TÜRKİYE'NİN GELECEKTEKİ SİBER SAVUNMA ORTAMI

Yrd.Doç.Dr. Can Kasapoğlu

Araştırma Görevlisi – EDAM

1. Giriş

Türkiye'nin internet kullanımı sosyal medya, özel sektörün artan gereksinimleri ve devlet ağının nitelikleri dolayısıyla hızla yükselen bir profildedir. Giderek artan söz konusu 'bağlantılılık' durumu *(interconnectedness),* Türkiye'nin kritik milli altyapısının siber ağlara olan bağımlılığı ve siber saldırılar, Türk milli güvenlik ajandasına siber güvenliğin karmaşık gerçekliklerinin girmesine neden olmuştur. Bu bağlamda Ankara, 20 Ekim 2012 itibariyle Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi ve Koordinasyonuna İlişkin Karar ile siber güvenlik koordinasyona ilişkin ilk milli hukuki düzenlemesini hazırlamıştır[1]. Ayrıca, Siber Güvenlik Ulusal Eylem Planı da 2013 yılında yürürlüğe girmiştir. Ulusal Eylem Planı siber saldırıların tespit edilmesindeki zorlukların altını çizmiş, hassas bilgilerin ve kritik milli altyapının korunmasına özel bir önem atfetmiştir[2]. Aynı zamanda, Ankara Türk Silahlı Kuvvetleri bünyesinde bir Siber Komutanlık kurmuş ve Türk Hükümeti 2011 yılında ülkenin kurumlar-arası ilk siber tatbikatını icra etmiştir[3].

Yukarıda aktarılan tüm çabalara karşın, siber tehditler Türkiye'nin siber güvenlik önlemlerini aşan bir süratte artmaktadır. Bir NATO üyesi olarak Ankara kendi milli güvenliği bağlamında siber güvenliğini sağlamak zorunda olduğu kadar, ittifakın da siber savunmasına katkıda bulunmak durumundadır. Bu doğrultuda Türkiye'nin ve NATO müttefiklerinin siber harbe ilişkin, taarruz ve müdafaa boyutlarını kapsayacak bir çerçevede, isabetli ve net bir anlayışa sahip olmaları büyük önem arz etmektedir.

Bu noktada, siber harbe ilişkin salt siyasa düzeyinde çözümler üretmeye yönelik bir çalışmanın dahi askeri ve güvenlik alanlarında kavramsallaştırmalara gereksinim duyacağı belirtilmedir. Çünkü öncelikle Batı dünyasının gelişmiş siber güvenlik doktrinleri ve konseptleri ile kıyaslandığında, Türkiye'nin önünde siber tehditlerle mücadelede ve bu bağlamda tehdit algılamasının mükemmelleştirilmesinde gidilecek uzun bir yol olduğu görülmektedir. İkinci olarak, siber harp tartışmalarının ilginç bir şekilde hava gücü *(Air Power)* askeri teorik tartışmaları ile benzeştiği, daha açık bir anlatımla askeri pratiğin teoriyi takip ettiğine ilişkin ciddi emareler bulunduğu gözlemlenmektedir. Bu tartışma çerçevesinde, Washington merkezli düşünce kuruluşu the Center for Strategic and International Studies (CSIS) tarafından hazırlanan bir rapor,

siber terörizm ile 2. Dünya Savaşı dönemi hava gücü teorisi ve pratiği arasındaki mukayeseli analizi şu şekilde açıklamaktadır:

> "Siber terörizm yeni bir teknolojinin stratejik zafiyet yaratmak amacıyla kullanıldığı ilk vaka değildir. Siber harp ve hava gücü teorileri arasında bir eşleşme olduğunu öne sürmek tam anlamıyla isabetli olmasa da, ikisi arasında bir mukayesede yarar görülmektedir. Birinci Dünya Savaşı'na bir tepki olarak Douhet ve Trenchard gibi Avrupalı stratejistler, düşman ileri hatlarının çok gerisine, kritik altyapıya yönelik hava taarruzlarının düşmanın savaşma gücünü akamete uğratacağını savunmuşlardır. Söz konusu teoriler 2. Dünya Savaşı sırasında ABD Silahlı Kuvvetleri ve Britanya Kraliyet Hava Kuvvetleri tarafından denenmiş; bu kapsamda stratejik bombardıman taarruzları elektrik hatları, ulaşım altyapısı ve üretim tesislerini hedef almıştır. İşte siber saldırılara ilişkin literatürün ilk safhaları birçok yönüyle stratejik bombardıman konseptine dair askeri teorik tartışmaları andırmaktadır ve hatta varlığını bu tartışmalara borçludur".[4]

Türkiye'nin muhtemel siber saldırılar karşısındaki zafiyetine ilişkin doğru bir anlayış geliştirmek için, öncelikle gelişen teknolojik trendlerin ve bahse konu trendlere bağlı olarak ortaya çıkan tehdit algılamalarının incelenmesi ve sayılan faktörlerin harbin geleceğini nasıl şekillendirdiğinin kavramsal olarak açıklanması gerekmektedir. Müteakip alt başlık kapsamında analiz edildiği üzere, siber yeteneklerin askeri meselelerde devrim *(Revolution in Military Affairs – RMA)* kapsamında nasıl değerlendirilebileceğine ışık tutulacaktır. Bu çalışma daha sonra mevcut ve potansiyel siber trendler ve tehditler ile bahse konu sahada Türkiye'nin ve NATO'nun göz önünde bulundurması gereken devletlerdeki imkan ve kabiliyetleri inceleyecektir. Daha sonra siber harbin, gelecekte savaşın 'beşinci boyutu' olarak nasıl ele alınabileceği 'ağ merkezli harp' çerçevesinde değerlendirilmektedir. Dördüncü alt başlık kapsamında ise siber güvenlik çerçevesinde devlet-dışı aktörler analiz edilmekte ve Türkiye için genel tehdit değerlendirmesi yapılmaktadır. Son olarak, bu çalışmanın bulguları ve önerileri aktarılmaktadır.

2."Siber-Yıldırım Harbinin" Kavramsallaştırılması: Yeni Askeri Meselelerde Devrim (AMD) Olarak Siber Harp

AMD kavramının kökleri esas olarak Sovyet Genelkurmay Başkanı Mareşal Ogarkov'un ortaya attığı "askeri teknolojik devrim" kavramına dayanmakla birlikte, konseptin evrimi teknolojik gelişmelerin ötesine geçmiştir. AMD, özü itibariyle, muharip yeteneklerde teknoloji, stratejik kültür, teşkilat yapısı, doktrin, eğitim, strateji ve taktik sahalarındaki kırılma düzeyinde ilerlemelere bağlı olarak gelişen büyük ve radikal artış olarak tanımlanabilir. Bu çerçevede, teknolojinin yenilikçi konseptler ve teşkilat adaptasyonu ile birlikte askeri sistemlere uygulanmasını içermektedir[5]. Andrew Krepinevich'in AMD kavramını incelediği "Süvariden Bilgisayara" *(From Cavalry to Computer)* adlı önemli eserinde dikkat çektiği gibi, gelişmiş simülasyonlarda kullanılan bilgisayar-destekli dizaynlar ve etkileri askeri teşkilatların yeteneklerini büyük ölçüde geliştirmektedir[6].

Yukarıda aktarılan çerçeve de göz önünde bulundurulduğunda, siber harbin bir sonraki –ya da hâlihazırdaki– Askeri Meselelerde Devrim olarak ele alınması gerektiği söylenebilir. Bu bağlamda, gelişmiş savaş komuta kontrol ağlarının, muhtemel hedeflerin tespiti, tanımlanması ve izlenmesi amacıyla yönetiminin yanı sıra; istihbarat-gözetleme-keşif sistemlerinin işletilmesi de küresel ortak varlıkların yörüngesel ve siber boyutlarına erişimi gerekli kılmaktadır. Dolayısıyla 'siber silahlanma yarışı' ağ-saldırıları, anti-uydu sistemleri ve yönlendirilmiş enerji silah sistemleri bağlamında ön plana çıkmaya başlamıştır. Esasen, uzay ve siber uzaydaki rekabetin, ki söz konusu alanlar akıllı mühimmatlar açısından da büyük önem taşımaktadır, harp sahasının yönetimi, komuta-kontrol, hedef tespiti gibi konular bakımından gerçek zamanlı bilgi akışı ve mekan ile ilintisi dolayısıyla doğrudan ve kritik etkileri olduğu görülmektedir[7].

Siber harp ile ilintili ancak yalnızca siber harbe indirgenemeyecek olan siber-espiyonaj da siber-teknolojilerdeki gelişmelerin güvenlik araçlarına dönüştürüldüğü, ön plana çıkan alanlardan biridir. Siber-teknolojik ilerlemeler casusluğu, ülke dışına çıkmadan yapılabilen bir etkinlik haline getirdiği gibi, buna bağlı olarak devletleri de kontr-siber espiyonaj faaliyeti

icra etmeye zorlamaktadır. Ayrıca, "kar amacı gütmeyen" siber espiyonaj sektörü halihazırda hassas bilgilerin kamuoyu ile paylaşıldığı bir alan haline gelmektedir[8].

Gelecek harp senaryolarının değerlendirilmesi ve stratejik öngörü geliştirilmesi bağlamında, siber fonksiyonlara ilişkin katı ayırımlar yapılmamasında yarar görülmektedir. Daha açık bir ifadeyle aktarmak gerekir ise, siber harp, sivil-asker ayrımını giderek bulanıklaştırmaktadır. On yıllar süren inovasyon ve deneylerin sonucu olarak siber silahlar ve robot teknolojisinin yeni AMD'nin temel taşlarını oluşturacağı görülmektedir. Tüm bu sayılanlar teknoloji-yoğun varlıklardır ve belirtildiği gibi on yıllarca süren çalışmaların ürünüdürler[9].

Siber harbe ilişkin tarihsel ve siyasa-amaçlı bir çerçeve oluşturmak amacıyla, özellikle enformasyon üstünlüğünün harp sahasındaki kilit rolünün açıklanabilmesi bağlamında, harp tarihinin kullanılması önem arz etmektedir.

