CYBERDETERRENCE AND CYBERWAR

Martin C. Libicki, (2009), RAND Corporation, Santa Monica,CA, pp 244, ISBN-13: 978-0833047342

Reviewed by Çetin Öğüt[♣]

Modern toplumlar bilgi ve iletişim teknolojilerine bağımlı bir düzen içinde yaşarlar. Bu bağımlılık hasımların az bir riskle klavyeleriyle uzaktan elektrik dağıtım istasyonlarına, bankacılık sistemlerine ve askeri güvenli ağlara saldırmasına imkân sağlayabilir. 2007 yılında Estonya'da yaşanan ve Rusya Federasyonu ile ilişkilendirilen siber saldırılar bunun ilk etkili örneklerinden biridir.

RAND'ın kıdemli araştırmacılarından olan Martin C. Libicki; "Cyberdeterrence and Cyberwar" isimli çalışmasında ABD Hava Kuvvetleri Komutanlığının "Siber Komutanlık Kurulması ve Siber Savaş'ın Tanımlanması" projesi kapsamında; potansiyel bir çatışma alanı olarak ortaya çıkan siber uzayda gücün sınırı ve "siber uzayda uçmak ve savaşmak "kavramının arkasındaki operasyonel gerçeklikler tartışılmaktadır. (s.,iii).

Kitaptaki ana fikir; siber uzayın –hava ve uzay ortamlarından farklı olarak- kendi başına bir ortam olduğu ve kendine has kuralları ve özelliklerinin bulunduğunun kavranmasıdır. Örneğin siber taarruz, klasik askeri harekâtta olduğu gibi büyük yığınaklanma ve kuvvet toplamayla değil düşmanın hassasiyetlerinin istismar edilmesiyle icra edilir. Kalıcı etki üretmek zordur. Siber ortam kimin neden saldırı yaptığı, neye ulaştığı ve saldırının tekrarlanabilmesiyle ilgili belirsizliklerle doludur. Bugün saldırı anlamında çalışan bir özellik yarın çalışmayabilir. İşte bu nedenlerle, caydırıcılık ve savaş teorisiyle ilgili kara-deniz-hava ve uzayda işleyen prensipler siber uzayda tam olarak işe yaramayacaktır. Söz konusu prensipler siber uzay özelinde yeniden düşünülmelidir ve bu kitap böyle bir yeniden düşünme gayretinin başlangıcıdır.

Profesör Martin C. Libicki, halen ABD Deni Harp Akademisinde Siber Güvenlik Araştırma Merkezinde öğretim görevlisidir. Savaş teorisi ve özellikle de siber uzayda savaş, caydırıcılık, yönetişim gibi alanlarda birçok çalışması vardır. 2009 yılında yazılan "Cyberdeterrence and

♣ Ankara Yıldırım Beyazıt Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Doktora Öğrencisi

Cyberwar" bu çalışmaların en önemlilerinden biridir. ABD güvenlik politikalarında önemli bir etkiye sahip yarı resmi RAND Düşünce Kuruluşunun kıdemli analist ve araştırmacılarından biri olarak, ABD Hava Kuvvetleri tarafından yürütülen ve daha sonra bağımsız bir kuvvet haline gelen Siber Komutanlığın kuruluş aşamasında önayak olmuştur. Son olarak 2016 yılında Deniz Harp Akademisinde ders kitabı olarak da okutulan "Cyberspace in Peace and War" kitabını yazmıştır. Siber uzay ile ilgili birçok konferansa ve çalıştaya açılış konuşmacısı" olarak katılmıştır.

"Cyberdeterrence ve Cyberwar" kitabı önsöz ve dokuz ayrı bölümden oluşmaktadır. Dokuzuncu bölüm çalışmanın genel sonuç bölümüdür. 20-25 sayfa arasında değişen her bölümün sonunda kısa bir sonuç kısmı yer almaktadır. Kitabın organizasyonu kolay anlaşılır ve takip edilebilir formdadır.

