Siber Savaş

Barış ERDOĞAN

Millî Güvenlik ve Askerî Bilimler Akademik Dergisi
Journal of National Security and Military Sciences
İlkbahar/Spring 2014, Cilt/Volume 1, Sayı/No 2, 171-192

Siber Savaş

Barış ERDOĞAN*

Öz

Bu makalenin amacı, siber savaşın uluslararası düzen içerisinde artan önemini ve milli güvenliğimize etkilerini ortaya koymaktır. Bu amaçla makalede, önce siber savaş teorisi üzerinde tartışılarak siber savaşın asimetrik doğasının anlaşılması hedeflenmiştir. Ulus devletler, siber ortam diye de adlandırabileceğimiz bu yeni mücadele alanında, üstünlük sağlamak için hasmın gücünü en az çaba sarf ederek istismar etmek istemektedirler. Siber savaşın güç mücadelesinde önemli yer kazanmasının sebebinin sağladığı bu asimetri olduğu değerlendirilmektedir. Buna karşın güçlü devletler siber savaşta hasımlarına karşı caydırıcılık silahını da kullanmaktadırlar. Güçlü devletler, konvansiyonel veya nükleer güçleri ile sağladıkları caydırıcılığın yanı sıra Birleşmiş Milletler sistemi içinde yer alan Güvenlik Konseyi gibi mekanizmalarında işgal ettikleri imtiyazlı konumu da istismar ederek toplam güçleri üzerinde çarpan etkisi yaratmayı hedeflemektedirler. Sonuç olarak teknolojide yaşanan gelişmeler klasik güvenlik algısı ve stratejilerinde geriye dönülmez dönüşümlere sebep olmuştur. Milli güvenliğimizi tehdit edebilecek risklerin değerlendirilerek gerekli yapıların kurulması için orta ve uzun vadede çalışmaların yapılması gerekmektedir.

Anahtar Kelimeler: : Siber savaş, siber, siber saldırı, siber savaş tartışmaları.

Cyber Warfare

Abstract

The main aim of this article is to emphasize the importance of cyber warfare in the international order and its potential effects to our national security. Discussing the theory behind cyber warfare allows us to better understand the its asymmetrical nature, and its role in modern warfare more generally. Nation states are anxious to gain superiority by trying to deter the adversary with the minimum effort possible. Cyber warfare has gained importance since it creates asymmetry in the struggle for power in the international order. In addition to asymmetrical means, powerful states are using their absolute power to deter potential adversaries, including conventional and nuclear power. Alongside military power, some states are able to leverage their privileged status in the United Nations Security Council as a means of enhancing their total power. Developments in information and telecommunications technologies have caused an irreversible transformation in classical security perceptions and strategies. Risks that can threaten national security should be evaluated accordingly, and the structures that are needed for the mid-to-long term should be established.

Keywords: Cyber warfare, cyber, cyber attack, cyber war discussions.

* bariserdogan@hotmail.com

Giriş

Yirminci yüzyılın ortasından itibaren bilgi ve iletişim teknolojilerinde yaşanan gelişmeler klasik güvenlik algısı ve stratejilerinde geriye dönülmez dönüşümlere sebep olmuştur. İnternet, bahse konu teknolojik gelişmelerin ulusal güvenlik stratejilerini ve algılarını başlı başına değiştirmesi bakımından bu makalenin yazılmasına sebep olan en büyük etkendir.

İnternet, 1950'li yıllarda Amerikan Savunma Bakanlığı tarafından askeri unsurların haberleşme ihtiyaçlarının giderilmesi için desteklenen bir AR-GE projesi (ARPANET) olarak ortaya çıkmış bir ağ konseptidir. Sonrasında üniversiteleri de kapsayacak şekilde gelişmiş ve sonunda tüm dünyaya yayılmıştır. Teknik olarak paket anahtarlama mantığı üzerine kurulmuş bu ağ konsepti, sonrasında TCP/IP ağ protokolünün devreye girmesiyle internetin ana omurgasını oluşturmuştur. Bugün bu omurga fiilen (*de facto*) siber uzay veya siber ortam ile eşanlamlı olarak kullanılmaktadır, oysa ki siber ortam sadece bilgisayar ağlarının birbirine belli protokollerle bağlandığı bir ortama indirgenemez. Siber ortam, içinde algılayıcıların, kontrolcülerin, sinyallerin, bağlantı ve iletişimin de doğrudan veya dolaylı etkileşimde bulundukları elektromanyetik tayf[1] içinde yer alan tüm bileşenleri kapsamaktadır. Son yıllarda yaşamımız pek çok yönüyle bu sayısal ortama göç etmektedir, bu bağlamda gözle görülmeyen ama hayatımızla bütünleşmiş, sürekli genişleyen bir ortamdan bahsettiğimizi söylemek doğru olacaktır.

Siber ortam ile ortaya çıkan yeni mücadele alanı, çıkar çatışması ve nüfuz mücadelesi bağlamında uluslararası güvenlik ve tehdit algılamalarında da birtakım değişimlere neden olmuştur. Devletler, tehdit veya risk olarak algıladıkları yeni durumlar karşısında stratejilerini belirleyerek kabiliyetleri çerçevesinde tedbir almak durumundadır. Siber ortam yeni bir risk ve tehdit alanı olarak ortaya çıkmış ve ulusal çıkarların korunması adına ülkemizin öncelikli olarak kapasite geliştirmesi gereken bir alan haline gelmiştir. Dünya düzeni pek çok düşünce ekolü ile açıklanmaya çalışılsa da teknolojik gelişmeler devletler arası ilişki biçimlerini de dönüştürmektedir. Güç mücadelesi üzerine kurulmuş bu düzende, güçlerini artırmak ve en azından muhafaza etmek isteyen oyuncular için çıkar savaşı artık kara, hava, deniz ve uzayın dışında siber ortama da sıçramış ve yirmi birinci yüzyılda siber savaşın bu güç mücadelesinin merkezine oturacağı değerlendirilmektedir.

Siber Savaş ve Asimetri

Taktik seviyede farklılaşmasına rağmen, stratejik hedefler göz önüne alındığında siber savaş tanımlanırken yeni bir savaş tanımı yapmak gerekmediği görülmektedir. Siber savaşın siber ortamda gerçekleşen bir mücadele olduğu, ancak sonuçlarının fiziksel ortama etkisi sebebiyle kolaylıkla kara, deniz, hava gibi askerî bir mücadele olarak değerlendirilebileceği söylenebilir.

Asimetrik savaş ile karşı karşıya olan büyük güçler, kaynağı pek çok durumda belirlenemeyen, belirlendiği durumlarda da bir devlet ile ilişkilendirilmesi oldukça güç olan saldırılara karşı Birleşmiş Milletler sistemi içerisinde yasal ve ahlaki cevap vermek için hukuki zemin oluşturmaya çalışmaktadırlar. Ancak, Güvenlik Konseyi daimi üyesi olmayan devletler için bahse konu hukuki zemin oluşsa bile, makalenin ilerleyen bölümlerinde İran örneğinde tartışılacağı gibi, meşru müdafaa hakkının kullanılması, onarılması güç fiili durumların yaşanmasına sebep olacaktır.

Bu tartışmadan önce siber savaş stratejisinin belkemiğini oluşturan asimetrik savaş olgusu incelenmelidir. İnsanoğlu binlerce yıldır savaş olgusu ile iç içedir. Önce insanın doğa ile savaşı başlamış, ardından nüfusun çoğalması ile birlikte kaynakların paylaşılması sorunu insanları birbirleriyle savaşır hale getirmiştir. Zaman içinde kabileler, derken devletler arasında savaşlar yaşanmış ve son olarak dünya savaşları ile birlikte savaşın yapısında ve ölçeğinde büyük değişimler olmuştur.

Clausewitz'in (2011), "Savaş Üzerine" adlı eserinde belirttiği gibi, devletlerin ulusal çıkarları çerçevesinde siyasi hedeflerini gerçekleştirmesinde, savaş siyasetin farklı yollardan devamıdır. Tarih boyunca ateşli silahların icadı veya nükleer teknolojinin kıtalararası balistik füzelere yüklenmesi gibi savaş alanını doğrudan etkileyen gelişmeler yaşanmasına rağmen, insanlık tarihi güçsüzün güçlüyü yenebildiği pek çok hadiseye şahit olmuştur. Bu noktada asimetri kavramı devreye girmektedir.

Asimetri sözcüğünü incelerken öncelikle Fransızca "*symétrie*" kelimesine bakmak gerekir. Simetri, Türk Dil Kurumu sözlüğünde "İki veya daha çok şey arasında konum, biçim ve belirli bir eksene göre ölçü uygunluğu, bakışım" diye tanımlanmaktadır. Asimetride ise bu karşılaştırmayı yapmak için ortak bir parametre veya yapıdan bahsetmek mümkün değildir. Savaş alanına yansıttığımızda, asimetri denk olmayanların mücadele ortamını tanımlamaktadır. Clausewitz'den farklı olarak Sun Tzu öğretisi dikkate alındığında, tüm savaşların asimetrik olduğu söylenebilir; çünkü Sun Tzu'ya göre amaç düşmanın zayıflıklarına saldırarak gücünün istismar edilmesi olmalıdır.

Siber ortamda devletler her zaman güçleri ile doğru orantılı olarak mücadele edemedikleri için, siber savaş benzer bir asimetrinin yaşanmasını sağlamaktadır. Bu asimetri Estonya, Gürcistan ve İran örneklerinde olduğu gibi bilgi üstünlüğüne sahip taraf lehine büyük avantaj sağlamaktadır. Önümüzdeki dönemde konvansiyonel olarak yenilmesi mümkün olmayan hasmın mağlup edilmesini mümkün kılabilecek bu tür asimetrik olaylara rastlanacaktır.

