak zarar gören taraf eşitliği sağlamak adına siber karşılık verebilir. Diğer bir deyişle ABD tüm avantajına rağmen misilleme eğer karşı misillemeyi getirirse düşmanlarından daha fazla zarar görülecektir. [4]

Uluslararası ilişkilerde oyun teorileri bağlamında bakıldığında siber caydırıcılık işe yarar bir enstrüman olarak görülmektedir. Soğuk Savaş boyunca ABD ile SSCB arasında yaşanan nükleer restleşmenin sağladığı tarihsel veriler siber caydırıcılığında kullanılabilir olduğunu düşündürmektedir. Aşağıda bulunan üç temel ve altı

destekleyici soru ise siber caydırıcılığı nükleer ya da kinetik caydırıcılıktan ayırmaktadır. Sorulan sorulara verilen cevaplarda oluşan bu farklar kinetik ve nükleer silahların aksine siber caydırıcılığın problemlerini ortaya koymaktadır. Nükleer caydırıcılığın temelini oluşturan ve siber caydırıcılıktan ayıran cevapları sağlayan üç temel soru incelendiğinde: [4]

A- Kimin yaptığını biliyor muyuz?

Misilleme yapılmadan önce saldırıyı yapanın kim olduğunun açıkça bilinmesi gerekmektedir. Eğer ilk misilleme gerçekleşmeden önce caydırıcılık işe yarayacaksa, diğerleri caydırıcı devletin kendisine saldıran devletin kimliğinden emin olacağını bilmelidir. Yanlış kişinin saldırıya uğraması sadece caydırıcılığın mantığını güçsüzleştirmeyecek aynı zamanda yeni düşmanların edinilmesini sağlayacaktır. "Eğer masum olmak umursanmıyorsa neden masum olmalı?" sorusu bağlamında ise muhtemel bir siber savaş yerine, kazayla saldırılan devletinde müdahil olmasıyla kendisini savunan devlet iki siber saldırıyla karşı karşıya gelecektir. [4]

B- Düşmanın varlığı risk altında tutulabilir mi?

Savaş zararı çok yönlü bir konudur. Saldırı ya da misilleme gerçekleşmeden önce, saldıranda hedef olanda saldırının doğurabileceği sonuçlar konusunda tam anlamıyla fikir sahibi değildir. Sonrasında dahi saldıranda, saldırılanda verilen hasarın boyutu noktasında emin olamayabilirler. Bu bağlamda bir petrol rafinerisini havaya uçurmak ve bu sayede bir yakıt kaynağının kullanılmasını engellemekle, rafineri kontrol sisteminde değişikliklere yol açan ve bu sayede yakıttaki kimyasal oranlarını değiştirerek araçlara zarar veren kurnazca saldırılar yapmak aynı şey değildir. [4]

C- Yapılan saldırı tekrarlanabilir mi?

Eğer bugün yapılan saldırı yarın ya da ondan sonraki gün yapılacak saldırıyı engelleyecekse caydırıcılık kırılganlaşabilir. Çoğu caydırıcılık şeklinde bu durum herhangi bir problem teşkil etmezken siber caydırıcılıkta bu durum problem oluşturmaktadır. Bazı caydırıcılık türleri (nükleer) o kadar kötü etkiye sahiptir ki hiç kimse bu yönde bir girişimde bulunmazken bazılarında ise yapılan misilleme bir sonraki saldırıyı engellememektedir. Siber uzayda misillemenin tekrar ve tekrar kullanımı gerekli olabilir fakat her kullanım bir sonraki kullanımın beklenen sonuçlarını olumsuz yönde etkileyebilir. [4]

a. Misilleme caydırıcılığı sağlamasa da silahsızlandırmayı sağlayabilir mi?

Misilleme saldırıları sadece caydırıcılık noktasında etkilidir. Konvansiyonel ve nükleer silahların aksine siber silahlar ise genel olarak saldırganın silahsızlandırılması noktasında etkisizdir. Bu durumda misilleme caydırıcılık etkisi doğuramıyorsa herhangi bir anlam taşımamaktadır. [4]

b. Üçüncü gruplar mücadeleye katılır mı?

Caydırıcı kapasite, saldıran devlete yaptığı saldırının istenmeyen sonuçları olabileceğini göstermek için bir sinyaldir. Tarafların belli olmaması ve muhtemel hasarın tespiti noktasındaki sorunlar ise yanlış algılamalara yol açabilir. Bunun dışında herkesin kafasını karıştıracak şekilde saldırı ya da karşı saldırı beklenenin dışında bir üçüncü gruptan da gelebilir. Bunun en önemli nedeni ise hackerların saldırmak için herhangi bir izne ihtiyaç duymamaları ve saldırılarını üçüncü bir devlet üzerinden gerçekleştirebilme kapasiteleridir. [4]

c. Misilleme tarafımıza doğru mesajı verir mi?