Kuşkusuz, yeni muharebeleri icra etmek için kullanılacak yeni imkân ve kabiliyetler kritik üstünlükler kadar kritik zafiyetleri beraberinde getirmiştir. Örneğin, Hannibal'ın savaş filleri harp meydanındaki en ağır ve çetin birlikleri teşkil etmişlerdir. Öte yandan, Zama Muharebesi sırasında Scipio Africanus'un ciritli birlikleri olan *velite* formasyonları kısa mesafeden fillerin görme yeteneklerini hedef alarak, onları takip eden düşman unsurları için bir koruma kalkanı yerine tehdide dönüştürmüştür[10]. Benzer durumu modern orduların enformasyon ve bilgisayar ağlarında da görmek mümkündür. Daha açık bir ifadeyle, modern ordular bilgisayar ağları ve gelişmiş ağ altyapıları ile önemli avantajlar kazansalar da, bahse konu avantajlar potansiyel düşmanlar için aynı zamanda yararlanılacak 'yeni taarruz alanları' açmıştır[11]. Türk Silahlı Kuvvetleri ve NATO bu duruma istisna değildir.

Askeri perspektiften bakıldığında, siber savaşın harp meydanı üzerinde enformasyon üstünlüğü ve kontrole dayandığını söylemek mümkündür. Bu bağlamda, John Arquilla ve David Ronfeldt, 13. yüzyıl Moğol ordularını siber savaşı kavramsallaştırmak için kullanmışlardır. Yazarlara göre, Moğol orduları birçok kez sayısal olarak dezavantajlı olsa da, steplerden gelen komutanlar Moğolistan'ın hafif ve süratli süvarileri sayesinde harp meydanında sistematik enformasyon ve sevk – idare üstünlüğünü kurmaları için sistematik olarak başarıyla kullanmışlardır[12].

Moğol ordularının enformasyon üstünlüğünü harp meydanında muharip başarıya çevirmelerine benzer şekilde, Arquilla ve Ronfeldt, siber savaşı "enformasyona bağlı prensipler ile askeri operasyonları icra etmek ve icra etmeye hazırlanmak" şeklinde tanımlamışlardır. Bu çerçevede, siber harp enformasyon ve muhabere sistemlerinin; düşmanın kendisine ilişkin farkındalığını da oluşturan ve askeri kültürü de içeren "kim olduğuna, nerede olduğuna, ne zaman neler yapabileceğine ve niçin savaştığına ve tehdit sıralamasına" ilişkin verilerin de akamete uğratılmasını içermektedir[13].

Yukarıda atıf verilen Arquilla ve Ronfeldt'in eserini takiben daha kapsamlı birçok analiz ortaya koyulmuş olsa da, söz konusu yazarların çalışmalarının başında Carl von Clausewitz'e atıfla belirttikleri alıntı siber savaşın, harbin geleceğine ilişkin dönüştürücü etkilerini açıklamaktadır: "bilgi, yeteneğe dönüşmelidir"[14]. Bu bağlamda yazarlar, harp meydanına ilişkin en iyi bilgiye sahip olunmasının en az harp meydanına daha fazla insan gücü, teknoloji ve sermaye aktarılması kadar önemli olduğunun altını çizmektedirler[15].

2.1. Yeni AMD'nin Somutlaştırılması ve Görünürlüğü

Siber harp yalnızca teknolojik atılımları değil, aynı zamanda teşkilat, doktrin, konsept ve askeri düşünce alanlarında bir dizi etkin gelişimi de gerektirmektedir. ABD siber savunma harcamaları, Başkan Obama dönemi 2014 bütçesindeki 800 milyon dolar artış ile tarihi bir çıkış göstermiş ve 4,7 milyar dolara ulaşmıştır[16]. Mukayeseli bir örnek vermek gerekirse, ABD'nin 2014 siber savunma bütçesi, Danimarka, Finlandiya ya da Ürdün'ün 2013 yılında tek başlarına savunma bütçelerinden fazladır[17].

Sözü edilen bütçe hareketleri ABD Silahlı Kuvvetleri teşkilat yapısındaki değişiklikleri de beraberinde getirmiştir. 2009 yılında dönemin Savunma Bakanı Robert Gates ABD Stratejik Komutanlığına Siber Komutanlık (USCYBERCOM) kurulması direktifini vermiştir. Söz konusu komutanlık ilk somut operasyonel imkân ve kabiliyetlere 21 Mayıs 2010 itibariyle kavuşmuştur[18]. Yeni Siber Komutanlığın görev tanımı Savunma Bakanlığı'nın özel enformasyon ağının korunması ve operasyonlarının yönetilmesi, planlanması, koordine edilmesi, entegrasyon ve senkronizasyonu ile emir verildiğinde siber-uzayda operasyonların tüm alanlarda icra edilmesi ve ABD ve müttefiklerinin siber-uzayda

hareket serbestisinin sağlanması, olası düşmanların da benzer bir hareket kabiliyetinden mahrum bırakılmasıdır[19].

Benzer şekilde, İsrail Savunma Kuvvetleri Genelkurmay Başkanı General Gadi Eizenkot da İsrail'in siber yeteneklerini konsolide edecek bir birim kurma kararı almıştır[20]. Söz konusu İsrail Siber Komutanlığı kurulmasına ilişkin ilk emareler, Savunma Bakanı Moshe Ya'alon'un 2014 Gazze Savaşı sırasında İsrail'in İran siber saldırıları tarafından hedef alındığını ancak önemli bir zarar verilemediğini belirten açıklamaları sırasında gelmiştir[21].

Estonya, Gürcistan ve Ukrayna'daki siber saldırıların olağan şüphelisi konumunda bulunan Rusya ise siber imkân ve kabiliyetlerini önemli ölçüde arttıran bir diğer devlettir. Bu çerçevede, Moskova'nın, siber harekâtı, mevcut hibrid harp stratejisi ve dış politikasının bir parçası olarak değerlendirdiği görülmektedir. Rusya'nın Ukrayna'daki saldırgan faaliyetleri çerçevesinde siber harbi bir 'koç başı' gibi kullandığı da göz önünde bulundurulduğunda, taarruzi siber yeteneklerin Moskova'nın askeri düşüncesine ve hatta askeri doktrinine entegre edildiği değerlendirilmektedir[22]. Rusya kaynaklı siber harp tehditlerine karşı koymak için NATO 2008 yılında, Estonya-Talin'de Müşterek Siber Savunma Mükemmeliyet Merkezi'ni kurmuştur. Merkezin görevi, NATO, üyeleri ve ortakları arasındaki siber savunma alanında yeteneklerin, işbirliğinin ve bilgi paylaşımının genişletilmesi olarak belirtilmektedir[23]. Ayrıca, 2014 Galler Zirvesi'nin ardından, NATO siber savunma ve güvenliğe daha çok ağırlık vermiş ve bu bağlamda siber savunmayı kolektif savunmanın ana görevlerinden biri olarak değerlendiren bir siyaset benimsemiştir[24].

Çin Halk Cumhuriyeti de siber uzayda yükselen güçlerden biri olarak görülmektedir. Çin'in siber harp programları, diğer aktörlere kıyasla, daha çok taarruzi yeteneklere odaklanmaktadır. Bazı analizlere göre, Çin'in siber yetenekleri, KGB'nin ABD teknolojik üstünlüklerine yönelik en önemli tehditlerinden biri olan endüstriyel espiyonaj yöntemlerine dayanmaktadır[25]. Çin'in siber doktrini ve harp teşkilatı kapsamında esas sorumlu birimin 61398. Birim olduğu değerlendirilmektedir. Söz konusu birim, Çin Genelkurmayı'nın 3. Departmanı'na bağlıdır ve bu departman 'bilgisayar ağları harekatlarını' yürütmekle sorumludur. China Telecom'un bahse konu birim için özel fiber-optik iletişim altyapısı sağladığı ve birimin personel sayısının 'yüzler ve hatta binlerce asker' ile ifade edilebileceği tahmin edilmektedir[26]. Çin Genelkurmayı doğrudan Komünist Parti'nin Merkezi Askeri Komisyonu'na bağlıdır. Bu nedenle, 61398. Birim'in siber

faaliyetleri doğrudan en üst düzey siyasal kontrol altında yürütülmektedir ve komünist idarenin karakterinden ötürü merkezi karar-alma mekanizmalarına tabidir.

61398. Birim'in siber faaliyetlerinin 'Gelişmiş Kalıcı Tehdit' kategorisinde (*Advanced Persistent Threat - APT*) değerlendirilmesi gerektiği öne sürülebilir. 'APT', "güçlü kaynaklar ve iyi eğitimle desteklenmiş düşmanın hassas ekonomik, hususi ya da milli güvenliğe ilişkin verileri birkaç yıl süren sızma harekâtları ile hedef alması faaliyetlerine karşılık gelmektedir. Bahse konu düşmanlar, hedeflerine çoğu konvansiyonel bilgisayar ağ savunma mekanizmalarını akamete uğratmak için tasarlanmış gelişmiş araçlar ve teknikler ile ulaşmaktadırlar"[27]. APT yoluyla potansiyel düşmanların hem endüstri hem de devlet segmentlerinde bilgi toplamayı amaçladıkları da düşünülürse, APT en önemli yükselen tehditlerden biri olarak değerlendirilmelidir[28].