Önemli Siber Saldırı Vakaları

Bugüne değin siber savaş ile ilgili olarak dünya kamuoyunun gündemine gelen

pek çok hadise yaşanmıştır. Bununla beraber karakteristik özellikleri bakımından özellikle 2007-2010 yılları arasında Estonya, Gürcistan ve İran'da yaşanan hadiseler mihenk taşı özelliğini taşımaktadır. Vakaların teknik detaylarını incelemeden önce bu üç siber saldırının neden önem arz ettiğine değinmek gerekir.

Estonya saldırısı dünya kamuoyunun siber savaş olgusuna hazırlıksız yakalandığı tarihi göstermesi açısından önem arz etmektedir. Daha önceleri kendi kendine güdülenmiş bireyler, ya da küresel şirketler tarafından tutulan profesyoneller veya devlet destekli casusluk faaliyetleri için gerçekleştirilen siber saldırılar tarihte ilk defa doğrudan bir devlete karşı gerçekleştirilmiştir.

Gürcistan'a yapılan siber saldırıda ise farklı bir ilkle karşı karşıya kalınmış, kinetik saldırı ile eş zamanlı olarak siber saldırıların gerçekleştirildiği görülmüştür. Buradan hareketle siber saldırının muharebe içinde yer alan unsurlardan biri olarak ortaya çıktığı görülmüştür.

İran'a yapılan siber saldırıda ise diğer iki vakada görülenin aksine, fiziksel zarara yol açmıştır. Kuvvet kullanma biçimi daha önce yaşanan askerî çatışmaların aksine kinetik bir eylem içermese de sonuçları değerlendirildiğinde etkileri silahlı saldırı düzeyine yükselmiştir. Bu hadisede güç kullanım sınırı aşılarak siber saldırının savaşın doğrudan ana unsuru halini aldığı görülmüştür. 2007 ile 2010 yılları arasında geçen süre zarfında ülkelerin kapasite geliştirme faaliyetlerinin geldiği noktayı göstermesi açısından da İran'a karşı yapılan siber saldırı dikkat çekicidir.

Vakalar üzerinde tartıştıktan sonra, bu yeni mücadele alanında başta Amerika Birleşik Devletleri, Rusya ve Çin gibi oyuncuların aldıkları pozisyonlar değerlendirilerek orta ve uzun vadede siber savaşın ülkemize ve ulusal çıkarlarımıza etkisi üzerinde düşünülmelidir.

Estonya'ya Karşı Gerçekleştirilen Siber Saldırı

Siber savaşın dünya gündemine oturmasına sebep olan en büyük hadise 2007 yılında Estonya'ya yapılan siber saldırılardır. Bu saldırının arka planını oluşturan sosyal ve siyasi dinamikler irdelenmeden sağlıklı analiz yapmak mümkün olmayacaktır.

Estonya yaklaşık elli yıl süren Sovyet hakimiyetinin ardından 1991 yılında bağımsızlığına kavuşmuştur.[2] Estonya Hükumeti, Nisan 2007'de aldığı kararla başkent Tallinn'in merkezinde bulunan ve 1947 yılında II. Dünya Savaşı'nda ölen Sovyet askerleri anısına dikilen anıtın şehir merkezi dışına taşınmasına karar vermiştir.[3] Bu kararın alınmasının ardından Estonya, daha önce hiç yaşanmayan büyüklükte protestolara sahne olmuş ve anıtın taşınmasını izleyen günlerde sokaklarda şiddet içeren eylemler devam etmiştir. Aslında bu heykelin taşınması ile ortaya çıkan şiddet eylemleri 1991 yılında yeniden bağımsızlığını ilan eden Es-

tonya'da gün geçtikçe artan Rus karşıtı politikalar ile nüfus içinde oranı %30'u bulan[4] Rus kökenli vatandaşlara uygulanan asimilasyon politikalarının bir uzantısı olarak görülebilir.

Sokak eylemlerinin başlamasından bir gün sonra 27 Nisan 2007 tarihinde gece geç saatlerde siber saldırılar başlamış, Eston Hükumetine bağlı kurum ve kuruluşlara ait internet siteleri saldırıya uğramıştır. Daha sonra Eston haber siteleri ile kamu ve özel kuruluşlara ait internet siteleri de bu saldırılara hedef olmuştur.[5] Dalgalar halinde gerçekleşen bu saldırılar üç haftadan uzun süre devam etmiş, Estonya ile Rusya arasında yaşanan gerginliğin azalması ile Mayıs ayı ortalarında saldırıya yönelik ağ trafiğinde azalma başlamıştır. Mayıs ayının sonuna gelindiğinde saldırıların şiddeti iyice azalmış ve ay sonunda sönüme ulaşmıştır.

Estonya'ya karşı yapılan siber saldırı; Estonya'da konuşlu Müşterek Siber Savunma Mükemmeliyet Merkezi tarafından yayınlanan raporda, ilk saldırı safhasının başladığı 27 Nisan 2007 tarihi ile ikinci safhanın bittiği 15 Mayıs 2007 tarihleri arasında birbirini takip eden iki safha olarak incelenmiştir. Birinci safhada, saldırılar daha çok internet forumları aracılığı ile siber saldırıya katılmak isteyenlere anlatılan basit tekniklerin siber eylemciler tarafından uygulanması ile başlamıştır. Forumlarda tarif edilen komut ve betikler her ne kadar basit olsa da pek çok kişi tarafından ortak hedeflere eş zamanlı olarak uygulanması sebebiyle Dağıtık Hizmet Dışı Bırakma Saldırısı (DDOS) olarak adlandırılan bu ilk safha saldırının başarılı olmasını sağlamıştır.

İkinci safha ise 30 Nisan -18 Mayıs 2007 tarihleri arasında yaşanan evredir. Bu evrede, siber saldırılar birinci evrenin aksine daha profesyonel ve karmaşık teknikler kullanılarak icra edilmiştir. Bu evrede köleleştirilmiş (Zombi)[6] bilgisayarlardan oluşan robot ağların (BOTNET)[7] kullanıldığı gözlemlenmiştir. Sırasıyla kamu internet sitelerine ve Alan Adı Sunucularına (DNS)[8] Dağıtık Hizmet Dışı Bırakma (DDoS) saldırıları gerçekleştirilmiştir. Daha sonra Dağıtık Hizmet Dışı Bırakma saldırılarının dozu artırılarak hedefler arasında yer alan kamuya ait pek çok internet sitesinin çalışmaz hale gelmesi sağlanmıştır. Devamında ise özellikle bankacılık ve mali sektöre yönelik saldırılar yoğunlaşarak, saldırının sönümlenmeye başladığı Mayıs ayı ortasına kadar devam etmişti (Tikk, 2010).

Siber saldırıların hedefi göz önünde bulundurulduğunda belirli hedeflere odaklandığı gözlemlenebilir. Öncelikli olarak Eston internet altyapısından sorumlu kurumların sunucuları ile kamu itibarını zedelemek amacıyla kamu kurumları, parlamento ve siyasi partilerin internet sayfaları hedef alınmıştır. Bunun dışında bankacılık ve finans alanında özel sektöre ait hedefler seçilerek etkinin artırılması planlanmıştır. O dönemde Estonya alan adı hizmetini yöneten KBFI'nin (Ulusal Kimya Fizik Biyoloji Enstitüsü) sunucuları internet forumları üzerinden servis edilen ufak betik ve teknik bilgiler aracılığıyla siber saldırılara hedef gösterilmiştir. Aynı şekilde o dönemde tüm kamu kurumlarının ve akademik kurumların inter-

net sunucularını yöneten EENet[9] de benzer saldırılara maruz kalmıştır. İnternet altyapısını çökertmeyi amaçlayan bu saldırıların yanı sıra dünya kamuoyunda daha çok yer bulacak kamu kurumları ve siyasi hedefler de unutulmamıştır. Bu bağlamda, Estonya Parlamentosu ile Cumhurbaşkanlığı, Başbakanlık ve neredeyse tüm bakanlıkların internet sayfaları ile ana muhalefet partisinin sayfaları da saldırıya uğramıştır. Özellikle internet bankacılığının yaygın olarak kullanıldığı Estonya'da Hansapank ve SEB Eesti Ühispank gibi Estonların %80'i tarafından kullanılan iki bankanın çevrimiçi bankacılık hizmeti veren internet siteleri 9-15 Mayıs tarihleri arasında belirli aralıklarla günde iki saate yakın çalışmaz hale getirilmiştir. Bunun dışında özel sektöre ait internet hizmet sağlayıcıları ile Estonlar tarafından yoğunlukla ziyaret edilen büyük haber sitelerinde de sık sık kesintiler yaşanmıştır.

Özellikle dağıtık hizmet dışı bırakma saldırıları, köleleştirilmiş Zombi bilgisayarların temel olarak kullanılması sebebiyle pek çok farklı coğrafi noktadan saldırı yapmaya imkan sağlamaktadır. Bu köle bilgisayarların yönetildiği asıl merkezin belirlenmesi oldukça güçtür. Pek çok durumda saldırgan taraf, siber saldırıları hasmın dost ve müttefik olduğu ülkelerden gerçekleştirmektedir. NATO Müşterek Siber Savunma Mükemmeliyet Merkezi'nin 2010 yılında yayınladığı rapora göre Estonya'ya karşı gerçekleştirilen siber saldırının 178 ayrı ülkeden gerçekleştirildiği bilgisi yer almaktadır. Bahse konu siber saldırının tarihsel gelişimi ve yaşanan olaylar göz önüne alındığında uluslararası kamuoyunda saldırının arkasında Rusya olduğu dile getirilse de bugüne kadar yaşanan siber saldırılar ile Rus devletinin ilişkisi kanıtlanamamıştır.

