SİBER GÜVENLİK PROBLEMLERİNİN ULUS-DEVLET ÜZERİNDEKİ ETKİSİ: STUXNET

Şeyma Altunkaya[1], İnönü Üniversitesi

ÖZET

Temelde Soğuk Savaş'ın iki kutuplu düzeninde ABD-SSCB arasında bir rekabet aracı olarak ortaya çıkan siber uzay, ARPANET'in kurulmasıyla ortaya çıkan internet ile milyonlarca kullanıcıya erişmektedir. Çok-merkezli inşa edilen siber uzayın zamanla kontrol edilemeyen bir alana dönüşmesi uluslararası ilişkilerde de güvenlik problemlerine yol açmıştır. Çalışmada 2010 yılında sıfır gün açıklıkları kullanılarak oluşturulan bilgisayar solucanı Stuxnet, özellikle İran İslam Cumhuriyeti'ndeki nükleer tesislere verdiği zarar bağlamında ulusal güvenlik problemi olarak ele alınmıştır. Uluslararası toplumda 2002'den itibaren İran'da nükleer silah üretimi şüphelerinin başlaması ve 2010'da bu şüphelerin yoğunlaşması İran üzerindeki uluslararası baskıyı arttırmış ve 2010'da Stuxnet saldırısının eşzamanlılığı Stuxnet'in, İran'ın ulusal güvenliğine tehdit oluşturan bir siber silah olduğu yorumlarının yapılmasına yol açmıştır. Siber güvenliğin ulus-devlet üzerindeki etkisinin incelendiği çalışmada Stuxnet, örnek olay olarak ele alınmıştır. Çalışmanın sonucunda İran'da 2009 ve 2010 arasında faaliyet gösteren santrifüj sayısının %23 gerilediği ve uranyum zenginleştirme faaliyetlerinin yavaşlatıldığı belirtilerek, İran İslam Cumhuriyeti'nin bir ulus-devlet olarak saldırıya uğradığı ve buradan hareketle ulus-devletlerin siber güvenlik problemlerine karşı savunmasız kaldığı vurgulanmıştır. Bu bağlamda, devletlerin siber güvenlik problemlerine karşı işbirliği yapmasının, uluslararası bir örgütün kurulmasının, uluslararası hukukun buna göre düzenlenmesinin ve nitelikli uzmanların istihdam edilmesi gibi girişimlerin gerekliliği değerlendirilmiştir.

Anahtar Kelimeler: Siber Uzay, Siber Güvenlik, İnternet, İran İslam Cumhuriyeti, Stuxnet

Giriş

Siber uzayın gelişmesi ile ortaya çıkan birçok teknolojik yeniliğin yanı sıra belirsizliklerin de ortaya çıkması Uluslararası İlişkiler disiplini açısından ele alınmaktadır. Ulus-devletlerin yaşanan belirsizlik içerisinde nasıl etkilendiği ise siber güvenlik kavramı çerçevesinde ele alınmaktadır. "*Birbirine bağlı sistemler ve onların altyapıları aracılığıyla bilgiyi kullanan tüm elektronik kullanıcıların eylemde bulunduğu operasyonel alan*" (Nye, 2010:3) olarak tanımlanan siber uzay, ortaya çıkardığı güvenlik problemleriyle özelde ulus-devletlerin genelde ise Uluslararası İlişkilerin 21.yy'da en çok ilgilendiği konuların başında gelmektedir.

[1] Araştırma Görevlisi, İnönü Üniversitesi İktisadi ve İdari Bilimler Fakültesi, Siyaset Bilimi ve Uluslararası İlişkiler Bölümü, Battalgazi/Malatya, ORCID ID: 0000-0001-6260-1344, seyma.altunkaya@inonu.edu.tr

Soğuk Savaş'ın iki kutuplu düzeninde siyasi güç rekabeti aracı olarak ortaya çıkan siber uzay kavramı, 1962 ARPANET'in (*Advanced Research Projects Agency*) kurulması ile sonuçlanmıştır. SSCB'nin Sputnik I ve II uydularına karşılık siyasi üstünlük elde etmek isteyen ABD, ARPANET'i kurarak farklı yerlerde bulunan bilgisayarlar arasında bağlantıyı sağlamış ve öncelikle Fransa ve İngiltere bağlantılarıyla İnternet kavramını (Bilgisayar ağlarının uluslararası ağı) ortaya çıkarmıştır. 80'lerle birlikte IP (*Internet Protocol*) adresleriyle küredeki tüm cihazların birbiriyle irtibat kurmasının sağlanmasıyla internet, herkes tarafından ulaşılabilir olmuştur. Bu durum hem siber uzay kavramının tanımını hem de siber güvenlik problemlerini eşzamanlı ortaya çıkarmıştır.