Daha geniş bir perspektiften bakıldığında, Çin Halk Kurtuluş Ordusu'nun (HKO) harp konseptlerinin siber harp, sinyal-istihbaratı, uyduları hedef alan yetenekler, psikolojik harp ve bilgi harekâtlarını giderek daha sistematik biçimde kullanarak geliştiği görülmektedir. HKO'nun askeri jeopolitik perspektifi, elektro-manyetik spektrum, siber-uzay ve uzay tarafından oluşturulan harp sahalarına ve bunların birleşimiyle meydana çıkan nihai bir "sanal harp sahasına" uzanmaktadır[29]. Pratikte, böyle bir askeri yaklaşım müşterek harp konseptleri çerçevesinde bir Çin modeli ortaya koyacak ve elektronik harp, hassas taarruz yetenekleri ve siber harbi kapsayacaktır. Soğuk Savaş dönemi Sovyet konsepti olan 'telsiz ve elektronik harp' anlayışını yeni boyutlara taşıyan Çin askeri stratejistleri, sadece harp sahasına ve taktik angajmanlara odaklanan Sovyet yaklaşımını geliştirerek, HKO'nun 'telsiz ve elektronik harp' anlayışını stratejik seviyeye taşıyabileceğini hesaplamaktadırlar. Bahse konu çabaların merkezinde uzay ve siber-uzayın entegrasyonu bulunmaktadır[30].

Son olarak, İran'ın da siber harp dünyasına gelişen ve iddialı bir aktör olarak girdiği söylenebilir. Diğer birçok otoriter rejim gibi, İran'ın siber adımlarının ilk olarak iç güvenlik odaklı başladığı görülmektedir. 2009 protestolarına müteakip, Tahran ülke içindeki bütün iletişimi gözetlemek için Çin yapımı kapsamlı bir izleme-dinleme sistemi kurmuştur[31]. Daha sonra, Stuxnet'in etkisiyle siber teknolojinin yıkıcı sonuçlarını gören rejim, Dini Lider Ayetullah Ali Hamaney'in onayı ile 2011 yılında Yüksek Siber-uzay Konseyi'ni kurmuştur. Söz konusu birim, hem müdafi hem

de taarruzi siber yeteneklerin yönetiminden sorumludur. Konsey, çeşitli istihbarat ve güvenlik kurumları ile kültür ve haberleşme bakanlıklarını da çalışmalarına dahil etmektedir. İran siber güvenlik mekanizmasında Devrim Muhafızları'nın da önemli bir rol oynadığı görülmektedir. Ayrıca, İran 2012 yılında ilk siber tatbikatını icra etmiştir ve Ruhani'nin devlet başkanlığına gelmesi ile siber operasyonlar bütçesini 20 milyon dolar arttırmıştır[32].

Stuxnet'in, İran'ın nükleer yeteneklerinin yaklaşık %20'sine zarar vererek göreceli bir başarı göstermesinin ardından, Tahran 'siber savaşçılar' yetiştirmeyi amaçlayan bir programa daha fazla yatırım yapmaya başlamıştır[33]. Söz konusu program ve siber savaşçılar bağlamında aktarılan noktalar önemlidir: "İran'da önemli seviyede bir hacker topluluğu bulunmaktadır. Bahse konu hacker'ların yetenek spektrumu, bilinen açıkları yazılım araçları kullanarak hedef alan amatörlerden, yeni açıklar ve hedef alma araçları üreten üstün hackerlara kadar uzanmaktadır"[34]. İran hacker toplulukları arasında önemli yere sahip olanlara Iran Babol Hackers Security Team, Ashiyane Digital Security Team ve Iran Hackers Sabotage Team örnek verilebilir[35]. Suudi Aramco şirketi ve Katar RasGas şirketine yönelik siber saldırılar, İran'ın bu alanda özellikle Körfez Bölgesi kritik enerji varlıklarına yönelik taarruzi yeteneklerinin boyutunu göstermesi bakımından önem arz etmektedir. Benzer şekilde, bahse konu saldırılar sırasında bazı ABD bankalarının da hizmet dışı bırakma saldırılarına maruz kaldığı bilinmektedir[36].

Yukarıda aktarılan bilgiler ışığında, Türkiye'nin ve NATO'nun 21. yüzyılda daha ciddi siber meydan okumalar ile karşılaşacağı değerlendirilmektedir. Yukarıda değinilen bütün yetenekler, devlet düzeyindeki aktörlerin siber imkân ve kabiliyetlerinin yanı sıra, yeni güvenlik tehditlerinin çerçevesinde siber vekalet savaşları tehditlerine de dönüştürülebilir. Devlet düzeyindeki aktörler özellikle '*false flag*' tarzı operasyonlara yönelebilirler, hackerlardan yararlanabilirler ve üçüncü devletleri siber operasyonlar için kullanabilirler. Bu karmaşık tehdit ortamı, Türkiye'nin milli güvenliğine ve NATO'nun işbirliğine dayalı güvenlik ve kolektif savunma prensiplerine yeni tehditler teşkil edecektir. Siber çalışmalar, aktör-temelindeki değerlendirmeler kadar, siber harp konseptine, savaşın beşinci boyutu olarak odaklanmalı ve etkilerinin ağ merkezli harp ortamına nasıl aktarıldığını incelemelidir; bunun Türkiye ve NATO müttefiklerinin siber tehdit hesaplarını daha iyi anlamasını sağlayacağı düşünülmektedir.

3. Savaşın Beşinci Boyutunu Kavramsallaştırmak: Siber-uzay ve Ağ Merkezli Harp

Siber harp sahasının yer aldığı bilgi sistemleri çevresi fiziksel, sinaptik ve semantik olmak üzere üç katmandan oluşur. Siber taarruzi yetenekler ve ağ merkezli harekâta yönelik destek operasyonları söz konusu üç katmanda icra edilmektedir. Fiziksel katman bilgisayarlar, donanım unsurları, kablolar ve radyo frekansı, elektronik sinyaller ve fotonlar gibi öğelerden oluşur[37].

Fiziksel katmanın, özellikle mevcut akıllı mühimmatlar, özel kuvvetler operasyonları ve 'görünmezlik teknolojisine' (*stealth*) ilişkin imkân ve kabiliyetler göz önünde bulundurulduğunda, kinetik askeri saldırılara açık olduğu görülmektedir. Sözdizimsel katman ise fiziksel sistem içinde dolaşan, bilgi sistemlerini aktive eden ve görevler veren emirlerden oluşur[38]. Söz konusu katman hacker saldırılarına açıktır ve bilgi sistemlerini korumak üzere siber savunma yetenekleri gerektirmektedir. Son olarak, semantik katman bilgi içeriğine 'anlam katılan' bölümdür ve bu nedenle aldatma ve şaşırtmacalara yönelik faaliyetlere karşı hassastır[39]. Bu bağlamda, mevcut askeri trendlerin 'kesin ve açık olmayan savaşların' ipuçlarını verdiği bu çerçevede 'savaşan tarafların kimliği ve savaşın bizatihi kendisinin' belirsizlikler taşıyabileceği görülmektedir. Özellikle teknoloji ve askeri teşkilatlardaki değişimler bahse konu trendlerin önünü açmaktadır. Belirtilen nedenlerle bu çalışma siber harbin geleceğin ağ merkezli harekatında oynayacağı rolü de irdeleyen bir paradigma üzerine kurulmuştur[40].

Siber savaşa ilişkin harp sahası kategorizasyonu karar vericilere geleceğin siber operasyonları ve operasyonların icra edileceği 'topografyaya' ilişkin önemli fikirler verebilecektir. Siber-uzay savaşın yeni bir sahası olarak algılansa da, enformasyon sistemlerinin fiziksel katmanı halen deniz-hava-kara kuvvetleri gibi 'geleneksel' güçlerin müdahalelerini gerektirmektedir. Ayrıca, sinaptik ve semantik katmanlarda icra edilen siber operasyonlar, düşman hacker faaliyetleri kinetik olmayan metotlar ve aldatmaya yönelik psikolojik harekat ile entegre edilebileceği için birbirine bağımlıdır. Bu nedenle siber-uzayda yeni nesil 'müşterek harekât' konseptleri, yani aynı anda fiziksel, sözdizimsel ve semantik katmanlarda icra edilen operasyonlar, müdafi ve taarruzi siber harekât anlayışında ciddi değişikliklere neden olabilir.

Çok katmanlı yapısının dışında, siber uzayı harbin beşinci ve yeni boyutu olarak algılamak, söz konusu zeminin savaşın diğer dört boyutundan izole biçimde düşünüldüğü anlamına gelmemelidir. Aksine, bu çalışma, siber uzayın ve siber savaşın gelecek ağ-merkezli harekât ortamında savaşın diğer boyutları ile birlikte önemli bir rol oynayacağını değerlendirmektedir. 2012 yılında Liles ve meslektaşları tarafından yapılan bir çalışmada vurgulandığı üzere, askeri prensiplerin siber harbe uygulanması:

> "…dijital bilgi teknolojilerinin katmanlı olarak silahlı kuvvetlerin silah platformlarına uyarlanması anlamına gelmektedir. Bu, ulus-devlet düzeyindeki aktörlere düşmana karşı önemli bir bilgi üstünlüğü sağlayacaktır. Siber-uzaydaki yeteneklerin karasal platformlara katmanlı olarak yayılması, özü itibariyle, deniz kuvvetlerine bağlı platformların kara kuvvetleri unsurlarını desteklemesinden çok da farklı değildir. Bu çerçevede bir diğer örnek uzaydaki unsurların askeri faaliyetleri olabilir. Örneğin keşif uyduları savaşın tüm doğal boyutlarını (hava-kara-deniz) desteklemektedir ve siber boyut da hâlihazırda komuta-kontrol sistemlerine benzer destekler sunmaktadır"[41].

Ağ merkezli harp yeteneklerinin gelişmesi, siber varlıklara operasyonel ve taktik imkân ve kabiliyetler kazandırılması bağlamında önemli avantajlar sağlayacaktır. Ağ merkezli harekâtın ve ağ merkezli harbin başarılı bir şekilde icra edilmesi düşman üzerinde enformasyon üstünlüğü kurulmasına, bahse konu enformasyon üstünlüğü de karar vericiler, muharip aktörler ve sensörler arasında güçlü bir bağlantı kurarak harp gücünü teşkil etme kapasitesine bağlıdır[42]. Askeri bir bakış açısıyla, belirtilen yaklaşım zaman, harp sahası ve konuşlandırılan kuvvet arasındaki korelasyonu ciddi biçimde değişikliklere uğratabilecek niteliktedir. Daha açık bir anlatımla, ağ merkezli harekât sayesinde, geniş harp sahalarına yayılmış kuvvetler artık daha etkin muhabere imkânları ile daha iyi senkronize olabilmektedirler[43].