Siber saldırıların Estonya üzerinde doğrudan ekonomik ve sosyal etkileri olmuştur. Yoğun olarak internet altyapısı üzerinden kullanılan bankacılık işlemlerine ek olarak pek çok e-Devlet hizmeti de sekteye uğramıştır. Estonya'nın siber saldırılardan bu derece etkilenmesinin bir diğer sebebi de bilişim teknolojileri altyapısına olan bağımlılık olarak göze çarpmaktadır. 1,3 milyon nüfusa sahip olan Estonya, kamu hizmetlerinin maliyet etkin biçimde sağlanması için e-Devlet çalışmalarına doksanların ortalarında başlamış ve iki binli yıllara gelindiğinde büyük mesafe kat edilmiştir. Bu gelişmeler çerçevesinde 2007 yılı itibariyle Estonya sınırlarının %98'inde internet erişimi olup, bankacılık işlemlerinin %95'i internet bankacılığı üzerinden gerçekleşmekte idi. İnternet üzerinden gerçekleştirilen işlemlerin yaygın olması sebebiyle pek çok hizmet için ayrılan personel sayısının kısıtlı olması, sistemler ayağa kalkana kadar pek çok hizmetin sağlanamamasına sebep olmuş, bu da maddi kayıplara yol açmıştır. Bilişim teknolojileri alanında ön plana çıkan Estonya için bu saldırı, maddi kayıpların yanı sıra, saldırı karşısında ortaya çıkan çaresizlik nedeniyle özgüven kaybına neden olmuştur. Siber saldırı esnasında ilk etapta Eston yetkililer tarafından Rusya Federasyonu'nun suçlanması, buna rağmen saldırı sırasında ve sonrasında yapılan analizler sonucu saldırının herhangi bir devlet ile ilişkilendirilememesi Dağıtık Hizmet Dışı Bırakma Saldı-

rılarının karakteristik özelliğidir ve iki devlet arasındaki ilişkilerin gerilmesine sebep olmuştur.

Estonya, siber saldırılara karşı tedbirler almaya çalışmıştır. İnternet altyapısını kullanılamaz hale getiren hizmet dışı bırakma saldırılarına karşı kamu sistemi sunucularına erişimin daha rahat sağlanabilmesi için bant genişliği arttırılmıştır. Bu sayede daha büyük çaplı saldırılara dayanacak kapasiteye erişilmiştir. Servis sağlayıcıların internet trafiğini filtreleme çabası ile başlayan önlemler daha sonra açıklık barındıran sistemlerin güvenlik yamalarının yapılması, güvenlik duvarı ve saldırı tespit sistemlerinin devreye alınması ile güvenliğin tekrar tesis edilmesine yardımcı olmuştur. Ayrıca NATO ve Amerika Birleşik Devletleri'nden teknik danışmanlık ve yardım talep edilmiştir. Bu konuda eşgüdüm Eston Savunma Bakanlığı tarafından sağlanmıştır.

Gürcistan'a Karşı Gerçekleştirilen Siber Saldırı

Siber savaşın dünya gündeminde kinetik bir savaş ile birlikte anılmasına sebep olan hadise 2008 yılında Gürcistan'a karşı gerçekleştirilen kara saldırısı ile neredeyse eşzamanlı gerçekleşen siber saldırıdır. Bu saldırının arkasında Gürcistan ile Rusya arasındaki Güney Osetya sorunu yatmaktadır.

1990'da Gürcistan'dan bağımsızlığını ilan eden Güney Osetya fiilen (*de facto*) kazandığı bağımsızlığını korumak için Gürcistan'la 2008 öncesinde de üç kez çatışmaya girmiştir. 1991'de çıkan çatışmaların sonrasında pek çok ateşkes ve barış girişimi olmasına rağmen bölgede tansiyon düşürülememiştir. 7 Ağustos 2008 tarihinde Gürcistan güçleri tarafında yapılan müdahaleden iki hafta önce henüz Rusya Federasyonu da Güney Osetya bölgesine girerek müdahalede bulunmamışken, Gürcistan devletine ait kamu kurumlarının internet sitelerine karşı siber saldırılar başlamıştır. Siber saldırılar, askerî hareketliliğin 12 Ağustos 2008 tarihinde bir ateşkes antlaşması ile sona ermesinin ardından Ağustos ayı sonlarına kadar devam etmiştir.

Siber saldırıların hedefi göz önünde bulundurulduğunda yine Estonya saldırısına benzer hedeflerin seçildiği görülmektedir. Bu bağlamda kamu kurumları ile Cumhurbaşkanlığı, Başbakanlık ve bakanlıkların internet sayfaları ile medya kuruluşları ile haber ve forum siteleri hedef alınmıştır. Ayrıca bankacılık ve finans sektörü ile ilgili kuruluşlar da saldırılardan nasibini almıştır.

Gürcistan'a karşı gerçekleştirilen siber saldırıda kullanılan yöntemler daha önce Estonya hadisesinde de yoğun olarak kullanılan yöntemlerle benzerlikler göstermektedir. Dağıtık Hizmet Dışı Bırakma saldırılarının yanı sıra, internet sayfalarında tahrifat yapılması gibi benzer metotlara ek olarak Gürcistan saldırısında, SQL[10] açıklıklarından yararlanmak için zararlı yazılım ve betik parçalarının yayılması ve e-posta adreslerinin yığın e-posta gönderilerek devre dışı bırakılması gibi metotlar kullanılmıştır.

Siber saldırılar Güney Osetya ile tansiyonun yükselmesini izleyen 19 Temmuz 2008 tarihinden itibaren, eşgüdümlü siber saldırılar ise 8 Ağustos tarihindeki Rus müdahalesinin ardından gelmiştir. Gürcistan Cumhurbaşkanı Mihail Şaakaşvili'nin resmi internet sitesi Dağıtık Hizmet Dışı Bırakma Saldırısı vasıtasıyla bir günden fazla yayın yapamamıştır. Aynı tarihlerde eş zamanlı olarak Dışişleri Bakanlığı, Savunma Bakanlığı ve benzer kamu kurumlarının internet sitelerine saldırılar gerçekleştirilmiştir. Bunun dışında Gürcistan haber siteleri ile Gürcistan lehine haber yapan pek çok haber sitesi ve tartışma forumuna da saldırılar düzenlenmiştir.

Gürcistan devletinin resmi haber dağıtım kanallarına yapılan bu saldırının amacı uluslararası kamuoyunda Gürcistan lehine yapılabilecek propagandanın engellenmesi olarak değerlendirilebilir. Saldırıların en yoğun ve eşzamanlı olduğu 8-12 Ağustos safhasında ".ge" uzantılı tüm siteler saldırıya uğramış ve bu saldırılar sönümlendiği 28 Ağustos'a kadar devam etmiştir (Hollis, 2011).

Gürcistan'a karşı gerçekleştirilen siber saldırılarda kamu internet sitelerine yapılan saldırılar ile devlet itibarının zedelenmesi amaçlanmış ve bu hedefe büyük ölçüde ulaşılmıştır. Özellikle Cumhurbaşkanı Şaakaşvili'nin Hitler'e benzetildiği fotoğraf kümesinin pek çok kamu internet sayfasında yayınlanması büyük yankı uyandırmıştır.

Dağıtık hizmet dışı bırakma saldırıları, yine köleleştirilmiş Zombi bilgisayarlar kullanılarak pek çok farklı coğrafi noktadan gerçekleştirildiği için saldırı merkezinin belirlenmesi mümkün olmamıştır. Özellikle uygulama açıklıklarının istismar edilmesinde Rus hacker gruplarının internet forumları vasıtasıyla sağladığı destek yadsınamaz. Kara harekâtıyla neredeyse eşzamanlı gerçekleştirilen siber saldırıların zamanlaması ile Rusya'nın bu saldırıların arkasında olma ihtimali arasında kurulmaya çalışılan illiyet bağı için kuvvetli bir delile ulaşılamamıştır. Bu anlamda gerçekleştirilen siber saldırıyı herhangi bir devletle ilişkilendirmek mümkün olmamıştır. Ayrıca uluslararası kamuoyunda Rusya'nın dahli konusunda gündeme gelen tartışmalar Rusya tarafından yalanlanmıştır.

Gürcistan medyasına ait pek çok internet sitesine ilave olarak kişisel blog ve forum sitelerinin de devre dışı bırakılması ile başta Gürcistan halkı olmak üzere uluslararası camia yaşananlar hakkında doğru ve gerçek haber alma şansını kaybetmiş ve bir süre bilgilendirme için Rusya tarafından yapılan yayına mahkum olmuştur.

Gürcistan'ın siber saldırılardan Estonya kadar etkilenmemesi, bilişim teknolojileri altyapısının gelişmemiş olmasına bağlanabilir. Gürcistan'da internet kullanıcı sayısı hızla artmaktadır. Buna rağmen, kamu tarafında sağlanan e-devlet hizmetlerinin yaygın ve yeterli olmaması bu hadisede olumlu bir etki yaratmıştır. Siber saldırılar esnasında devlet hizmetlerine erişim konusunda Gürcistan'da yaşananlarla

Estonya'da yaşananlar karşılaştırıldığında, Gürcistan halkı çok büyük sorun yaşamamış, ancak internet çıkışları için Türkiye, Azerbaycan, Ermenistan ve Rusya üzerinden geçiş yapması sebebiyle yönlendirilmiş siber saldırılara karşı savunmasız kalmıştır. Batıdaki müttefiklerden hizmet alarak Fiber optik kablolarla Karadeniz üzerinden internete bağlanarak bağımlığı azaltma çabası ancak bu çatışmadan sonra gündeme gelmiştir.