Siber hedeflerin bir kısmı hükümet sistemleriyken bir kısmı da özel sektöre aittir. Özel sektöre ait olan bu hedefleri örneğin ABD'de enerji, iletişim ve finans kritik altyapıları oluşturmaktadır. Bu hedeflere yapılan saldırılar halkın dikkatini çekme potansiyelini sahipken birkaç istisna hariç devlet devlete ait sistemler gündelik hayatta çokta önemli değildir. Özel sektöre ait sistemlerin savunulması ise genelde özel ellerdedir. Bu yapılar üzerinde devletin dolaylı olarak uygulamaya koyacağı düzenlemeler ve kanuni zorlamalar dışında, doğrudan etkisi bulunmamaktadır. Özel sistemlerdeki açıkları hükümetler tespit etme şansına sahip değillerken, şirket sahipleri de bunları söyleme konusunda istekli değillerdir. [4]

d. Saldırıya cevap vermek için bir eşik var mıdır?

Ne kadar sert bir saldırı misilleme yapmayı haklı kılar? Savunucu siber uzayda yeteneklerine zarar verdiğini düşündüğü herhangi bir girişim için misillemede bulunabilir. Yani sonrasında saldırıyı yapacağını duyurduğu bir anı eşik olarak belirleyebilir. [4]

e. Tırmanmadan kaçınılabilir mi?

Nükleer caydırıcılık noktasında stratejistler nükleer gerginliğin ötesinde ne olacağı noktasında endişelenmezler. Zira eğer saldırgan devlet nükleer silah kullanırsa misilleme durumunda bundan daha fazla ne yapacağını tartışmak mantıklı değildir. Siber caydırıcılık noktasında ise stratejistler sonrasında ne olacağını düşünmelidir. Siber misilleme sonrasında saldırgan buna kinetik hatta nükleer güç kullanarak karşılık verebilir. Bu çerçevede Rusya Federasyonu stratejik bir siber saldırıya cephaneliğin de bulunan herhangi bir stratejik silahla karşılık vereceğini deklare etmiştir. Saldırgan devlet gerilimi tırmandırma noktasında eğer:

1- siber misillemenin hak edildiğine inanmıyorsa,

2- iç kamuoyundan sert bir biçimde cevap verilmesi şeklinde baskı görüyorsa,

3- yada siber misillemeye siber saldırıyla karşılık vermesi durumunda kaybedeceğine inanmıyorsa,

Farklı enstrümanlarla cevap verebilir. [4]

f. Saldırgan devlette vurmaya değer bir şey yoksa ne olur?

Özelliklede ABD'nin karıştığı durumlarda tamamen simetrik bir savaş durumu mümkün değildir. Fakat siber savaş bu durumdan daha da asimetrik olabilir. Birleşik Devletler ekonomisi ve toplumundaki fazlasıyla ağ tabanlılık* ordusuna da yansımaktadır. Aksine saldırgan devlette ise karşılık olarak saldırılabilecek dijitallikte bir hedef bulunmayabilir, devlet bu ağları yeterince önemsemeyebilir ya da bu hedefler dış dünyaya bağlı olmayabilir. Örneğin Estonya'ya 2007'de yapılan DDOS saldırıları büyük bir şoka neden olmuşken, 2008'de Gürcistan'a yapılan saldırılar o kadar etkili olmamış, 2009'da Kırgızistan'a yapılan saldırılar ise neredeyse fark edilmemiştir. [4]

* "networked" kelimesi için kabul gören bir Türkçe karşılığa rastlanmamaktadır.

IV. SONUÇ

Yukarıdaki makalenin sınırları dâhilinde genel ve soyut olarak belirttiğimiz veriler göz önüne alındığında ABD her ne kadar resmi hiç bir belgede deklare etmese de Pentagon raporlarından sızan[3] şekliyle kendisine yapılan bir siber saldırıya konvansiyonel silahlarla karşılık verebileceğini belirtmiştir. ABD'nin ayni ile mukabele yerine geliştirdiği bu stratejinin temelinde Libicki'nin de belirttiği gibi ABD'nin nükleer ve konvansiyonel anlamda sağladığı caydırıcılığı, bu alanda tüm çabasına rağmen sağlayamaması/sağlayamayacağı gerçeği yatmaktadır.