"Giriş" bölümü olan birinci bölümde, ; siber uzayın önemini vurgulayanların bakış açısı tanıtılmaktadır. Bu çevreler siber uzaya hakim olan gücün diğer ortamlarda (kara-deniz-hava ve uzay) bilgi üstünlüğüne ulaşmasının sadece zaman meselesi olduğunu iddia etmektedir. Buradan hareketle siber taarruz ve siber savunma yeteneklerinin oluşturulması, geliştirilmesi ve idamesinin önemi vurgulanmaktadır. Kitabın amacının siber caydırıcılık konusundaki kuramsal ve uygulamaya yönelik çerçeveyi oluşturmak olduğu belirtilmektedir. Ancak siber caydırıcılığın siber savaşın ayrılmaz bir parçası olduğundan hareketle başlangıçta siber savaşın temel özelliklerinin inceleneceği belirtilmektedir. (s.5) Giriş bölümünde ayrıca siber uzayın doğasının farklı olması sebebiyle konvansiyonel ve nükleer savaş ortamında işleyen caydırıcılık kavramının aynı esaslarda siber uzayda da etkili olmasının beklemenin mantık dışı olduğu anlatılmaktadır. Bugünkü şartlarda, siber taarruzun konvansiyonel taarruzu desteklemek maksadıyla kullanıldığı "operasyonel siber taarruzun", bir devlet politikası olarak hasmı etkilemek amacıyla uygulanacak stratejik siber taarruzdan daha kullanışlı ve uygulanabilir olduğu belirtilmektedir. Bu nedenle operasyonel siber taarruzun kuvvet çarpanı olabilecek özel bir yetenek olarak geliştirilmesi vurgulanmaktadır. (s.7)

İkinci bölümde siber uzay ile ilgili kavramsal çerçeve oluşturulmuştur. Siber taarruz ve siber caydırıcılık kavramları tanımlanmıştır. Başlangıçta siber uzayın sanal ve insan yapısı olduğu belirtilmekte, daha sonra da siber uzayın katmanlı yapısı anlatılmaktadır. Daha sonra siber taarruz tanımlanmaktadır. Buna göre siber taarruz bir devletin başka bir devletin hedef sistemini bozması veya devre dışı bırakmasıdır. (s.23) Tartışmaların sınırlanması maksadıyla,

Siber ağ casusluğu siber taarruz olarak kabul edilmemiş, ne tür saldırıların siber taarruz kabul edileceği Ek-A'da örnekleriyle açıklanmıştır.(s.179-181). Caydırıcılık kavramının yerinde tartışılabilmesi için kitaptaki aktörler devletten devlete olarak kabul edilmiştir. Çünkü siber taarruz tehdidi yoluyla siber caydırıcılık oluşturulması devletlerin kabul edebileceği bir sonuçtur. (s.26). Siber misillemenin kinetik çatışmalara dönüşebilme potansiyeli nedeniyle bazıları misilleme konusunda çekingen davranmaktadırlar. Ayrıca siber taarruzun gerçek kaynağının tespiti ve orantılılık konusunda da belirsizlikler olabilmektedir. (s.27)

"Siber Caydırıcılık Neden Farklıdır?" başlıklı üçüncü bölümde, siber caydırıcılık kavramı tartışılmakta ve nükleer caydırıcılıktan farkları üzerinde durulmaktadır. Bu bölümde dokuz soruya cevap aranarak siber caydırıcılığın genel askeri (nükleer dahil) caydırıcılıktan farkı üzerinde durulmaktadır (s.39). Üç ana soru; kimin taarruz ettiğini biliyor muyuz?, hasmın kritik sistemlerini tehdit edebiliyor muyuz?, siber taarruzu tekrarlayabiliyor muyuz? (s. 35-59). Altı yan soru ile de siber caydırıcılığın farkı güçlendirilmektedir(s.59-71). Bölüm sonunda siber misilleme niyetinin ve isteğinin açıkça önceden beyan edilmesinin siber caydırıcılığı daha inandırıcı hale getireceği vurgulanmaktadır. Ayrıca güçlü bir siber savunma yeteneğinin de siber caydırıcılığın inandırıcılığını artıracağı belirtilmektedir (s.74)

"İlk Siber Taarruzun Maksadı Neden Önemlidir?" başlıklı dördüncü bölümde, siber taarruz kavramı tartışılmakta ve hasmı siber taarruz icra etmeye iten etkenler incelenmektedir. Bu kapsamda siber taarruz edenin maksadı hata, zorlama, kuvvet ve diğer etkenler kapsamında tartışılmaktadır (s.75) Siber uzayda taarruzun nedeniyle ilgili veriler hasmın niyeti ve misillemeye karşı tutumuyla ilgili ipucu verebilir. Örneğin küçük ölçekli taarruzlar zorlama için yapılmış olamazlar veya büyük ölçekli planlı taarruzlar kazayla olamazlar. Bazı taarruz türleri sadece askeri hedefleri etki altına alırken, örtülü siber taarruzlar misilleme olarak algılanamaz veya üçüncü tarafları etkileyemezler, çünkü örtülüdür, gizli kalmaya mahkûmdur. Kısaca hasmın taarruz maksadı, yapılacak misillemeye karşı tepkisi hakkında fikir verebilir (s.90).