Son olarak, ağ merkezli harekâtın hem teknolojik trendler hem de askeri düşünce bağlamındaki anti-tezinin platform-merkezli yaklaşım olduğu vurgulanmalıdır. ABD Kara Kuvvetlerinden Albay Alvin Bailey'in görüşleri doğrultusunda platform-merkezli harp anlayışının kısıtlılıkları aşağıda aktarılmaktadır:

> "ABD Kara Kuvvetleri dünyanın en çok korkulan, sofistike ve ölümcül zırhlı araçlarına sahiptir. Abrams Tankı ve Bradley Zırhlı Muharebe Aracı çöl koşullarında dahi yüksek hızlarda intikal ederek düşmanlara korku salmaktadır. Bahse konu platformların görevleri o kadar başarılı olmuştur

> ki, düşmanlar açık çöl arazisinde dahi ABD zırhlı birliklerine karşı koymaktan kaçınmışlardır. Öte yandan, Kara Kuvvetlerinin yıllar boyunca platform-merkezli harbi başarıyla icra etmesine karşı bu anlayışa dayanmak gelecekteki harekât ortamı için bazı zorluklar da ortaya koyabilir. Bu büyük platformları hızla konuşlandırmak kolay değildir. ABD Kara Kuvvetleri henüz bu platformları tüm kuvvet çapında modern teknoloji sağlayarak otomatize edebilmiş değildir. Veritabanından bilgi alarak aktarma faaliyeti farklı sistemler arasında enformasyon paylaşımına dayanmaktadır. Son olarak, bant genişliğinde hâlihazırda var olan kısıtlamalar mevcut teknoloji kullanılarak yapılan bilgi paylaşımını sınırlamaktadır. Belirtilen hususlar günümüzdeki platform merkezli harp yaklaşımı yerine alternatif konseptler arayışını da gerekli kılmaktadır".[44]

Dolayısıyla, Türkiye ve müttefikleri yeterli taarruzi ve müdafi siber yetenekler geliştirmedikleri sürece Türkiye'nin ağ merkezli harekât konseptleri gelecekte akamete uğratılabilir ve 'kazara platform merkezli' bir düzeye indirgenebilir.

4. Stratejik Silahlar olarak Siber Silahlar: Türk ve NATO Siber Güvenliği için İmkan ve Kabiliyet Odaklı Yeni bir Modeli Düşünmek

Siber silahlara ilişkin bir diğer tartışma konusu da bu unsurların stratejik silahlar kategorisinde değerlendirilip değerlendirilemeyeceğidir. Siber silahların doğasının ve karakteristik özelliklerinin iyi anlaşılması Türkiye ve müttefikleri için hayati önemdedir. Stratejik silahların karmaşık karakteristik nitelikleri üst düzeyde yıkıcı kapasiteyi ve psikolojik olarak terör-korku etkisini ve dehşet dengesi oluşturabilecek unsurları içermektedir.

Tabanksy'e göre siber harbi anlarken kullanılacak doğru yöntem klasik olarak yeni bir silah sistemine yaklaşımımıza benzer olmalıdır. Siber harbin karakteristik özelliklerini ölçmek ve kavramsallaştırabilmek için analistlerin, menzil, yıkıcı etki ve (silahın) kullanımı durumunda siyasi maliyet ve kısıtlılıklara odaklanmaları gerekmektedir[45]. Ayrıca, ilk darbe (*first strike*) avantajı da siber harp kapsamında açık biçimde görünmektedir. Bu kapsamda, siber teknolojinin komuta-kontrol sistemlerine uygulanmasının sonuçları açısından taarruz müdafaadan daha cazip bir seçenek olarak ortaya çıkmakta ve düşmanın misilleme yeteneklerini sınırlandırmaktadır[46]. Kritik milli altyapı, finans ve bankacılık sistemleri, hassas iletişim sistemleri, internet kullanımı gibi geniş bir hedef spektrumunun bulunması da siber silahları konvansiyonel silahlardan daha korkutucu kılabilmektedir.

Yukarıda açıklanan metodolojiye ek olarak, Center for Strategic and Budgetary Assessments (CSBA) adlı ABD merkezli düşünce kuruluşunun konuyla ilgili raporu siber silahlar ve siber harbe ilişkin aşağıdaki değerlendirmeleri vermektedir:

> "Nükleer silahlar ve siber silahların paylaştığı önemli bir özellik de her iki kategorinin taarruzu avantajlı kılarak ön plana çıkarmasıdır. Daha farklı bir ifadeyle, diğer tüm kaynakların eşit kabul edildiği bir varsayımda, taarruzi yeteneklere yatırım yapan taraf avantajlı olacaktır. Nükleer yarış bağlamında, ABD Silahlı Kuvvetleri dünyanın teknolojik olarak en sofistike gücü olarak kabul edilse de, nükleer yeteneklere sahip balistik

füzelere karşı etkili bir savunma mekanizmasını yarım yüzyıldan beri milyarlarca dolar harcamasına karşın henüz tam olarak geliştirmiş değildir. Benzer şekilde, taarruzi siber yetenekler geliştirmek için kurgulanacak harcamalar siber savunma altyapısı için yeterli olacak bütçeden çok daha azdır. Durum tam tersi olsa idi, siber ekonomik harp, siber suçlar ve siber espiyonaj bugünkü düzeylerde sorun oluşturmayacaktı"[47].

Öte yandan, siber silahları tam anlamıyla 'stratejik silah sistemleri' olarak kategorize etmek henüz mümkün görünmemektedir. Peki, bu durumda söz konusu teknolojinin askerileşmesini ve silah haline dönüşmesini nasıl formüle etmek gerekmektedir? 2012 yılında Royal United Services Institute (RUSI) tarafından yayımlanan bir çalışma yüksek potansiyele sahip siber silahların 'anti-radyasyon füzelerine' ve 'at ve unut' karakterli hassas güdümlü silahlara benzetilmesi gerektiğini önermektedir. Söz konusu silahlar, spesifik hedeflerin hazırlanarak sistemlerine yüklenmesine gereksinim duymaktadırlar[48]. Teknik bir perspektif ile ifade etmek gerekirse, gelişmiş anti-radyasyon füzeleri düşmanın entegre hava savunma sistemlerini coğrafi lokasyona bağlı sistemler, aktif yaklaşma güdümlü sistemleri ve ağ-entegre komünikasyon sistemleri vasıtasıyla imha etmek üzere dizayn edilirler[49]. Askeri planlamada, anti-radyasyon füzeleri, düşman hava savunma sistemlerinin imhası görevlerinde kullanılır ve böylece daha geniş hava saldırıları için gerekli zemini hazırlarlar.

Spektrumun bir ucunda, siber silahlar 'kötücül yazılım' (*malware*) unsurlarına dayanmaktadır ve her ne kadar sistemleri etkileme kapasitesine sahip olsalar da, bu unsurlar ciddi zararlar verebilecek şekilde sızma yeteneklerine sahip değildir. Öte sızma, spektrumun yüksek potansiyelli diğer ucunda korunmuş sistemlere otonom penetrasyon yeteneklerine ve ciddi zarar verme kapasitesine sahip gelişmiş kötücül yazılım unsurları bulunmaktadır[50]. Dolayısıyla, siber silahlar düşmanı muharebeden önce felç etme fonksiyonları dolayısıyla anti-radyasyon füzeleri ile benzerlik göstermektedirler.

Öte yandan siber harp yetenekleri savaşan taraflara, stratejik ve taktik hedefleri uzak mesafeden ve genel harekât için operasyonel riskleri minimize edecek şekilde imha etme imkânı vermektedir. Söz konusu avantaj, siber taarruzun belirsizliğine dayanmaktadır ki, bu belirsizlik saldırıya maruz kalan taraf için saldırıyı, bizatihi kendi sisteminden kaynaklanan teknik arızalardan ayırma zorunluluğu ortaya çıkarmakta ve olaylar ile sonuçlar arasında bağlantı kurmayı zorlaştırmaktadır[51].

Askeri istihbarat perspektifinden bakıldığında, siber saldırıların tespiti ve kimlik saptaması biyolojik harp ile benzerlikler göstermektedir. Siber saldırının başında, en kritik öncelik düşman faaliyetinin tespit edilmesi, tanımlanması ve gerekli önlemlerin alınmasıdır[52]. Biyolojik silah programlarında olduğu gibi, siber silah programlarını gizlemek kolaydır ve taarruzi yetenekler çift-kullanımlı teknolojilerin gelişmesi ile doğrudan ilintilidir. İlk askeri istihbarat tespitleri kullanılan biyolojik harp ajanına göre değişebileceği gibi, aynı prensip siber-ajan için de geçerlidir. Ayrıca, özel sektörün ve birey düzeyinde oyuncuların da dâhil olmasıyla, siber harp sahasında 'savaşan tarafları' kesin netlik ile belirlemek giderek daha da zorlaşmaktadır.

Sonuç olarak, biyolojik silahların yayılmasının önlenmesine ilişkin hususlar gibi, siber silahlar ve siber harp de devlet düzeyinde ve devlet dışı aktörlerin faaliyetlerinin izlenmesi için benzer gelişmiş askeri istihbarat yeteneklerini gerektirmektedir. Biyolojik harp ve siber harp için gerekli olan istihbarat ihtiyaçları geniş bir spektrumda imkan-kabiliyet ve niyetler ile ilgilenmektedir. Yine söz konusu istihbarat çalışması, bireyler için ticari olarak ulaşımı mümkün araçları, küçük radikal grupları ve birey-düzeyinde radikalleri de izlemekle yükümlüdür.