Silahlanmanın tüm alanlarında olduğu gibi siber uzayda silahlanma noktasında da savunma yapısını geliştirmek, saldırıdan çok ekonomik güç, teknoloji ve emek gerektirmektedir. Siber saldırı noktasında ise diğer alanların aksine çift yönlü bir farklılık bulunmaktadır. Birinci olarak asgari düzeyde teknik imkânlar konvansiyonel silahlanmanın aksine belli bir tekel ya da grubun elinde bulunmamaktadır ve edinilen imkânlar diğer devletler tarafından takip edilememektedir. İkinci ve daha önemli olan farklılık ise siber uzayda teknolojik olarak en gelişmiş devletin siber saldırıya en müsait devlet olduğu gerçeğidir. Bu noktada kritik altyapıların yönetimi ve kontrolü ön plana çıkmaktadır.

Devletten devlete tanımı ve içinde bulunan unsurlar belli oranlarda değişmekle birlikte devletin devamlılığı noktasında fiziki gereklilik olan tüm yapılar kritik altyapı olarak adlandırılabilmektedir. En genel kabul olarak: su, su tutma ve iletim sistemleri, enerji üretim ve iletim sistemleri, iletişim, finans ve ulaşım altyapısı kritik altyapılar olarak kabul edilmektedir. Devletlerin siber uzayla ilişkileri arttıkça bu yapılar üzerindeki kontrol mekanizmaları mekanik ve insan odaklı yapıdan, ağ merkezli yönlendirilen dijitalleşmenin hâkim olduğu SCADA sistemlerine geçmektedir. Örneğin 2010 yılında STUXNET isimli kötücül yazılımla İran nükleer tesislerine, resmen kabul edilmese de ABD ve İsrail tarafından yapıldığı düşünülen saldırı SCADA sistemlerine gerçekleşmiş, bu sistemlere yapılabilen bir saldırının ne kadar zarar verebileceği ilk defa pratik olarak gözlemlenmiştir. Yapılan saldırı her ne kadar üstü örtülü olarak ABD'nin gücünü göstermiş olsa da buna paralel olarak zafiyetini de ortadan koymuştur. Zira dünyadaki çoğu devletin aksine birçok kritik altyapısı özel sektörün elinde olan ABD'nin, dünyada teknolojiyi üreten ülke olarak sistemleri de çok daha fazla ağ merkezli ve SCADA sistemlerinin kontrolündedir. Kritik altyapı sistemlerinin büyük oranda özel sektörün elinde olduğu göz önünde bulundurulduğunda bu sistemleri savunmak ekonomik maliyetin yanında kanuni düzenlemelerde gerektirmektedir. Ancak, serbest piyasa işleyişini bozacak bu düzenlemeler ABD'nin liberal ilkeleriyle ters düşmektedir. Tam tersi durumdan bakıldığında ise siber saldırı için gerekli teknik imkânı sağlayan herhangi bir üçüncü dünya ülkesinin, doğru insan gücünü yetiştirdiğinde kritik altyapıları siber uzaya bu kadar bağımlı olmadığı için saldırı yapması durumunda, yapılacak siber misillemeden çok daha az düzeyde etkilenecek ya da hiç etkilenmeyecektir. Çalışmada siber caydırıcılığın etkisiz olabileceğine verilen örneği tekrarlamak gerekirse 2009 yılında Kırgızistan'a yapılan saldırılar bu anlamda Estonya'nın aksine gündelik yaşamı ve devlet işleyişini çok daha az etkilemiştir. ABD bu durumun bilincinde olduğu için siber saldırılara karşı konvansiyonel karşılığı öne sürmektedir. Bu bağlamda bizce Libicki'nin de eserinde belirttiği gibi siber caydırıcılığın nükleer caydırıcılığa benzer şekilde etkili olması mümkün değildir.

KAYNAKLAR

[1] http://investigatinghistory.ashp.cuny.edu/images/m12/nsc162.htm

[2] http://journal.georgetown.edu/2013/02/06/a-theory-of-cyber-deterrence-christopher-haley/

[3] http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html

[4] Martin C. Libicki, Cyberdeterrence and Cyberwar, Rand Corparation, 2009.

[5] Oral Sander, Siyasi Tarih 1918-1994, 18. Baskı, Ankara: İmge Kitabevi, 2009.

[6] Tayyar Arı, Uluslararası İlişkiler ve Dış Politika, 7. Baskı, Bursa:MKM Yayınları, 2008.