"Karşılık Verme Stratejisi" başlıklı beşinci bölümde, taarruza uğrayan tarafta hasmın siber taarruzuna cevap verirken veya misillemede bulunurken ortaya çıkan sorular tartışılmaktadır. Maruz kalan taraf siber taarruza uğradığını bildirmeli midir? Siber taarruzdan sorumlu tutulan devlet açıklanmalı mıdır? Siber misilleme görünür olmalı mıdır? Siber misillemenin geciktirilmesi uygun mudur? Devlet kontrolündeki hackerlere karşı misilleme nasıl

yapılmalıdır? Caydırıcılık politikası açıklanmalı mıdır? Bunlar başarılı bir caydırıcılık politikası için cevap aranan sorulardır (s. 93-114). Siber caydırıcılık konusunda klasik caydırıcılıktan farklı bir bakış açısı gereklidir. Genelleme yapılacak olursa; hiçbir devletin açıktan bir siber caydırıcılık politikası olmamalı, ama hiçbir devlet de misilleme konusunda tereddüt etmemelidir. Siber taarruz gerçekleştiren bir devlet, başarılı taarruz sonrasında misilleme gelmemesini hedef devletin yeteneksiz ve güçsüz olmasına bağlamamalıdır. Misillemede en önemli faktör, kaynak ülkeyi inandırıcı bir şekilde sorumlu tutabilmektir. Bunun kadar önemli olan diğer bir faktör de misilleme söyleminin kamuoyu gözü önünde gerçekleşmesi ve her iki tarafın kamuoyları tarafında da dikkatlice izlenmesidir. Bu nedenle siber uzayda misilleme yapma ve bunun şekli bir devletin göstermek istediği yüzüyle doğrudan ilgilidir. (s.116)

"Stratejik Siber Savaş" başlıklı altıncı bölümde, stratejik seviyede siber savaşın ortaya çıkması tartışılmaktadır. Stratejik savaş bir aktörün hedef devletin politik bir davranışını değiştirmek maksadıyla icra edilen siber taarruz zinciridir. Stratejik siber taarruz tartışılırken üç varsayım yapılmıştır. Birincisi devletler arasında henüz kinetik askeri taarruzlar, çatışmalar yaşanmamaktadır. Hatırlayalım ki, kinetik taarruzları destekleyen siber taarruzlar operatif nitelikte idi. İkincisi varsayım siber savaşın iki devlet arasında gerçekleşen çift taraflı bir nitelikte olduğudur. Son varsayımda ise siber taarruza karşı hukuki, diplomatik ve ekonomik yaptırımlar ile ilgili aşamanın geçildiği, karşılıklı siber taarruzların icra edildiği kabul edilmiştir. (s.117) Siber savaşın dış ve iç amaçları vardır. Dış amaç, hedef devletin savaşma arzusunu yok etmektir. İç amaç ise çatışmanın boyutunu kısıtlamak, gereksiz fiziki çatışmayı engellemekle ilgilidir. (s.118) İki devletin kinetik çatışmaya girmeden sadece siber taarruz yöntemleri içeren bir siber savaş yapmaları mümkün müdür? Teorik olarak evet, çünkü kinetik çatışmaların yer aldığı savaş ile siber savaş karşılaştırıldığında; siber savaşta arazi kaybetme endişesi yoktur. Siber savaşın maliyeti daha düşüktür. Topluma olan etkileri sınırlıdır. Böylece kinetik çatışma istemeyen iki devletin sadece siber taarruzlar içeren bir siber savaşa girmeleri teorik olarak mümkündür. (s.122) Siber taarruzlar ile hedef devletin bilgi teknoloji sistemlerindeki zafiyetler açığa çıkarılarak, bırakın kinetik bir çatışmaya girmesi, siber taarruzlara misilleme de bulunması bile önlenebilir. Bu tür bir zorlama için arka arkaya siber taarruz yeteneğinin devam ettirilebilmesi önemlidir. (s.127-129) Bu bölümde sonuç olarak stratejik siber savaşın başlıca problem alanları; zayıf zorlama etkisi, hedef üzerinde oluşturduğu kısıtlı baskı, stratejik taarruzların devamlılığının zorluğudur. Bu nedenle stratejik siber savaş klasik kinetik savaş teknikleriyle karşılaştırıldığında tercih edilmemesi

gereken bir araçtır. Bu neden ile de ABD Hava Kuvvetleri Komutanlığı tarafından öncelikli bir yatırım alanı olmamalıdır. (s.137)