5. Türkiye için Devlet Dışı Tehdit Analizi: Değişken bir Siber Güvenlik Ortamı

Orta Doğu'da devlet Weber'in tanımladığı anlamda bir düşüş yaşarken, devlet-dışı silahlı gruplar siber operasyonlara giderek daha büyük ilgi duymaktadırlar ve bu durum siber-uzaydaki çatışmaya bir yayılma etkisi kazandırmaktadır. Bu çerçevede, Suriye Elektronik Ordusu (SEO) dikkat çekicidir. Bu grubun icra ettiği siber operasyonların merkezi Dubai'dir ve grubun bir bölümü de halen Suriye'de bulunmaktadır. Beşşar Esad'ın kuzeni Rami Makhlouf tarafından finanse edilen grup, Suriye diktatörü Beşşar el Esad tarafından 'sanal gerçeklikte gerçek bir ordu' olarak tanımlanmaktadır[53]. IHS Jane's adlı askeri kaynağa göre, SEO'nun temel yöntemi özel hazırlanmış ve gönderilmiş emailler üzerinden alıcıyı bazı linklere yönlendirmek ve SEO'nun ele geçirdiği ya da vandalize ettiği sitelere çekmektir[54]. Grubun siber operasyon sabıkası The Washington Post, UNICEF, ABD Kara Kuvvetleri web-sitesi, Le Monde, International Business Times ve Reuters gibi önemli hedefleri içermektedir[55]. Grubun yeni gönüllüler aradığı ve sızdırdığı bazı bilgileri yayımladığı bir internet sitesi de bulunmaktadır[56].

Açık kaynaklı istihbarat bilgileri de SEO'nun Baas rejimi adına bir siber vekalet savaşı yürüttüğünü doğrulamaktadır. The New York Times'a göre, "eğer araştırmacılar Esad rejiminin bu grup ile yakın bağlarını doğrular ise, devletler [rejime] yanıt vermeyi tercih edebilirler zira bu [grup tarafından düzenlenen] saldırıların somut sonuçları bulunmaktadır." Örneğin SEO, The Associated Press'in Twitter hesabını ele geçirerek Beyaz Saray'da patlamalar olduğuna ilişkin sahte haberler yayarak borsaya ciddi zarar verebilmiştir[57].

Suriye Bilgisayar Topluluğu'nun (SBT) Bassel el Esad tarafından kurulduğu ve daha sonra Beşşar el Esad'ın bu topluluğun başkanlığını yürüttüğü bilinmektedir. SEO'nun nüvesini SBT teşkil etmektedir[58]. Ayrıca, Rami Makhlouf'un grup ile bağları da dikkat çekicidir. Beşşar al Esad'ın annesi Anise el Esad'ın mensup olduğu Makhlouf ailesi her zaman rejimin kilit pozisyonlarında etkili olmuştur. Örneğin, Rami Makhlouf'un kardeşi, Hafız Makhlouf, Suriye'nin oldukça kötü bir namı olan Genel Güvenlik Direktörlüğü'nün iç güvenlik biriminin başkanlığını yürütmüştür. Dahası, Başkanlık Muhafızlarından 105. Tugay Komutanı Tuğgeneral Talal Makhlouf gibi bahse konu aileye mensup generaller de rejimin askeri yapısında önemli yer tutmakta ve hatta özel olarak savaş suçları ve insanlığa karşı işlenen suçlar iddiaları ile anılmaktadırlar[59]. Belirtilen karanlık aile geçmişi ile Rami Makhlouf, Baas rejiminin finansal dinamosu olarak görülmektedir ve yabancı yatırımcılar ile Suriye firmaları arasında köprü olduğu düşünülmektedir[60].

Bu noktada, SBT'nin rolü ve evrimini incelemekte yarar görülmektedir. Beşşar el Esad SBT'nin başkanlığını 1990'lı yıllarda üstlenmiştir. Proje Beşşar'ın 1994'te bir trafik kazasında vefat eden kardeşi Basel tarafından 1989 yılında oluşturulmuştur. SBT projesinin iki amacı bulunmaktadır. Bunlardan ilki çerçevesinde, kontrollü ve tedrici olarak artan bir tempoda rejimin imaj çalışmasının yapılması ve bilgisayar teknolojileri ile internetin rejimin kontrolünde ülkeye girmesi amaçlanmıştır.[61] Diğer yandan ise, kinetik olmayan bir hareket tarzı ile enformasyon harbi ve psikolojik harekât yöntemleri kullanılarak internette Baas rejimi karşıtı propaganda ile mücadele edilmesi hedeflenmiştir[62].

SBT'nin SEO ile bağları, SBT'nin iç savaş koşullarında siber harp gibi bir misyonu olduğunu ve Suriye iç savaşının harbin beşinci boyutu olan siber-uzaya taşındığını göstermesi bakımından önemlidir. Bu çalışma, Suriye Baas rejiminin iç savaş dâhilinde siber harekât ortamında geliştirdiği yüksek deneyimin ve mevcut siber yeteneklerinin, rejimin ayakta kalması durumunda, daha tehditkâr boyutlara varabileceğini değerlendirmektedir. Ayrıca, rejimin müttefiklerinin, özellikle Çin ve İran'ın siber harp yeteneklerinin de rejimin siber harp imkân ve kabiliyetine kritik katkılar yapabileceği düşünülmektedir.

SEO ve SBT'nin yanı sıra, IŞİD bağlantılı Siber-Halifelik Türkiye'nin dikkat etmesi gereken bir diğer aktördür. Grubun en ses getirici siber operasyonu, 8 Nisan 2015 tarihinde Fransız TV5 Monde Televizyonu'nun hacklenmesi ve 'Je suis IS' mesajının yayımlanmasıdır[63]. Daha tehditkâr biçimde, Siber-Halifeliğin anti-IŞİD operasyonlarda yer alan Fransız askerlerinin kişisel kimlik bilgilerini yayımlamış olması da kritiktir[64]. Son olarak, grubun 2015 yılı başlarında ABD Merkez Komutanlığı'nın resmi Twitter hesabını hacklemiş olması da önemlidir[65].

IŞİD'in siber-uzayda geliştirdiği imkân ve kabiliyet ve varlık ciddiye alınmalıdır. Hoffman ve Schweitzer tarafından Nisan 2015 tarihli çalışmalarında belirtildiği gibi:

> "Siber-uzayın cihatçı bir örgüt tarafından kullanılması yeni olmasa da, IŞİD interneti ve özellikle sosyal medyayı diğer terör örgütlerinden oldukça yoğun biçimde kullanmaktadır. Örgütün teknolojik yeteneklerinin yanı sıra, siber-cihat özelliklerinin IŞİD'i herhangi bir köktendinci İslamcı örgütten, Batı ve İslam dünyasında küresel bir markaya dönüştürdüğü görülmektedir. Örgütün Orta Doğu'da ve küresel ölçekte etki alanı oluşturma çabalarının bir parçası olarak, IŞİD Dabık adlı periyodik yayınında propaganda çalışmaları yapmakta ve YouTube, Twitter ve diğer web platformlarında yüksek kalitede görsel yayınlar hazırlamaktadır. Ayrıca, örgüt sosyal ağları kendi gereksinimleri ve hedefleri doğrultusunda daha önce görülmeyen bir

> ölçekte kullanmaktadır. IŞİD Twitter, Facebook, Tumblr ve Instagram'ı etkin biçimde kullanmaktadır ve ABD yetkililerinin ifade ettikleri gibi örgütün mensupları ve destekçileri günde ortalama 90,000 tweet atmaktadırlar. Son yapılan araştırmalarda, IŞİD destekçilerinin 200 – 500 kadarı her gün aktif olarak kullanılan toplam 46,000 Twitter hesabına sahip oldukları belirtilmektedir ve örgüt propagandası bu hesaplar aracılığıyla yayılmaktadır. …Sosyal medya kullanımının yanı sıra, IŞİD'in siber-cihat faaliyetleri web sitelerine saldırıları da içermektedir"[66].

Siber-Halifeliğin faaliyetleri Türkiye açısından özellikle gençlik arasında radikal fikirlerin yayılması bağlamında kritik tehditler oluşturmaktadır, zira Türkiye'de internet kullanımı diğer Orta Doğu ülkelerine göre çok daha yüksektir. Ayrıca, Türkiye'nin IŞİD kaynaklı siber saldırılara maruz kalması, söz konusu saldırıların resmi internet siteleri ile ana akım medyaya yönelik olması da muhtemeldir.

5.1. 2008 Boru Hattı Saldırısı ve 2015 Elektrik Kesintileri: Türkiye için Siber Alarm mı?

Türkiye'ye yönelik siber saldırılar ve faaliyetler çerçevesinde, bu çalışma iki örnek vaka analizine yer verecektir. Bunlardan ilki 2008 yılında Bakü-Tiflis-Ceyhan petrol boru hattında yaşanan patlamalar ve ikincisi de 2015 yılında Türkiye'deki genel elektrik kesintisidir. Erzincan yakınlarında meydana gelen ilk örnek olay kapsamında, Türkiye'deki boru hatlarının her zaman terörist saldırılara karşı kırılgan bir yapıları olduğu belirtilmelidir. 1987 ile 2010 yılları arasında Türkiye'deki boru hatlarına yönelik 59 sabotaj olmuş, söz konusu 59 sabotajın 19'u 2007 ile 2010 yılları arasında gerçekleştirilmiştir[67].

2008 yılında yaşanan saldırıyı ise 'her zamanki saldırılardan biri' olarak tanımlamak mümkün değildir. Bazı kaynakların belirttikleri üzere, "soruşturmanın gizliliğinden ötürü isimlerinin açıklanmasını istemeyen dört kişinin ifadelerine göre, hackerlar alarmları kapatmışlar, iletişimi kesmişler ve borulardaki ham petrolün basıncını yükseltmişlerdir. 30 Ağustos 2008 tarihinde kullanılan esas silah bir 'klavyedir' ve basıncı değiştirerek büyük bir patlamaya neden olmuştur".[68] Bahse konu saldırı Rusya'nın 2008 yılında Gürcistan'da icra ettiği harekât ile aynı döneme rastlamıştır ve bu nedenle şüphe çekmektedir, zira BTC hattı Moskova'nın Avrasya coğrafyasındaki enerji bağlamındaki jeostratejik çıkarlarına ters düşmektedir[69]. Gerçekten de ilgili olayda boru hattı tesislerine yönelik jammer kullanımı, alarm sistemleri ve iletişimin kesilmesi ve uydu sistemleri ile bağlantının kesilmesine yönelik çabalar tespit edildiği bazı kaynaklarca doğrulanmaktadır[70].