Gürcistan, siber saldırılara karşı çeşitli tedbirler almaya çalışmıştır. İnternet altyapısını kullanılamaz hale getiren hizmet dışı bırakma saldırılarına karşı Rus internet sayfalarına erişim engellenmiş, böylece hem sağlıksız bilgi akışı önlenmiş hem de veri trafiği engellenerek bant genişliği kapasitesi boşaltılmıştır. Bununla birlikte, NATO ve diğer müttefik devletlerden teknik danışmanlık ve yardım talep edilmiştir. Bilgisayar Olaylarına Müdahale Ekipleri (BOME) kısa süre zarfında bölgeye ulaşarak teknik konularda danışmanlık sağlamıştır. Gürcistan sınırları içinde yer alan sunucular tarafından sağlanan pek çok hizmet ülke dışındaki sunuculara aktarılarak buradan internet hizmeti verilmesi sağlanmıştır.

İran'a karşı gerçekleştirilen siber saldırı

Siber savaşın dünya gündeminde başlı başına bir savaş olarak tartışılmasına sebep olan hadise 2010 yılında İran'a yapılan siber saldırıdır. İran'a karşı gerçekleştirilen siber saldırı; kullanılan teknikler, saldırının kapsamı ve etkisi, geri planında doğrudan devlet desteği bulunması sebebiyle siber savaş konseptinin doğrudan muharip güç haline geldiğini göstermesi bakımından çok önemlidir. İran'a karşı gerçekleştirilen siber saldırıyı analiz etmeden önce siyasi çerçeveden içinde bulunulan durumun tespit edilmesi önem arz etmektedir.

Amerikan'ın İran'la ilişkileri değerlendirilirken Orta Doğu'ya karşı ilgisi ve İsrail'in güvenliği göz ardı edilemez. Orta Doğu'nun şekillendirilmesinde Büyük Orta Doğu Projesi'nden daha önce uygulamaya konan projeler çerçevesinde 1953 yılında İran'da CIA tarafından planlanan ve uygulanan bir darbe gerçekleşmiştir.[11] İran'ın nükleer macerası işte tam bu tarihlerde Amerika'nın yardımı[12] ile başlamıştır. İran İslam Devrimi'nden sonra programa son verilse de İran'ın devam ettirdiği faaliyetler ile nükleer kabiliyetini askerî savunma amaçlı olarak da kullanabilecek bir seviyeye taşıdığı değerlendirilmektedir. Bu noktada Amerika Birleşik Devletleri, müttefiki ve Orta Doğu'daki uzantısı olarak gördüğü İsrail'in güvenliği başta olmak üzere İran'ın kazanabileceği nükleer silah teknolojisinin dünya barışını tehdit edeceği görüşündedir.

Bu konuda en resmi değerlendirme, Amerikan istihbarat kurumlarından Savunma İstihbarat Ajansı (DIA) eski direktörü Korgeneral Ronald Burgess'in 14 Nisan 2010 tarihinde Senato Silahlı Kuvvetler Komitesi huzurunda verdiği ve tutanaklara geçen açıklamasında yer almıştır. İran'ın yeterli dış destek ile 2015 yılı

itibariyle Amerika Birleşik Devletleri'ne ulaşabilecek kıtalararası menzilli bir füze testi gerçekleştirmesinin mümkün olabileceğini ifade etmiştir. Amerika Birleşik Devletleri tarafından yapılan tüm değerlendirmeler İran'ın 10.000 km uzaklıktaki bir hedefe gönderebileceği kıtalararası menzilli balistik füze testlerini yapma kabiliyetine odaklı olup, balistik füzenin menzili içinde herhangi bir nükleer başlığı başarıyla Amerika kıtasına ulaştırıp ulaştıramayacağı konusunda bir değerlendirme içermemektedir. Bu noktada, "nükleer İran gerçekten Amerika'yı tehdit etmekte midir?" sorusu gündeme gelmektedir. Amerikan kamuoyunu bu konuda ikna etmek için İran'ın Amerika Birleşik Devletleri için de büyük bir tehdit olduğu algısının yaratılması gerekmektedir. Oysa ki İran'ın sahip olduğu uzun menzilli füze sistemleri incelendiğinde, bu menzilin batı Avrupa sınırını aşamadığı açıkça görülmektedir. Türkiye'de konuşlandırılan ancak NATO tarafından kumanda edilen füze savunma sistemi ile radarı Çek Cumhuriyeti'nde yer alan ve Polonya'da konuşlu bataryalar vasıtasıyla da savunma hattı aslında çoktan kurulmuştur. Amerika Birleşik Devletleri kendi güvenliği için savunma hattını daima Atlantik ötesinde çizmektedir. Böylece anakarasını uç karakollar[15] vasıtasıyla koruyarak tehdidi topraklarına ulaşmadan bertaraf ederek güvenliğini sağlamayı hedeflemektedir. İran'a karşı yapılan siber saldırıyı bu çerçevede değerlendirdikten sonra Ortadoğu'da çıkar birliği içinde bulunduğu dost ve müttefik İsrail ile birlikte gerçekleştirilen bu siber saldırının detaylarına geçebiliriz.

Kamuoyunda Stuxnet bilgisayar solucanı olarak da bilinen zararlı yazılım, ilk olarak 2010 yılı Haziran ayında belirlenmiştir. Bu zararlı kod, Microsoft Windows işletim sistemi açıklıklarını kullanarak nükleer tesis içinde yayılıp Siemens endüstriyel kontrol sistemleri (SCADA)[14] vasıtasıyla (PLC)[15] cihazlarını kullanarak tahribat gerçekleştirmektedir.

Bu saldırının öncelikli hedefinin, zararlı kod aracılığı ile santrifüj makinalarının hızları ile oynanarak aşırı basınca maruz bırakılması, böylece nükleer tesise ve nükleer programa onarılamaz zarar verilmesi olduğu düşünülmektedir (Kushner, 2013). Gayri resmî tahminlere göre İran'ın nükleer programını en azından bir yıl sekteye uğratacak tahribat sağlanabilmiştir. Saldırının ikincil hedefi dışarıya tesisle ilgili bilgilerin sızdırılmasıdır. Bu konuda da kısmen başarı elde edilmiştir. Meselenin yalnızca İran'ın nükleer programının geciktirilmesi olmadığı, siber saldırıyı gerçekleştiren gücün aslında saldırının tespit edilebilmesi ile ilgili kaygı duymadıkları, daha sonra tersine mühendislik ile yapılan kod analizleri sonucu ortaya çıkmıştır. Yazılımı tasarlayan ekibin bir anlamda siber ortamda hakimiyetin ilanı olarak da sayılabilecek izler bırakması, hedeflerden birinin de uluslararası kamuoyuna Amerikan egemenliğinin bu yeni mücadele alanında da varlığının ilanı anlamına gelmektedir.

Bu saldırının arkasında devlet desteği olduğunun düşünülmesinin en önemli sebebi, daha önce rastlanmayan (*zero-day*)[16] Microsoft Windows açıklıkları ile Siemens sisteminin açıklıklarını aynı anda kullanarak sadece belirli cihazların devre

dışı bırakılabilmesini sağlama kabiliyetidir. Bu konuda yıllardır çalışan Kaspersky Laboratuvarları Stuxnet kodunu incelediğinde bunun ancak bir devlet desteğinde uzun süre üzerinde çalışılarak tasarlanmış olabileceği sonucuna varmış, benzer görüşler F-Secure ve Symantec uzmanları tarafından da gayri resmi olarak teyit edilmiştir. Siemens'in yaptığı açıklamada İran dışındaki ülkelerde bulunan cihazların zarar görmediğini açıklaması, Alman istihbarat örgütü BND elemanlarının bu saldırıyı Siemens vasıtasıyla desteklediği konusunda tartışmaları gündeme getirmiştir.

Bugün resmi olarak kabul edilmese bile Olimpiyat Oyunları Harekâtı (*Operation Olympic Games*) 2006 yılında, o dönem STRATCOM[17] içinde örgütlenen siber savaş birimi tarafından başlatılmıştır (Rosenzweig, 2012). Orgeneral Cartwright o dönem bizzat bu çalışmaların içinde yer almış ve bu konuda Amerikan Başkanı Bush ve Obama'yı bilgilendirmiştir (Kaplan, 2013). Bu bilgi 1 Haziran 2012 tarihinde New York Times yazarı David Sanger tarafından derlenen bir haber ile kamuoyuna yansıtılmıştır. Uluslararası kamuoyu Stuxnet ile ilgili pek çok bilgiye ilk defa bu vasıtayla erişmiştir. Daha sonra Sanger'in "Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power" ismi ile kitaplaştırdığı eserinde Orgeneral James Cartwright'dan yaptığı alıntı daha sonra bahse konu general hakkında soruşturma açılmasına sebep olmuştur. Kitapta Orgeneral Cartwright'ın "gizli olan bir silahın caydırıcılık sağlayamayacağı ve varlığından haberdar olunmayan silahın kimseyi korkutmayacağı" ifadeleri yer almıştır. Kitapta aslen sorgulanan Amerikan devlet sistemi gizlilik esaslarının Amerikan çıkarları ile ilişkisi olsa da Amerikan Adalet Bakanlığı Haziran 2013 tarihinde Amerika'nın bir dönem en yüksek ikinci rütbeli subayı olan Orgeneral James Cartwright hakkında Stuxnet hakkında gizlilik dereceli bilgileri sızdırdığı iddiası ile soruşturma açmıştır (Zara, 2013).