"Operatif Siber Savaş" başlıklı yedinci bölümde, operatif seviyede siber taarruzun klasik savaşın bir destekçisi olarak kullanılması incelenmektedir. Operatif siber savaş, devam eden klasik çatışmalar sırasında askeri hedeflere ve asker hedeflerle ilintili sivil hedeflere karşı icra edilen siber taarruzlardır. (s.139) İki önemli özelik hatırlatılmaktadır. Birincisi operatif siber savaş ile kinetik çatışmanın kazanılamayacağıdır. Yani, siber taarruzların destekleyici rolü abartılmamalıdır. İkinci özellik ise siber üstünlüğün imkânsızlığıdır, çünkü tek bir siber uzay yoktur. Hedef devletin siber sistemlerine tamamen hâkimiyet (cybersupremacy) mümkün değildir. (s..140-141) Operatif siber taarruzların savaşı destekleyen üç önemli rolü olabilir. Birincisi baskına uğrayan hasmın teknik yeteneklerini sekteye uğratması, ikincisi hasım üzerinde geçici ama etkili bir felç durumu yaratması, üçüncüsü de hasmın kendi sistemlerini güvenli bir şekilde kullanmasını engellemesidir. (s.142) Bu bölümde sonuç olarak, bilgi çağında yaşamanın operatif siber savaşı, savaşın tek ve en etkin yolu yapmadığı vurgulanmaktadır. 20.yy boyunca Hava Kuvvetlerinde olduğu gibi operatif siber savaş klasik çatışmaları destekleyici roldedir. Küçük kıpırtılar görülmekle birlikte, henüz gerçek anlamda bir operatif siber savaş örneğini dünya yaşamamıştır. Bununla birlikte operasyonel siber savaş; tek sefer de olsa büyük sürprize sebep olması, kritik hedeflere göre hassas zamanlanmış etkisi ve hasmın ağ-merkezli ve koalisyon yeteneklerini kısıtlaması bakımından dikkat çekmeye ve uygulama alanı bulmaya devam edecektir. (s.158)

"Siber Savunma" başlıklı sekizinci bölüm, siber savunma üzerinde yoğunlaşmaktadır. Askeri bilgi teknoloji ağlarının ve benzeri güvenlik temelli ağların siber taarruzların kurbanı olmaması için gerekli tecrit, izlenebilme / sorumlu tutma, inkar etme ve aldatma uygulamaları incelenmektedir.

Sonuç bölümü olan dokuzuncu bölümde ise çalışma sonunda ele edilen sonuçlar kısaca özetlenmektedir. Siber uzayda en iyi savunma, güçlü taarruz yeteneğine sahip olmak değil savunmayı güçlendirmektir. Siber caydırıcılık klasik caydırıcılık gibi etkili değildir. Bu nedenle siber caydırıcılık yerine diplomatik, hukuki ve ekonomik yaptırımların uygulanacağı vurgulanmalıdır. (s.176) Uluslararası ilişkilerin anarşik ortamında siber taarruz ve siber misilleme döngüsü bir taraf krizi tırmandırana kadar çete saçlarına benzer bir dinamik içinde seyredecektir. Bütün zorluklarına rağmen siber caydırıcılık ve siber savaş ABD için

kaçınılmaz bir durum değildir. Bir gün hasım bir devlet açıkça ABD.ne toplumda büyük infial yaratacak şekilde taarruz ederse, yöneticiler sadece siber misillemeyle – yetersiz kalacaktır- kendilerini sınırlandırmamalıdır. (s.178)

Libicki'nin "Cyberdeterrence ve Cyberwar" açık ve iyi organize edilmiş bir çalışmadır. Yazar siber savaş ile ilgili örnek olayları incelemek yerine Soğuk Savaş dönemindeki olaylarla karşılaştırma yaparak teorik çerçevede güçlü bir kurgu sağlamıştır. Yöneticilerin ve askerlerin siber caydırıcılık ve siber savaşa başvurmadan önce dikkate alması gereken faktörler belirtilmiştir. Klasik savaş ve caydırıcılık konusundaki başyapıtlara yaptığı vurgular ve geniş referans listesiyle önemli bir kaynak olarak kullanılabilir. Kitap yayınlandıktan sonra teknik bir bakış açısı yerine siber uzayı tarihi bir perspektif ve Soğuk Savaş dönemi normlarıyla incelediği için bazı güvenlik çevreleri tarafından eleştirilmiştir. Bu tür eleştirilere rağmen; kitabın siber uzay, siber savaş ve siber politikalar konusunda çalışan akademisyenlerin ve lisansüstü eğitim gören öğrencilerin temel başvuru yayınlarından biri olması gerektiği değerlendirilmektedir.