Hackerların ilgili olayda güvenlik kamerası kayıtlarını sildiği anlaşılmaktadır. Ancak olay yerini gören kızıl ötesi bir kamera söz konusu tesis yakınında bulunan ve dizüstü bilgisayarlar taşıyan iki kişinin görüntülerini kaydetmiştir[71]. Rusya – Gürcistan Savaşı öncesinde Ankara – Tiflis ilişkileri oldukça yakın bir profildeydi ve Türk yönetimi Gürcistan'ın NATO üyeliğini desteklemiştir. Bu bağlamda, 2008 Rusya – Gürcistan Savaşı sırasında bazı Rus yetkililerin, Ankara'yı, Gürcistan'ı cesaretlendirmek ve askeri destek vermekle suçlaması da dikkat çekicidir[72].

İncelemeye alacağımız ikinci ses getirici siber saldırı iddiası 31 Mart 2015 tarihinde Türkiye'nin 81 ilinin 44'ünü etkileyen elektrik kesintileri ile ilgilidir. Bu olayda siber saldırı ihtimali bizzat Başbakan Ahmet Davutoğlu tarafından dile getirilmiştir ve bazı medya kaynakları saldırının arkasında İran olabileceğini belirtmişlerdir. Bu çerçevede İran'ın söz konusu saldırıyı Cumhurbaşkanı Erdoğan'ın Tahran'ı bölgesel hegemonya kurmakla suçlaması ve Yemen'de Körfez ülkelerinin yürüttüğü operasyonlara destek vermesine cevaben gerçekleştirdiği de söylenmiştir[73]. Gün boyu süren kesintilerin 298 organize sanayi bölgesinde üretimi durdurduğu ve yaklaşık 700 milyon dolara mal olduğu tahmin edilmektedir[74]. Bazı uzmanlar daha kötümser tahminlerde bulunarak zararın 1 milyar doları bulabileceğini öne sürmüşlerdir[75]. Elektriğini doğrudan İran'dan alan Van'ın kesintilerden etkilenmemesi dikkat çekici olsa da[76], henüz teyit edilebilen ve saldırıların failinin İran olduğunu kesin biçimde doğrulayan verilere, kamuya açık kaynaklar ile ulaşmak mümkün olmamıştır.

2010 yılında CSIS adlı ABD merkezli düşünce kuruluşu için kaleme aldığı raporda, James Andrew Lewis elektrik hatlarının siber saldırılara maruz kalabileceğini açık ifadelerle belirtmiştir. Lewis'e göre:

> "Elektrik güç sistemleri her zaman askeri ve gayrinizami unsurlar için yüksek öncelikli hedefler olmuştur. Zira iletim hatlarının havaya uçurulması ya da sistemin kapatılması ve güç santrallerinin hedef alınması gayrinizami unsurlar için her zaman kolay ve ucuz olmuştur. Bu gerilla harbinin normal akışı içinde değerlendirilmelidir. Düzenli ordular da benzer şekilde enerji santrallerini ya da hidroelektrik tesislerini hedef almayı, bir bombardıman operasyonu çerçevesinde planlamaktadırlar. … Idaho Ulusal Laboratuvarlarında gerçekleştirilen Aurora testleri büyük jeneratörlerin kendilerini imha etmelerine ya da zarar vermelerine neden olabilecek uzaktan müdahalelerin mümkün olduğu kanıtlamıştır. Araştırmacılar jeneratörlerin operasyonel döngülerini uzaktan değiştirebilmişlerdir. İlgili kayıtlar jeneratörün sarsıldığını ve dumanlar çıkararak çalışmayı durdurduğunu göstermektedir. … Yine belirlenemeyen yabancı kaynakların elektrik ağlarına yönelik bilgisayar ağı tabanlı müdahalelerine ilişkin kanıtlar mevcuttur. Bazı elektrik şirketleri her ay kaynağı belirlenemeyen benzer

binlerce girişim rapor etmektedirler ancak birçok kez bunun bir askeri keşif faaliyeti mi yoksa siber suç mu olduğunu tam olarak tespit edememekteyiz. Ayrıca elektrik hatlarına yönelik ağ altyapısını hedef alan keşif ve siber saldırı girişimleri ve potansiyel zafiyetleri anlamak için bu çerçevede yapılan çalışmaların olduğu da bilinmektedir[77].

Stratejik olarak elektrik hatları yüksek değerli hedeflerdir zira düşmana doğrudan ve dolaylı zarar verebilme kapasitesine sahiptirler. Askeri bir perspektiften bakıldığında, bir elektrik iletim hattına maksimum zarar yüksek irtifada nükleer patlama ya da siber harp yoluyla verilebilir. Rusya, Çin, İran ve Kuzey Kore gibi devletler kritik milli altyapı hedefleri bağlamında elektrik hatlarına saldırmayı da değerlendirdiklerinin sinyallerini vermişlerdir[78].

5.2. Türkiye'nin Siber Yeteneklerini Geliştirme Çabaları

2015 yılında yaşanan kesintilerin siber saldırı olma ihtimali 2008 boru hattı patlamaları kadar ciddiye alınmamıştır. Öte yandan ilgili kesinti bir siber saldırı sonucu gerçekleşmiş olmasa da bir uyandırma-zili olarak işlev görebilmeli ve günlük bir milyar dolar zarara neden olabilecek ve Türkiye'de günlük hayatı felce uğratacak olası bir siber saldırıya ilişkin, yıkıcı etkileri bağlamında, dikkat çekmelidir. Nitekim Türkiye'de resmi internet ağlarına ve web sitelerine yönelik siber saldırılar Mayıs 2015'ten sonra tedrici olarak gözlemlenmiştir. Belirtilen saldırılar yaklaşık 12 'siber taarruz çıkış hattından' eş zamanlı olarak kurgulanmıştır.

Bakü-Tiflis-Ceyhan petrol boru hattına yönelik 2008 saldırısı Türk karar vericiler için çok değerli dersler içermektedir. Öncelikle, söz konusu saldırı siber taarruzun kinetik etkilerini göstermesi bağlamında önemlidir. İkincisi, bahse konu saldırı bölgesel güvenlik konuları, enerji jeopolitiği ve askeri-siyasi rekabet arasındaki bağlantıyı göstermiştir. Üçüncü olarak, bu siber saldırı kritik milli altyapının zafiyetine ve savaşın beşinci boyutundaki tehditlere dikkat çekmiştir.

BTC saldırısına cevaben, Ankara siber savunma kapasitesini yükseltmeyi hedeflemiştir. Bu çerçevede, 2010 yılında Milli Güvenlik Kurulu konuyu gündemine almış, 2012 yılında da TSK bünyesinde Siber Komutanlık kurulmuştur[79]. 2011 yılında Türkiye ilk milli Siber Güvenlik Tatbikatı'nı icra etmiş, tatbikat kapsamında senaryolar ve kırmızı-takımlar tarafından gerçekleştirilen yıkıcı faaliyetler yer almıştır[80]. Dört yıl sonra Türkiye'nin Kırmızı Kitap olarak bilinen ve Türk Devletinin kurumları için stratejik rehberlik ve doktrin kaynağı olan Milli Güvenlik Siyaset Belgesi, siber güvenliği de esas konuları arasına almıştır[81].

6. Sonuç ve Öneriler

Askeri bir perspektiften bakıldığında, yüksek profilli bir siber silahın, nükleer silah, biyolojik silah, zaman ayarlı bomba, anti-radyasyon füzesi, özel kuvvetler ve bir Orta Çağ kılıcının karakteristik niteliklerini aynı anda taşıdığı söylenebilir. Yüksek profilli bir siber silah bir ölçüde nükleer silah karakteristiği taşır zira kritik milli altyapıyı ciddi biçimde zarar verecek şekilde hedef alabilir; aynı zamanda bir ölçüde biyolojik silahları andırır zira siber saldırının tespit edilmesi ve saldırganın kimliğinin belirlenmesi özel istihbari çalışma gerektirmektedir. Bir boyutuyla anti-radyasyon füzelerine benzemektedir zira sinyalleri izleyerek hedefine varabilir ve daha müteakip saldırılar için zemin hazırlar. Bir ölçüde zaman ayarlı bir bombayı anımsatmaktadır zira saldırı anı ile etki zamanı arasındaki boşluk saldırgan tarafından dizayn edilebilir. Özel ve gizli operasyon unsurları olmaları nedeniyle, siber silahlar bir ölçüde de özel kuvvetler harekâtlarını andırmaktadır. Son olarak, caydırıcılık bağlamında siber silahların bir Orta Çağ şövalyesinin kılıcına benzetilmesi mümkündür zira kılıcı kalkan ile caydırmak olası değildir.

Belirtilen askeri değerlendirmeler ışığında, siber harbin karmaşık bir fenomen olduğu ve savaşı, teknolojik ilerlemenin ötesinde bir değişime zorladığı söylenebilir. Siber harbin içerdiği teknolojik ilerlemeler ve imkânlar, gerek kinetik gerekse kinetik olmayan etkileri ve yetenekleri ile orantılı olarak, yeni doktrinler, teşkilat yapıları, konseptler, stratejik ve taktik yaklaşımlar, taarruzi ve müdafi hareket tarzları ve daha da önemlisi, yeni bir savaşçı sınıfı oluşturmaktadır. Öte yandan, siber harp savaşlar için yeni bir boyutu da tanımlamaktadır. Daha önce belirtildiği üzere, savaşın boyutları birbirleri ile ilintilidir ve çatışma trendleri giderek müşterek harekât konseptlerini ön plana çıkarmaktadır. Bu durum da, hava-kara harekatı, hava-deniz harekatı gibi hususlar, kara, hava ve deniz kuvvetleri unsurlarını giderek daha entegre biçimde çalışmaya itmektedir ve ağ merkezli harekatı da teşvik etmektedir. Son yüzyılda uzayın da bu karmaşık resme dahil olması önem arz etmektedir ve mevcut askeri harekat ortamlarında uzay-tabanlı yetenekler vazgeçilmez bir önem kazanmıştır.