Uluslararası düzende hasma verilen zarar abartılarak moral üstünlük sağlanması hedeflenir, saldırıya uğrayan ülke için de tersi geçerlidir. İran tarafından zararın mahiyeti konusunda resmi bir açıklama yapılmaması da bunun bir göstergesidir. Her ne kadar fiziksel zararın boyutları bilinmese de, bu siber saldırının İran'ın nükleer programını ileri bir tarihe ötelemesine neden olduğu açıktır. Bu konuda özellikle Amerikan basınında, bir Amerikan-İsrail ortak projesi olan Stuxnet aracılığı ile, İran'ın nükleer santrifüjlerinin beşte birinin tahrip edildiği yönünde haberler yayınlanmıştır.[18]

Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT) raporuna göre İran kendisine karşı gerçekleştirilen siber saldırıya misilleme olarak 2012 yılı Ekim ayında Orta Doğu'da konuşlu petrol ve gaz şirketlerinin tesislerinde yer alan veri işleme merkezlerine saldırıda bulundu. Kamuoyunda Shamoon virüsü olarak da adlandırılan bu siber saldırı ile 2012 yılı Ağustos ayında Suudi Arabistan kökenli küresel bir petrol firması olan Aramco'nun merkezinde yer alan yaklaşık 30,000 bilgisayarın sabit diskleri tahrip edildi. Bu esnada ekranlarda yanan bir Amerikan bayrağı resminin yer alması da küresel petrol anlaşmaları ile iş yapan Aramco

firmasının seçilmesinin bir mesaj olarak algılanmasına neden oldu. Aynı zararlı yazılımın Katar'da yer alan RasGas firması için de kullanıldığı ortaya çıkmıştır. İran'ın kendisine karşı gerçekleştirilen saldırıya ancak iki yıl sonra cevap verebilmesinin en büyük sebebi bu konuda daha önce kapasite geliştirememiş olmasıdır.

Genel Değerlendirme

İlk başta merak gibi insani güdüler ile başlayan ve yazılımlardaki açıklıkların istismar edilmesiyle çeşitli sosyal mesajların verilmesini amaçlayan siber saldırılar, süreç içerisinde, uluslararası şirketlerin ekonomik çıkarları adına gerçekleştirdikleri daha profesyonel casusluk eylemlerine, çeşitli yasadışı terör örgütlerinin eylem alanına, son aşamada ise devletler arasındaki güç mücadelesinin temel vasıtalarından birine evirilmiştir.

Vakalar incelendiğinde siber savaşın zaman içinde daha karmaşık teknikler kullanılarak barış zamanında siyasi emellerin gerçekleştirilmesinde kullanıldığı gözlenmektedir. Bunun en büyük sebebi, uluslararası hukuk belgelerinin kaleme alındığı tarihte bugünkü teknolojinin olmaması sebebiyle oluşan gri bölgenin suiistimal edilebilmesidir.

Daha önce kitle imha silahlarına sahip olduğu iddiası ile Irak'ı istila eden Amerika Birleşik Devletleri, Birleşmiş Milletler Güvenlik Konseyi daimi üyesi olmanın da verdiği güçle Irak'ta kitle imha silahı bulunmamasına rağmen gerçekleştirdiği saldırı ile ilgili olarak hesap vermek zorunda kalmamıştır. Ancak bu durum uluslararası kamuoyunda Amerika'nın tek taraflı uygulamalarına karşı tepki oluşturmuş ve meşruiyet tartışmalarını tırmandırmıştır.

Amerika Birleşik Devletleri kendisine yapılacak herhangi bir siber saldırı karşısında kara, hava ve deniz unsurları dahil olmak üzere tüm askeri kabiliyeti ile cevap vereceğini deklare etmiştir. Benzer bir şekilde, Rus ve Çinli muhataplar kendilerine yönelecek bir siber saldırı durumunda karşılığın nükleer cevap olabileceğinin sinyallerini vermişlerdir. Ancak burada dikkat edilmesi gereken nokta, siber ortamda gerçekleşen hadiselerin istismar edilerek küresel istilaya zemin hazırlayabilecek hukuksal düzenlemelerin önünün açılmasıdır. NATO Müşterek Siber Savunma Mükemmeliyet Merkezi, 2013 yılında Tallinn Kılavuzu adında bir belge yayınlamıştır. Bu belge incelenerek, belgenin hazırlanmasında başrolde olan Amerika'nın, siber ortamın geleceği hakkında stratejik olarak orta ve uzun vadede biçtiği pay daha iyi değerlendirilebilir. Amerika uluslararası normların siber ortamda da geçerli olduğu tezini savunmaktadır. Aslında bu tezin arkasında yine küresel güç mücadelesi yatmaktadır. Oysa ki, dünya savaşı şartlarında kaleme alınan ve günümüz teknolojileri icat edilmemişken kabul edilen savaş hukuku metinlerinin bugün siber saldırılara karşı da uygulanabileceği tezini savunmak ileride çok büyük sıkıntılara yol açacaktır.

Rusya Federasyonu, Çin Halk Cumhuriyeti ve Amerika Birleşik Devletleri, çıkarları doğrultusunda siber güvenlik konusunda birbirlerinden farklı pozisyonlar almaktadır. Güvenlik politikalarındaki bu ıraksama bahse konu devletlerin egemenlik anlayışlarındaki farklılıklardan kaynaklanmaktadır. Siber ortamda milli kabiliyet geliştiren ve uluslararası düzende başat rol üstlenen bu devletler gri bölgeyi suiistimal etseler de yakın zamanda asimetri sağlayan görece güçsüz hasımlarından gelecek saldırılar karşısında ileride alacakları pozisyonlara meşru zemin hazırlamak için çabalayacak ve uluslararası hukuki düzenlemelerin takipçisi olacaklardır. Bunun en güzel örneği, Amerikan Dışişleri Bakanlığı tarafından 7 Haziran 2013 tarihinde yapılan basın açıklamasında, Birleşmiş Milletler nezdinde yaşanan gelişmelerden duyulan memnuniyetin dile getirilmesi ile görülmüştür.[19] Bahse konu gelişme, Birleşmiş Milletler Bilişim ve Telekomünikasyon Alanında Uluslararası Güvenlik Bağlamında Yaşanan Gelişmeler Hakkında Kamu Uzmanları Grubu'nda"[20] yaşanan tartışmalar sonucunda Birleşmiş Milletler Şartı başta olmak üzere uluslararası hukuk normları, kurallar ve prensiplerin siber ortamda da geçerli olduğu konusunda oluşan görüş birliğidir. Bu çalışma grubunun A/68/98[21] sayılı raporu ile uluslararası hukuk normlarının siber ortam için de uygulanabilir olduğu, ayrıca barış ve istikrarın temini ve korunmasında olmazsa olmazlardan olduğu vurgulanmaktadır.

Birleşmiş Milletler ve NATO gibi tam üyesi olduğumuz örgütlerde ulusal çıkarlarımıza aykırı olabilecek tüm gelişmeler dikkatle takip edilerek uluslararası hukuk alanında ileride ülkemizin bekasını tehdit edebilecek tüm girişimler engellenmelidir. Birleşmiş Milletler Şartı dışında Cenevre Sözleşmeleri ve Silahlı Çatışma Hukuku gibi uluslararası metinler, siber ortamda beliren tehditlerle ilgili olarak sadece devletler arası ilişkileri düzenlemektedir. Buna ek olarak, devlet dışı aktörlerin doğurduğu asimetrik tehdit ile oluşan güvensizlik ortamı, barış ve istikrarın sağlanması için uluslararası eşgüdüm mekanizmalarının geliştirilmesini zorunlu kılmaktadır.

Estonya'ya karşı gerçekleştirilen siber saldırı ile konu ilk defa dünya gündemine oturmuştur. Gürcistan'a karşı gerçekleştirilen kara harekâtı ile neredeyse eşzamanlı gerçekleşen siber saldırılar ise konunun dünya gündemine konvansiyonel bir savaş ile birlikte girmesine sebep olmuştur. İran vakası ise siber savaşın dünya gündeminde başlı başına bir savaş şekli olarak tartışılmasına sebep olan hadisedir. Bu üç vaka sonucunda ortaya çıkan resim, siber savaşın gelişimini göstermesi bakımından değerlidir. Kısa zaman için saldırıların karmaşıklığı ve hedeflerin internet sayfalarında gerçekleştirilen tahrifatlar veya bankacılık ve mali sistem üzerinde oluşturulacak kayıplardan ziyade can kayıplarına yol açacak fiziksel tahribata doğru ilerlemesi en başta sözünü ettiğimiz güvenlik algısı ve stratejilerinde geriye dönülmez dönüşümlere sebep olmuştur. İran'a karşı gerçekleştirilen siber saldırı öncesinde hiç bir siber saldırı güç kullanım eşiğini bu derece zorlar nitelikte olmamış, savaş hukukunun ilgi alanına girecek şiddete ulaşmamıştır. Ancak Stuxnet saldırısı

ile saldırı sonuçları fiziksel etkileri bakımından ihmal edilemeyecek boyuta ulaşmış ve Birleşmiş Milletler şartının meşru müdafaa hakkının kullanılmasını gündeme getirmiştir.

Ulusal Güvenlik Ajansı (NSA) ve Merkezi Haberalma Teşkilatı (CIA) eski direktörü Orgeneral Michael Hayden Amerikan CBS televizyonunun hazırladığı 60 dakika programında yaptığı açıklamada, Stuxnet ile beraber yeni bir döneme girildiğini belirtmiştir. Hayden'e göre, daha önceden hizmet dışı bırakma veya bilgi sızdırma gibi amaçlarla gerçekleştirilen siber saldırıların ilk defa doğrudan fiziksel tahribat hedeflenerek gerçekleştirilmiştir. Birleşmiş Milletler sistemi, kuvvet kullanımını meşru müdafaa hakkı saklı kalmak koşuluyla açıkça yasaklamıştır. Hayden'e göre Stuxnet saldırısı ile güç kullanım eşiği aşıldığından, Birleşmiş Milletler Şartı'nın tanıdığı meşru müdafaa hakkının kullanılabileceği sonucu doğmaktadır.[22]

Özellikle kaynağının belirlenmesinde yaşanan teknik zorluklar ortada iken, Birleşmiş Milletler Güvenlik Konseyi daimi üyelerinden birinin kendisine bir ülkeden siber saldırı yapıldığını bildirip meşru müdafaa hakkını kullanması sonucunda kaos kaçınılmazdır. Uluslararası düzene yön veren başat ülkeler kendilerine yapılacak herhangi bir siber saldırı karşısında kara, hava ve deniz unsurları dahil olmak üzere tüm askerî kabiliyetleri ile cevap vereceğini deklare etmektedir. Bu durumda felaket senaryolarından biri şudur. Hasım ülke tarafından gerçekleştirilmiş süsü verilecek ve fiziksel tahribat yaratacak bir saldırı gerçekleştirilir. Bunun için hasım ülke sınırları içinde Zombi bilgisayarlar kullanılarak bu ülke IP adreslerinden saldırı yapıldığı tespit edilir. Fiziksel zarar verilmesi sayesinde güç kullanım eşiği aşıldığından Birleşmiş Milletler şartına göre Güvenlik Konseyi kararı aranmaksızın meşru müdafaa hakkı kullanılabilecektir. Bir önceki örnekte olduğu gibi bu planı gerçekleştiren ülkenin Amerika Birleşik Devletleri gibi Birleşmiş Milletler Güvenlik Konseyi daimi üyesi bir ülke olması durumunda ise Birleşmiş Milletler Güvenlik Konseyinden çıkacak bir kararı müteakip hasma karşı askeri bir müdahale bile gündeme gelebilecektir.

Sonuç Yerine

2007 yılında Estonya saldırısı ile başlayan süreçte uluslararası güvenlik algılarında paradigma boyutunda kayma yaşanacağı tahmin edilememiştir. Aslında tamamen bilgi üstünlüğünün bir sonucu olarak gelişen ve önceleri destek aracı iken zaman içinde ana muharip unsura dönüşen siber güç, klasik güvenlik algısı ve stratejilerinde geriye dönülmez dönüşümlere sebep olmuştur.

Estonya'ya karşı gerçekleştirilen siber saldırıdan çıkarılacak pek çok ders vardır. Bunlardan birincisi, belki de en önemlisi saldırıların kaynağının tespiti edilmesinde yaşanan zorlukların oluşturduğu durumdur. Bu durumun, muhatabın belirlene-

memesi sonucu, sorumluların cezalandırılması hususunda uluslararası hukuk alanında tartışma yaratabilecek uygulamalara neden olabileceği değerlendirilmektedir. Estonya örneğinde olduğu gibi siber saldırı ile hasma konvansiyonel teknolojiler (Hava, Kara, Deniz, Uzay) dışında da saldırı gerçekleştirilebileceği gerçeği bir kez daha gözler önüne serilmiştir. Saldırı, Zombi bilgisayarlar üzerinden gerçekleştirilen Dağıtık Hizmet Dışı Bırakma saldırısı, doğası gereği, binlerce ayrı fiziksel noktadan gerçekleştirilmiştir. Estonya hadisesi sonrasında aylar süren adli analiz çalışmasının sonucunda, yaşanan siber saldırının kaynağına ve Rusya Federasyonu'nun bu çatışmaya müdahil olup katkı verdiğine ilişkin elle tutulur deliller ortaya konamamıştır.

Gürcistan savaşı öncesinde ve esnasında yaşanan siber saldırılar ile Rusya, Gürcistan harekâtında psikolojik üstünlük sağlamıştır. Gürcistan internet erişim hizmetleri pazarının iki büyük servis sağlayıcısı günlerce hizmet veremez hale getirilmiştir. Bu yüzden Gürcistan halkı hem sağlıklı bilgi alabileceği kamu sitelerine, hem de sesini duyurmak veya gelişmeleri takip etmek için yurtdışındaki bilgi kaynaklarına erişememiştir. Bu suretle, Gürcistan harekâtında siber saldırılar Rusya lehinde çarpan etkisi yaratmıştır. Siber saldırılarda Rusya Federasyonu'nun dahli ispatlanamamıştır. Estonya hadisesinde olduğu gibi siber saldırılara, kendi hür iradesi ile veya bilgisayarının kendi bilgisi dışında komuta edilmesi sonucu bir şekilde siber saldırılara karışan sivillerin durumunun uluslararası hukuk çerçevesinde nasıl değerlendirileceği konusunda tartışmalar yaşanmıştır.

1990'lı yıllarda ortaya atılan dördüncü nesil savaş tartışmaları ile savaşın değişimine vurgu yapan pek çok makale ve eser yayımlanmıştır. Dördüncü nesil savaş ile yaşanan değişimin aslen taktiklerde değil, savaş alanında sivil-asker ayrımının kalkması, barış ile savaş arasındaki ayrımın bulanıklaşması, devletlerin karşısında devlet dışı aktörlerin yer alması ve gerilla tipi harekâtın modernite ile revize edilmesi ile yaşandığı belirtilmektedir. (Lind vd. 1989:22-26'dan aktaran Bilgin, 2013: 47) Savaşan (*combatant*) ve savaşmayan (*non-combatant*) arasındaki fark uluslararası hukuk için büyük önem taşımaktadır. Geçmişte, savaşanlar ülkelerinin silahlı kuvvetlerine mensup oldukları için meşru saldırı hedefi olarak görülmeleri uluslararası hukukun bir normudur. Ancak savaşmayanların korunması da aynı şekilde hukuk açısından garanti altına alınmıştır. 1949 tarihli Cenevre sözleşmeleri dikkate alındığında işte tam bu noktada savaşmayanlara istisnai olarak getirilen yükümlülükler vardır. Savaşmayanlara karşı sağlanan koruma ancak düşmanlıklarda rol almayan siviller için geçerlidir. Burada karşımıza bir soru çıkmaktadır. İki devlet arasında çıkan silahlı çatışma esnasında vatansever duygular ile devlet kontrolü ve bilgisi dışında gerçekleştirilen siber saldırıların faillerinin belirlenmesi durumunda, bu kişiler Cenevre sözleşmeleri çerçevesinde savaş mahkemesinde mi yargılanacaktır?.

İran'a karşı gerçekleştirilen siber saldırı ile beraber siber savaş yeni bir boyut kazanmış ve daha önce de gündeme gelen ancak ölçülen fiziksel zararın güç kul-

lanım eşiğinin çok altında olması veya zararın doğrudan ölçülemiyor olması sebebiyle meşru müdafaa hakkının kullanımının önünde yer alan meşruiyet engelinin kalkmasına sebep olmuştur. İran'a yapılan saldırı ile beraber doğrudan İran'ın nükleer programı hedef alınmış ve nükleer programın durdurulması veya en azından geciktirilmesi için tesis altyapısına fiziksel zarar verilmiştir. Bu yapılan saldırının tesis içinde yer alan cihazların havadan bombalanması ile büyük bir farkı yoktur.

Bu saldırıda Amerika Birleşik Devletleri ve İsrail (Almanya[23]) bilgi üstünlüğünü kullanarak saldırıyı[24] gerçekleştirmiştir. İran'ın meşru müdafaa hakkı saklı olduğu halde İran şu ana kadar misilleme gerçekleştirmemiştir. Burada Amerika Birleşik Devletleri güçlü devlet olmanın verdiği caydırıcılık silahını çok iyi kullanmıştır. İran, saldırının kaynağını tespit etmiş olsa bile Amerika Birleşik Devletleri'ne karşı saldırıda bulunarak muhatap olacağı cevap karşısında riski göze alamamış ve sessiz kalmak zorunda kalmıştır. Benzer durum Estonya ve Gürcistan'a karşı gerçekleştirilen siber saldırılarda yaşanmıştır. Daha güçsüz iki bağımlı devlet, saldırıların arkasında olduğunu ispat edemedikleri güce karşı misilleme yapmak yerine uluslararası camiada "mağduru oynayarak" yeni kurulan devletleri için görünürlük artırma arayışı içine girmişlerdir.

Siber güvenliğin sağlanması teknik olarak oldukça zorlu bir süreç olarak değerlendirilebilir. Ancak bunun sağlanabilmesi için teknik çözümler tek başına yeterli değildir, siber güvenlik stratejisi belirlenerek eylem planları ile tüm paydaşlarla beraber topyekûn mücadele zorunlu hale gelmiştir.