Günümüz itibariyle, füze savunma ya da kıtalararası balistik füze operasyonları gibi karmaşık görevler uzay-tabanlı sistemler olmadan yapılamazlar. Topçu sistemleri, ana muharebe tankları, hatta modern piyade dahi GPS-tabanlı sistemlerden ve taktik istihbarat ağlarından

doğrudan harekât alanında yararlanmaktadırlar.

Siber bağımlılıkta ve ileri elektronik teknoloji altyapısında yaşanan hızlı değişimler siber-uzayın harbin diğer boyutları ile daha güçlü entegre olmasını sağlamaktadır. Bu bağlamda, ağ merkezli harekât konseptleri komuta-kontrol-komünikasyon-bilgisayar-istihbarat-keşif-gözetleme (C4ISR) altyapısı ve hassas güdümlü silahlar bağlamında giderek daha çok bilgisayarlara bağımlı olmaktadır. Bu şartlar altında, siber silahlar düşmanı felce uğratma ve komuta-kontrol altyapılarını körleştirme yetenekleri dolayısıyla önem kazanmaktadır. Ayrıca, elektronik harp, hava kuvvetleri başta olmak üzere birçok askeri kuvvetin ve birliğin faaliyetlerinde giderek artan bir yer tutmaktadır ve siber harp ile daha yakın ilişki geliştirmektedir. Benzer bir durum enformasyon operasyonları ve psikolojik harp için de söylenebilir.

Sonuç olarak, siber harp, harbin yeni bir boyutu ve askeri teknolojik gelişmelerin bir tezahürü olarak ortaya çıkmaktadır. Bu nedenle, Askeri Meselelerde Devrim teorisinin de gerektirdiği şekilde, adaptasyon kapasitesi yalnızca savunmaya ilişkin bir zorunluluk olarak değil, aynı zamanda devlet ve devlet dışı aktörler için taarruzi avantaj kazanılacak bir işlev olarak önem kazanmaktadır. Türkiye 21. yüzyılın karmaşık siber tehdit ortamında bir istisna değildir. Türk ekonomisinin büyümesi enerji altyapısına, elektrik üretimine ve hidro-stratejik öneme sahip barajlara doğrudan bağımlıdır. Türkiye bir enerji geçiş merkezi olmak ya da İstanbul'u bir havayolu ulaşımı merkezi haline getirmek gibi stratejik hedeflerini izlemeyi sürdürmektedir. Türkiye'nin devlet ve özel sektör alanlarındaki veri tabanlarının büyük bölümü, finans ve bankacılık faaliyetlerinin önemli kısmı ve enformasyon akışı dijital ortamda yer almaktadır. Bu nedenle siber güvenlik Türk güvenlik ortamının kritik bir parçasıdır.

Bu çalışma aşağıda paylaşılan önerileri Türk karar vericilerin dikkatlerine sunmaktadır:

- TSK bünyesinde bir Siber Komutanlık kurulması takdirle desteklenmektedir. Türk Siber Komutanlığı ile NATO bünyesindeki Cooperative Cyber Defense Center of Excellence, US CYBERCOM ve diğer müttefik teşkilatlar arasındaki işbirliğinin derinleştirilerek geliştirilmesinde yarar mütalaa edilmektedir.

- 2011 yılında icra edilen ve birçok kurumun katıldığı siber tatbikat takdirle desteklenmektedir. Siber tehditler ile mücadelede kurumlar arası eşgüdüm ve işbirliği hayati önemdedir. Türk Siber Komutanlığı ile ilgili açık kaynaklı bilgiler sürekli ve sistematik kırmızı-takım çalışmasının ve sızma testlerinin eksikliğini göstermektedir. Bu nedenle düzenli olarak siber tatbikatlar düzenlenmesi ve etkili kırmızı takım aktivitesi tavsiye edilmektedir.

- Güvenliğe yönelik yeni meydan okumalar ışığında, Ankara'nın, kritik milli altyapıya yönelik stratejik hesaplarını, siber espiyonaj, ağ merkezli harp, psikolojik harp, enformasyon harbi, elektronik harp ve sinyal istihbaratı gibi alanları da dikkate alarak, siber harp kapsamındaki kinetik ve kinetik olmayan etkiler bağlamında gözden geçirmesinde fayda mütalaa edilmektedir. Böyle bir dönüşüm için farklı disiplinlerden gelecek uzmanlar tarafından oluşturulacak bir komisyon oluşturulmasında yarar görülmektedir. Böyle bir komisyon, MGK Genel Sekreterliği bünyesinde oluşturulabilir ve siber güvenliğe ilişkin tartışmaları devletin zirvesine taşıyabilir. Ayrıca MGK'nın anayasal olarak iki ayda bir toplanması konunun fikri takibi açısından da süreklilik sağlayacaktır.

- Askeri teorik ve doktriner perspektifle, yalnızca siber savunmaya yatırım yapmanın 'tek kanatla uçmak' anlamına geldiği vurgulanmalıdır. Bu nedenle, siber taarruzi faaliyetler için gerekli yasal çerçeve ve yetenekler bağlamında, NATO imkân ve kabiliyetleri ile uyumlu çalışmaların yapılması önem arz etmektedir.

- Bu çalışma, Silahlı Kuvvetler, kolluk güçleri, iç güvenlik istihbaratı, Dışişleri ve yargı makamlarını kapsayacak kurumlar-arası bir yapının kurulmasında yarar görmektedir. Ayrıca, TSK bünyesindeki Siber Komutanlığın seviyesinin yükseltilmesi de ilerleyen yıllar için değerlendirilebilecek bir husustur.

- Siber güvenlik çok disiplinli bir sahada yükselen bir ihtisas alanına karşılık gelmektedir. Bu nedenle, Türk güvenlik güçleri için akademik dünya, düşünce kuruluşları ve özel sektörün de dâhil olduğu yeni eğitim programları oluşturulması yararlı olacaktır.

- Özel sektör ve devlet güvenlik birimleri siber savunma ve güvenliğe yönelik bütüncül bir yaklaşımın vazgeçilmez aktörleridir. Özel sektörün

siber zafiyetleri, birer 'siber taarruz çıkış' hattı olarak olası düşmanların planlarına hizmet edebilir. Ayrıca, dijital sistemlerin karşılıklı bağımlılığı gereği ve bilginin hızlı akışı nedeniyle, güvenlik açıkları yıkıcı siber espiyonaj faaliyetleri için daha karmaşık olanaklar sunabilir. Dahası, Türkiye özel sektör ve devlet arasında siber güvenlik alanında işbirliği için net bir organizasyon modeline veya doktrine sahip değildir. Belirtilen nedenlerle bu çalışma, Türkiye için siber güvenliğe ve savunmaya, hem teşkilat yapılanması hem de kültürel boyutlarda, daha bütünsel ve geniş kapsamlı bir yaklaşımın geliştirilmesini önemle tavsiye etmektedir.

- Nihayet Türkiye'nin siber savunma ve siber saldırı yeteneklerinin geliştirilmesinde NATO'nun bu alandaki potansiyel yöneliminin de önem taşıyacağı açıktır. 2016 yılındaki Varşova Zirvesi öncesinde NATO liderlerinin siber konusu ile ilgili önemli bir karar arifesinde oldukları bilinmektedir. Söz konusu Zirve NATO'nun siber yeteneklerinin geliştirilmesi açısından bir dönüm noktası olabilir. Bu bağlamda NATO içinde süren tartışma, siberin, aynı kara, hava ve deniz gibi ilave bir operasyonel alan olarak tanımlanması ile ilgilidir. Siber alanın bu tanıma kavuşması ile NATO içinde, aynen nükleer alanda olduğu gibi, mevcut siber savunma ve siber saldırı yeteneklerin paylaşılması söz konusu olacak, NATO ittifak halinde ülkelerin siber savunmalarına yardımcı olmakla mükellef olacak ama aynı zamanda ülkelerin tamamlayıcı siber yetenekler geliştirmeleri hususunda da bir rol üstlenecek ve bununla ilgili bir yol haritası çıkaracaktır.

- Türkiye, NATO'nun bu daha iddialı siber doktrinine yönelmesini savunan müttefik ülkeler arasındadır. Buna karşılık, ABD gibi kısmen kendi mevcut yeteneklerini açıklamak ve bunları bu aşamada diğer NATO müttefiklerine destek vermek için kullanmak istemeyen ülkeler olduğu gibi, Fransa gibi siber güvenlik konusunda NATO yerine AB'nin öncü rol üstlenmesini isteyen ülkeler de bulunmaktadır. Ancak Türkiye'nin Aralık ayı içinde karşılaştığı siber saldırı gibi örneklerin de önümüzdeki dönemde artması muhtemel olduğundan, NATO liderlerinin, 2016 Varşova Zirvesinde İttifakın siber doktrinini, bu alandaki görev ve yeteneklerini güçlendirme yönünde karar almaları beklenmektedir. Böylesine bir karar Türkiye'nin de siber alanda yeni adımlar atmasını ve yeteneklerini geliştirme yönünde daha tutarlı bir iradeye sahip olmasını beraberinde getirecektir.

1- T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, SOME-Sektörel Kurulum ve Yönetim Rehberi, 2014.

2- Türkiye'nin Siber Güvenlik Ulusal Eylem Planı, http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1- 1.pdf, Erişim tarihi: 7 Temmuz 2015.

3- http://www.radikal.com.tr/teknoloji/tskda_siber_ordu_icin_onemli_adim-1194093, Erişim tarihi: 29 Haziran 2015.

4- James A, Lewis., Assessing the Risk of Cyber Terrorism, Cyber War and Other Cyber Threats, CSIS, 2002. s.2.