Yakın tarihte gerçekleşen hadiseler göz önüne alındığında, millî tehdit değerlendirmesi içinde siber tehdidin öncelikli olarak ele alınması gerektiği ortaya çıkmaktadır. Siber tehdit zaman içinde değişim göstermiştir. Önceleri çoğunlukla devlet dışı aktörlerin faaliyet alanına giren siber faaliyetlerin, Estonya saldırısı ile başlayıp İran saldırısı ile devam eden süreçte devlet destekli veya doğrudan devlet eliyle yürütülen bir hale dönüştüğü görülmektedir. Tehdit kaynağının sadece devlet, veya devlet destekli taşeronlar olmaması, ayrıca organize suç örgütleri, bağımsız gruplar veya bireylerin müdahil olmaları sebebiyle tehditle mücadele hukuki anlamda daha da zorlaşmaktadır. Uluslararası örgütler nezdinde yasal çerçeve oluşturma süreçlerine dahil olunması ve ulusal çıkarlarımızın gözetilmesinde proaktif olunması gerekmektedir. Ayrıca ulusal mevzuat çalışmaları tamamlanarak özellikle siber suç kapsamında değerlendirilebilecek hadiselere karşı gerekli yaptırımın uygulanması zorunluluk arz etmektedir.

Dünyada yaşanan gelişmeler göz önünde alındığında, özellikle bilişim sistemlerine bağımlı kritik altyapıların korunması önem kazanmaktadır. Bu kapsamda ilk olarak "Kritik Altyapı Önceliklendirme Programı" olarak adlandırılabilecek çalışma yapılmalı, Türkiye'nin en kritik altyapılarının hangileri olduğu belirlenmeli ve siber güvenlik açısından durumları tespit edilmelidir. Bu noktada, kamu-özel sektör ilişkilerinin eşgüdümü önem taşımaktadır. İnternet servis sağlayıcıları başta

olmak üzere siber güvenlik altyapısının kurulması için idari ve teknik tüm imkanlar seferber edilmeli ve yasal mevzuat içinde görev, yetki ve sorumluluklar özel sektörü de kapsayacak şekilde tanımlı hale getirilmelidir. Kamu güvenliğinin temini ancak tüm paydaşların katılımı ve desteğiyle sağlanabilmektedir. Bu hedefe ulaşılması için tüm sektörler için bilim sanayi ve teknoloji politikalarının gözden geçirilmesi gerekmektedir. Siber güvenlikle ilgili araştırma ve geliştirme faaliyetlerine hız verilmesi ile kritik altyapı bileşenlerinde kullanılan yazılım ve donanımların mümkün olduğunca millileştirilmesi bir devlet politikası haline getirilmelidir.

Ulusal güvenliğimize büyük tehdit oluşturabilecek siber saldırılara karşı, ülke içinde her türlü teknik kabiliyetin geliştirilerek siber savaşın gerek savunma gerekse saldırı boyutu düşünülerek kapasite geliştirilmesi şarttır. Bugün gelinen noktada siber ortam diğer mücadele alanlarından ayrı düşünülemez, bu nedenle askerî siber savunma ve siber taarruz kabiliyetinin geliştirilmesi önem kazanmaktadır. Amerika Birleşik Devletleri, Rusya Federasyonu ve Çin Halk Cumhuriyeti gibi uluslararası düzende söz sahibi olan devletlerin örgütlenmelerine bakıldığında, siber yapılanmanın özellikle taarruz boyutu ile ilgili olarak silahlı kuvvetlerin ön planda olduğu görülmektedir. Bunun için gerekli operasyonel merkezlerin kurulması, siber güvenlik ile ilgili tüm kurum kuruluşların eş zamanlı gerçekleştirdiği faaliyetleri takip ederek eşgüdümü sağlayacak bir merkezinin hayata geçirilmesi şarttır. Bu bağlamda, askerî kabiliyetlerin geliştirilerek sivil-asker işbirliği çerçevesinde eşgüdüm içinde faaliyet gösterilmesi önem kazanmaktadır.

Stratejik olarak belirlenen millî hedeflere ulaşılması için gerekli kabiliyetlerin, milli imkanlarla geliştirilmesi orta ve uzun vadeli bu çalışmaların hayata geçirilmesi ile mümkün olacaktır. Bu kabiliyetlerin geliştirilmesi ancak yeterli ve yetkin insan kaynağı oluşturmak ile mümkün olacaktır. Bu yönde çalışmalar yapılarak insan faktörünü çarpan etkisi yaratacak şekilde lehimize kullanmamız gerekmektedir. Farkındalığın artırılması ve eğitimin daha ileri düzeye çıkarılması için devlet kurumlarının eşgüdümü ile orta ve uzun vadeli eylemlerin uygulamaya sokulması gerekmektedir.

Milli güvenliğimize yönelebilecek her türlü tehdide karşı caydırıcılık sağlamak için ulusal çıkarlarımızın siber ortam dahil olmak üzere her ortamda savunulması hayati öneme sahiptir. Gerekli risk analizi ve tehdit değerlendirmeleri yapılarak ülkemizin çıkarlarının korunması için bu stratejik çalışmaların devlet ciddiyetine yakışır şekilde gerçekleştirilmesi gerekmektedir.

Notlar

1 Elektromanyetik tayf hayatımızın görünmeyen bir parçasıdır. Bunu daha iyi anlamak için günlük hayattan örnekler verebiliriz. Örneğin evlerimizde kullandığımız televizyon uzaktan kumandaları veya arabalarımızı uzaktan açmamızı sağlayan anahtarlarımız aslında birer elektromanyetik vericidir. Evlerimizdeki radyo ve televizyonlarımız ise birer elektromanyetik alıcı içerir. İnsanlarla iletişim kurmamızı sağlayan cep telefonlarımız elektromanyetik alıcı-verici içerir. Yemek ısıtmakta kullandığımız mikrodalga fırın da dahil olmak üzere bu ve benzeri tüm bu cihazlar ile elektromanyetik tayf içinde ayrılmaz bir bütünün parçaları olarak yaşamaktayız. Buna ek olarak teknolojinin gelişmesi ile elektromanyetik tayf ile siber ortam birbirine kaynaşmıştır. Özellikle yüksek hızlı kablosuz ağların ev, işyerleri ve kamuya açık alanlarda yaygınlaşması, ayrıca uydu haberleşmesi üzerinden uçak, gemi ve araba gibi hareketli araçların da internete bağlanması ile bilgisayar ağları da bu tayfın içine girmiştir.

2 Birinci Sovyet Hakimiyeti 1940-1941, İkinci Sovyet Hakimiyeti 1944-1991

3 Bahse konu anıtın kaldırılması için Pro Patria partisinin girişimleri ile süreç başlamıştır. Konu o dönemde Avrupa basınında da oldukça yankı uyandırmıştır. Bunun için bkz. http://news.bbc.co.uk/2/hi/europe/6255051.stm

4 Estonya İstatistik kurumunun 2011 resmi verilerine göre Estonya nüfusunun %24,8'i Rus etnik kökenlidir. http://www.stat.ee/sdb-update?db_update_id=13545

5 Müşterek Siber Savunma Mükemmeliyet Merkezi tarafından 2010 yılında yayınlanan "Uluslararası Siber Olaylar ve Yasal Değerlendirmeler" isimli eser için bkz. http://www.ccdcoe.org/publications/books/legal-considerations.pdf

6 Zombi terimi çeşitli zararlı yazılımlar tarafından ele geçirilen ve sahibi dışında uzaktan yönetilen bilgisayarlar için kullanılmaktadır.

7 Botnet terimi Zombi bilgisayarların, bir başka deyişle zararlı yazılımlarla robotlaştırılmış/ köleleştirilmiş bilgisayarların oluşturduğu ağ için kullanılmaktadır. "Robot" ve "Network" kelimelerinin ilk heceleri bir araya getirilerek üretilmiştir.

8 Alan Adı Sunucuları, IP ağlarında isim-adres eşlemesini yaparak kullanıcıların ve tabi ki bilgisayarların birbirine erişimini kolaylaştıran telefon rehberine benzetilebilir.

9 Estonya Eğitim ve Araştırma Ağı adıyla bilinen EENet, 1993 yılında kar amacı gütmeyen kamu kurumu olarak kurulmuştur.

10 SQL Structured Query Language bir veritabanı dili olarak tasarlanmış, ilişkisel veritabanı yönetim sistemlerinde verilerin çekilmesi ve yönetilmesi ile veritabanı şemalarının yaratılması ve yapılandırılması ile veritabanı nesnelerinin erişim kontrolü yönetiminin gerçekleştirilmesinde kullanılmaktadır.

11 Amerikalılar tarafından TPAJAX Projesi olarak da adlandırılan bu darbe, İran petrollerinin 1951'de millileştirilmesi üzerine CIA ve MI6 tarafından uygulamaya konan ve Musaddık rejiminden kurtulmak için gerçekleştirilen bir darbedir. Üzerinden 50 yıl geçmesini müteakip 2013 yılı Ağustos ayında CIA bu darbenin içinde yer aldığını kabul etmiştir.

12 Amerikan Başkanı Eisenhower tarafından başlatılan "Atoms for Peace" programı ile Amerikan şirketlerine İran'da nükleer endüstriler alanında yatırım yapma imkanı sağlanmıştır. 1970'lerin sonuna, İran İslam Devrimi'ne kadar bu program devam etmiştir.

13 Bu uç karakol sadece yurt güvenliği değil ayrıca ticaretin, hammadde sömürüsünün uzak coğrafyalarda da korunmasını amaçlamaktadır. Dünya haritasına bakıldığında Amerikan askeri üslerinin ve Savunma İşbirliği Teşkilatlarının diğer büyük güçlerin çıkar çatışmalarından ve olası gelecek çatışmalarından azami ölçüde faydalanılmasını sağlayacak şekilde konumlandırıldıkları görülmektedir. Son dönemde Güney Asya tarafına yönelmesi ve buradaki askeri ve siyasi varlığını artırması orta vadede planlanan Amerikan aygıtlarının asimetrik tehditten ziyade, mücadele etmekte daha başarılı olduğu kutuplu dünya düzeni çerçevesinde yeni bir soğuk savaş yaratmak için Çin'e karşı oluşturulmak istenen Çin dengenin kurulması için hazırlıktır.

14 SCADA (*Supervisory Control and Data Acquisition*). SCADA sistemleri, özellikle enerji sektörü gibi otomasyonun yoğun olarak kullanılması gereken kurulumlarda güvenlik tehdidi oluşturabilecek ana bileşendir. Esasen tehdit, Dünya'da son derece sınırlı sayıda firma tarafından üretilen SCADA sistemlerinin izleme, bakım ve güncelleme gerekçeleri ile Internet üstünden geliştirici firmaların tesislerine bağlı durumda çalışmalarından kaynaklanmaktadır. Bu sistemler algılayıcılar vasıtasıyla verileri toplayarak, terminal kullanıcılarına gerekli bilgileri görüntüleyip kaydederek ana yapının işleyişini sağlamaktadır. Bu sistemler kontrol sisteminin bir parçası olarak algılayıcılardan gelen bilgi çerçevesinde kontrolcülere komuta edilmesini sağlayarak kritik altyapılarda çokça kullanılan mekanik bileşenlerin yönetilmesini sağlamaktadır. Bu sistemlerin

kullanılması ile binlerce mekanik bileşenden oluşan baraj, rafineri ve santral gibi kritik altyapı tesislerinin yönetilmesi mümkün olabilmektedir.

15 PLC (*Programmable Logic Controller*) özellikle baraj, santral, rafineri vb. gibi büyük endüstriyel tesislerde elektromekanik süreçlerin otomasyonu için kullanılan bilgisayarlardır. Sıradan bilgisayarlardan farklı olarak PLC'ler kullanıldıkları alana has ihtiyaçların giderilmesi için tasarlanmıştır. Bu işlevleri için özelleştirilmiş giriş-çıkış arayüzleri vardır. Ayrıca PLC'ler yüksek ısı, titreşim ve benzeri dış ortam değişkenlerinden en az etkilenecek şekilde üretilmektedir.

16 *Zero-day* saldırılar, hedef alınan sistemlerde daha önceden bilinmeyen açıklıkların istismar edilmesine verilen addır. Bu tür saldırılarda sistem geliştiriciler daha önceden karşılaşmadıkları bu açıklığın giderilmesi için vakit bulamamışlardır. Ancak bu açıklığın ortaya çıkması ile sistemlerde gerekli yamanın yapılması için çalışmalar başlatılır. Genelde bu tür açıklıklar ortaya çıkarılması ile yamanın yayınlanması arasında geçen süre zarfında yeraltı pazarında astronomik fiyatlara alıcı bulmaktadır. Yama yayınlanmadan önce geçen sürenin yıllar mertebesinde olabildiği görülmüştür.

17 Amerikan Stratejik Komutanlığı STRATCOM, 2009 yılına kadar siber savaş birimlerini içermekte idi. 23 Haziran 2009 tarihinde STRATCOM komutanına verilen emrin ardından 21 Mayıs 2010 tarihinde müstakil bir komutanlık olarak organize edilmiştir.

18 İran'a karşı gerçekleştirilen siber saldırıların etkileri ile ilgili internette çeşitli bilgiler dolaşmaktadır ancak resmi olarak gerçekleşen zarar hakkında net bir bilgi mevcut değildir. Bu konu ile ilgili habere bağlantıdan ulaşılabilir: http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11#ixzz2nmGYCKnw (Erişim: 26.12.2013).

19 Siber güvenlik ile ilgili konularda Birleşmiş Milletler nezdinde yaşanan gelişmeler hakkında 7 Haziran 2013 tarihli basın açıklaması için bkz. http://www.state.gov/r/pa/prs/ps/2013/06/210418.htm (Erişim: 27.12.2013).

20 UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

21 Birleşmiş Milletler Kamu Uzmanları Grubunun Raporu için bkz. http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98 (Erişim: 27.12.2013).

22 BM Şartı Madde 51: Bu Antlaşma'nın hiçbir hükmü, Birleşmiş Milletler üyelerinden birinin silahlı bir saldırıya hedef olması halinde, Güvenlik Konseyi uluslararası barış ve güvenliğin korunması için gerekli önlemleri alıncaya dek, bu üyenin doğal olan bireysel ya da ortak meşru savunma hakkına halel getirmez. Üyelerin bu meşru savunma hakkını kullanırken aldıkları önlemler hemen Güvenlik Konseyi'ne bildirilir ve Konsey'in işbu Antlaşma gereğince uluslararası barış ve güvenliğin korunması ya da yeniden kurulması için gerekli göreceği biçimde her an hareket etme yetki ve görevini hiçbir biçimde etkilemez"

23 Siemens sistemleri ile ilgili açıklıklar da kullanıldığı için bazı kaynaklara göre Almanya Federal Devleti istihbarat birimlerinin de katkı vermiş olabileceği değerlendirilmektedir.

24 Saldırı ile ilgili olarak pek çok bilgi Edward Snowden isimli eski Ulusal Savunma Ajansı görevlisi tarafından ifşa edilmiştir. Ancak makalenin yayına hazırlanması sürecinde bu saldırı resmi olarak hiç bir devlet veya örgüt tarafından üstlenilmemiştir.

Kaynakça

Bilgin K.R. (2013). Savaşı Anlamak için Savaş Çalışmalarını Anlamak. Milli Güvenlik ve Askeri Bilimler 1(1), 25-56

Clausewitz C. (2011). *Savaş Üzerine.* İstanbul: Doruk Yayınları.

Hollis, D. (2011). Cyberwar Case Study: Georgia 2008. Small Wars Journal, January 2011.

Kaplan, F. (2013). Who Leaked the Stuxnet Virus Story? http://www.slate.com (Erişim: 24.12.2013).

Kushner, D. (2013). The Real Story of Stuxnet. http://spectrum.ieee.org Erişim: 26.12.2013).

Lind W.S., Nightengale, K., Schmitt, J. F, Sutton, J. W. ve Wilson, G. I. (1989). The Changing Face of War: Into the Fourth Generation. *Marine Corps Gazette,* 22-26.

Tikk E., Kaska K., Vihul L. (2010). *International Cyber Incidents: Legal Considerations.* Tallinn: Cooperative Cyber Defence Centre of Excellence.

Operation Olympic Games — A Legal Setback and a Strategic Opportunity http://www.lawfareblog.com (Erişim: 24.12.2013).

OSCE (Organization for Security and Co-operation in Europe). (2013). *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace*, http://www.osce.org (Erişim: 30 .12.2013).

Rosenzweig, P. (2012). Operation Olympic Games - A Legal Setback and a Strategic Opportunity. http://www.lawfareblog.com (Erişim: 24.12.2013).

Zara, C. (2013). Obama's Favorite General? Cartwright DOJ Leak Investigation Complicates Story Of Stuxnet Cyber-Attack On Iran http://www.ibtimes.com (Erişim: 24.12.2013).

Summary

Cyber Warfare

Barış Erdoğan*

Recent developments in information and telecommunication technologies have led to the transformation of classical security perceptions and strategies. With this transformation, cyber security has become a main concern for decision-makers. This study discusses the theory of cyber warfare to better understand the asymmetrical nature of cyber warfare. Nation states are willing to gain superiority by trying to deter the adversary with the minimum effort possible. Cyber warfare has gained importance since it creates asymmetry in struggle for power in the international order, which offers gains in both effectiveness and efficient use of resources. In addition to asymmetrical means, powerful states are using their absolute power to deter potential adversaries, including conventional and nuclear power. Alongside military power, those states are leveraging their privileged membership in the United Nations Security Council as a means of enhancing their total power.

Cyber attack against Estonia was a wake-up call for the international community. Cyber warfare entered the agenda of the nations' security priorities. It showed international community that attribution is the main problem in cyber incidents. You cannot use deterrence as a tool of Defence without developing capabilities and knowing your adversary. By using zombie computers, distributed denial of service attacks forensic analysis.

Cyber attacks against Georgia in 2008 showed that cyber fare could play a vital role in gaining psychological superiority before, during and after kinetic conflict. Not only the international community but also Georgian citizens could not be informed properly about the incidents happening inside their borders. Although Russia's involvement in cyber attacks against Georgia has never been publicly acknowledged or formally proven, Russia appears to have immensely benefited from the cyber attacks in their Georgian campaign. It is not even clear that formal state institutions were involved in this aspect of the Russian campaign, and if civilians were involved from nationalist motives, it would add another layer of complexity from an international law perspective, and thus another layer of cover for the Russians.

Stuxnet hit Iran's uranium enrichment facility and damaged its ability to produce enriched uranium for some period of time. Stuxnet was a demonstration of U.S and Israel cyber power capabilities to deter adversaries. Although neither nation has acknowledged its involvement, this was a military operation that tested

* bariserdogan@hotmail.com

the boundaries of international law. Cyber attack is a powerful weapon that can allow cost escalation; Iran could not retaliate for the Stuxnet incident due to lack of cyber capabilities. Use of cyber capabilities must be brought under the umbrella of international law, norms and principles.

This article also aims to provide considerations for decision makers tasked with ensuring cyber security at the national level. Developing a cyber security strategy and implementing action plans for such a strategy is a must for our national security. A program for the prioritization of critical infrastructure would help to classify critical systems and identify the security risks. Public and private sector coordination has vital importance in this area, since most systems depend on commercial cyber infrastructure as well as state-owned or state-managed infrastructure. Developing offensive capabilities is an integral part of the deterrence strategies and human capital is the most valuable part of the deterrence. Risk analysis and threat assessments must be improved to provide relevant data for developing strategies to ensure cyber security in the long term. The cyber domain must be treated as an operational domain like air, land and sea.