5- Steven Metz ve James Kievit., Strategy and Revolution in Military Affairs: From Theory to Policy, US Army SSI, 1995, ss. 2-3.

6- Andrew Krepinevich., "Cavalry to computer; the pattern of military revolutions." The National Interest n37 (Fall 1994 n37): 30(13). General Reference Center Gold. Thomson Gale. University of Florida. 19 Kasım 2006.

7- Barry D. Watts, The Maturing Revolution in Military Affairs, CSBA, 2011, ss.15-20.

8- Erik Gartzke., "The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth", University of California, 2012, ss.28-29.

9- Paul J Springer., Thinking about Military History in an Age of Drones, Hackers, and IEDs, Air Command and Staff College, http://www.fpri.org/docs/springer1.pdf, Erişim tarihi: 7 Temmuz 2015.

10- Roma hafif piyadesi için bkz: Adam, O. Anders., Roman Light Infantry and the Art of Combat, Cardiff University, 2011.

11- James A. Lewis., The Role of Offensive Cyber Operations in NATO's Collective Defense, The Tallinn Papers, CCDCOE, 2015, s.3.

12- John Arquilla and David Ronfeldt. "Cyber War is Coming" in In Athena's Camp: Preparing for Conflict in the Information Age, RAND/MR-880-OSD/RC 1997, s.24

13- A.g.e. s.30

14- A.g.e.

15- A.g.e. s.23.

16- Jennifer, J. Li and Lindsay Daugherty, Training Cyber Warriors, RAND, 2015, s..xi.

17- Detaylı savunma harcamaları için bkz: IISS, Military Balance 2014.

18- US Cyber Command Fact Sheet, 25 Mayıs 2010, http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED %20replaces%20May%2021%20Fact%20Sheet.pdf, Erişim tarihi: 29 Haziran 2015.

19- A.g.e.

20- http://www.al-monitor.com/pulse/originals/2015/06/israel-idf-cyber-intelligence-new-unit-eisenkot-war- future.html, Erişim tarihi: 29 Haziran 2015.

21- http://www.defensenews.com/story/defense/policy-budget/cyber/2015/06/24/israel-target-for-iranian- hezbollah-cyber-attacks/29210755/, Erişim tarihi: 29 Haziran 2015.

22- Joel Mullish. "Russia's Growing Reliance on Cyber Warfare Setting Dangerous Precedent for Future Foreign Policy", INSS, http://www.inss.org.il/uploadImages/systemFiles/Russia's%20growing%20reliance%20on %20cyber%20warfare%20setting%20dangerous%20precedent%20for%20future%20foreign%20policy.pdf, Erişim tarihi: 29 Haziran 2015.

23- NATO CCDCOE, https://ccdcoe.org/, Erişim tarihi: 29 Haziran 2015.

24- NATO, Cyber Security, http://www.nato.int/cps/en/natohq/topics_78170.htm, Erişim tarihi: 29 Haziran 2015.

25- Magnus Hjortdal., "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence", Journal of Strategic Studies, Cilt: 4 No: 2, Yaz 2011.

26- Detaylı bilgi için bkz: Mandiant, APT1: Exposing One of China's Cyber Espionage Units, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf, Erişim tarihi: 28 Temmuz 2015.

27- Eric, M. Hutchins v.d. Intelligence Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven- Defense.pdf, Erişim tarihi: 29 Temmuz 2015.

28- A.g.e.

29- Larry M. Wortzel., The Chinese People's Liberation Army and Information Warfare, US Army SSI, 2014, pp.1-8.

30- A.g.e. ss.12-13.

31- Ilan Berman., The Iranian Cyber Threat Revisited, ABD Temsilciler Meclisi, Siber Güvenlik, Altyapı Koruması ve Güvenlik Teknolojileri Yurtiçi Güvenlik Alt-Komitesi önünde sunulan bildirge, 2013, s.2.

32- James Andrew Lewis., Cybersecurity and Stability in the Gulf, CSIS, Ocak 2014.

33- Executive Cyber Intelligence, INSS-CSFI, Nisan 1, 2015.

34- Jason, P. Patterson and Matthew, N. Smith., Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran, Naval Postgraduate School, 2005, s.44.

35- A.g.e, ss.44-50.

36- James Andrew Lewis., Cybersecurity and Stability in the Gulf, CSIS, Ocak 2014.

37- Craig Stallard., At the Crossroads of Cyber Warfare: Signposts for the Royal Australian Air Force, School of Advanced Air and Space Studies, Maxwell Air Force Base, 2011, ss.35-36.

38- A.g.e.

39- A.g.e.

40- Martin, C. Libicki., "The Specter of Non-Obvious Warfare", Strategic Studies Quarterly, Güz 2012.

41- Samuel Liles. vd. "Applying Traditional Military Principles to Cyber Warfare", 4th International Conference on Cyber Conflict, C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), 2012, s.171.

42- Jeffrey R. Witsken., Network-Centric Warfare: Implications for Operational Design, School of Advanced Military Studies-US Army Command and General Staff College, 2002, s.3.

43- A.g.e. ss.17-18.

44- Alvin L. Bailey., The Implications of Network Centric Warfare, US Army War College, 2004, ss.2-3.

45- Lior Tabansky., "Basics Concepts in Cyber Warfare", Military and Strategic Affairs, Cilt: 3 No: 1, Mayıs 2011.

46- Erik Gartzke., "The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth", University of California, 2012, s.25.

47- Andrew F. Krepinevich., Cyber Warfare: A Nuclear Option, CSBA, 2012, s.66.

48- Thomas Rid and Peter McBurney, "Cyber Weapons", The Rusi Journal, Şubat/ Mart 2012, Cilt: 157 No: 1, s.6.

49- Austin Miller. Advanced Anti-Radiation Guided Missile: Strengthening DEAD Capability in the Fleet, 43rd Annual Systems: Gun and Missile Systems Conference and Exhibition, Nisan 21-24 2008 Brief.

50- Thomas Rid and Peter McBurney, "Cyber Weapons", The Rusi Journal, Şubat/ Mart 2012, Vol: 157 No: 1, s.8.

51- Lior Tabansky., "Basics Concepts in Cyber Warfare", Military and Strategic Affairs, Cilt: 3 No: 1, Mayıs 2011.

52- Mehmet Nesip Ogun and Adem Kaya., "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", Güvenlik Stratejileri, Yıl: 9 Sayı: 18, s. 147.

53- Jane's Intelligence Review, Middle East Conflict Spills into Cyberspace, 2015, ss.3-4.

54- A.g.e.

55- http://sea.sy/index/en, Erişim tarihi: 28 Haziran 2015.

56- A.g.e.

57- http://www.nytimes.com/2013/05/18/technology/financial-times-site-is-hacked.html?pagewanted=all&_r=1, Erişim tarihi: 28 Haziran 2015.

58- A.g.e.

59- Human Rights Watch, By All Means Necessary: Individual and Command Responsibility for Crimes Against Humanity in Syria, 2011, s.87.

60- Jeremy M Sharp., Unrest in Syria and U.S. Sanctions Against the Assad

Regime, Congressional Research Service, 2011, s.4.

61- 1990'lı yılların ortalarında Suriye'de her 1000 kişi başına 2 bilgisayar düştüğü ve 1997'de 400 Suriyeliden oluşan pilot bir grubun internete erişimine izin verildiği belirtilmelidir.

62- John B Alterman., New Media New Politics: From Satellite Television to the Internet in the Arab World, Washington Institute for Near East Policy, 1998, ss.40-41.

63- http://rt.com/news/248073-islamic-state-hackers-french-tv/, Erişim tarihi: 28 Haziran 2015.

64- A.g.e.

65- http://rt.com/usa/221927-central-command-hackedcybercaliphate/, Erişim tarihi: 28 Haziran 2015.

66- Adam Hoffman and Yoram Schweitzer. "Cyber Jihad in the Service of the Islamic State (ISIS)", Strategic Assessment, Cilt: 18 No: 1, Nisan 2015, s.73

67- USAK, Kritik Enerji Altyapı Güvenliği Sonuç Raporu, No: 4, 2011.

68- http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new- cyberwar, Erişim tarihi: 29 Haziran 2015.

69- A.g.e.

70- http://www.milliyet.com.tr/siber-savasin-miladi/dunya/detay/1982549/default.htm, Erişim tarihi: 29 Haziran 2015

71- A.g.e.

72- http://www.hurriyet.com.tr/dunya/9623756.asp, Erişim tarihi: 29 Haziran 2015.

73- http://www.dailysabah.com/diplomacy/2015/04/28/iran-allegedly-behind-nationwide-power-outage, Erişim tarihi: 29 Haziran 2015.

74- http://www.hurriyet.com.tr/ekonomi/28611619.asp, Erişim tarihi: 29 Haziran 2015.

75- EDAM, Elektrik Altyapısı ve Siber Güvenlik, 2015. http://www.edam.org.tr/tr/IcerikFiles?id=1028, Erişim tarihi: 3 Ağustos 2015.

76- http://www.hurriyet.com.tr/gundem/28604226.asp, Erişim tarihi: 29 Haziran 2015.

77- James A. Lewis., The Electrical Grid as a Target for Cyber Attack, CSIS, 2010.

78- Cynthia E. Ayers and Kenneth D. Chrosniak., Terminal Blackout: Critical Electric Infrastructure Vulnerabilities and Civil-Military Resiliency, US Army War College Center for Strategic Leadership and Development, Issue Paper, Cilt 1- 13, 2013.

79- http://www.radikal.com.tr/teknoloji/tskda_siber_ordu_icin_onemli_adim-1194093, Erişim tarihi: 29 Haziran 2015.

80- Bilgi Teknolojileri ve İletişim Kurumu, http://www.tk.gov.tr/sayfa.php?ID=28, Erişim tarihi: 29 Haziran 2015.

81- http://www.haberler.com/tsk-siber-savunma-komutanligi-ndan-hacker-atagi-7035427-haberi/, Erişim tarihi: 29 Haziran 2015.