Çok-merkezli olarak inşa edilen ve herkes tarafından kullanılabilen siber uzayın ilk güvenlik problemleri 1980'lerde bireysel saldırılar olan 'Elk Cloner' virüsü ve 'Moris Kurtçuğu' ile başlamıştır; fakat özellikle ulus-devletler için bir problem haline gelmesi, 2000'li yıllara tekabül etmektedir. Bu minvalde değerlendirilebilecek olan en önemli saldırılar 2007 Estonya saldırıları, 2008 Rusya-Gürcistan anlaşmazlığının hibrid savaşa dönüşmesi ve 2010 İran'a uygulanan Stuxnet saldırısı olarak belirlenmiştir. Bu çalışma siber güvenliğin ulus-devletleri nasıl etkilediğini 2010'da İran'a yönelik Stuxnet saldırısı kapsamında değerlendirecektir. Her ne kadar saldırganların kimliği ve amacı net olarak saptanamasa da saldırıdan en çok zarar gören ülkenin İran olması ve saldırı neticesinde İran nükleer tesislerinin kapasitesinin zarar görmesi, Stuxnet saldırısı hakkında fikir yürütmeyi mümkün kılmaktadır.

İnternetin Tarihi ve Siber Uzay

Teknolojinin gelişmesi, taşınabilir bilgisayarlar, internetin yaygınlaşması, akıllı telefonlar, nesnelerin interneti, bulut teknolojisi ve nicesi ile coğrafi sınırların önemsizleştiği ve 21.yy'nin dünyayı yeniden şekillendirdiği görülmektedir. Teknolojinin sağladığı bu kolaylıkların yanı sıra birtakım belirsizliklere de yol açması birçok disiplin tarafından değerlendirilmektedir. Uluslararası ilişkilerin aktörlerinden biri olan ulus-devletler şekillenen dünyayı yönetilebilir kılmak için bilişim teknolojilerini değerlendirmeye ve geliştirmeye çalışmaktadırlar. Değerlendirmenin ve gelişimin başlangıç noktası ise internetin icadı olmaktadır.

1957'de SSCB'nin ilk yapay uydusu Sputnik I ve sonrasında Sputnik II'yi uzaya göndermesi Soğuk Savaş'ın iki kutuplu dünyasında ABD'nin güvenlik endişelerini arttırmıştır. SSCB'nin teknolojik ilerlemesinin gerisinde kalmamak için Eisenhower yönetimi teşvikiyle ABD, 1958'de hem uzay araştırmaları projeleri hem de balistik füze savunması ve nükleer tesislerin saptanması gibi projeleri içeren ARPA'yı (*Advanced Research Projects Agency-İleri Araştırma*

Projeleri Ajansı) kurarak teknolojik olarak SSCB'nin üstünlüğünü ele geçirmeye çalışmıştır. İlk etapta bir ajans olarak kurulan ARPA'nın çoklu bilgisayar sistemine entegre edilmesi ve çok sayıda bilim insanının tek bir ağda bir araya getirilmesi 1962 yılında ARPANET'in (*İleri Araştırma Projeleri Ajansı Ağı*) kurulmasıyla sağlanmıştır (Bıçakçı, 2013: 5-6). Güvenlik endişeleriyle kurulan ARPANET, farklı alanlarda bulunan bilgisayarlar arasında bağlantı kurmayı hedeflemekteydi. Bu sebeple, bir bilgisayar zarar görse bile sistemin çalışmasına devam etmesi amaçlanmıştır. Buradan hareketle, ARPANET ilk kurulduğunda esas güvenlik meselesi siber güvenlikten ziyade fiziksel güvenlik olarak düşünülmüştür.

İnternetin ilk nüvesi olarak sayılan ağ (*Network*) sistemi 1969'da kurulmuştur. Temelde dört farklı yerde bulunan bilgisayarlar (Los Angeles Kaliforniya Üniversitesi, Stanford Araştırma Enstitüsü, Utah Üniversitesi ve Santa Barbara Kaliforniya Üniversitesi) arasında bilgi aktarımı yapılmaya çalışılmaktadır (Akyeşilmen, 2018: 26-27). Nihayetinde ARPANET ile artık bilgisayarlar arası başarılı ağ aktarımları yapılabilmiş; fakat bu ağların nasıl dizayn edileceği hala bir problem olmuştur (Brendon, 2010: 79-80). Bu bağlamda Paul Baran (1962: 4) bilgisayarları birbirine bağlamanın üç muhtemel örneğini üretmiştir; her programlama düğümünün tek bir merkezden yönlendirildiği merkezi ağ (*centralized),* merkezi olmayan ağ (*decentralized*) ve dağıtık ağ (*distributed)…* Dağıtık ağda hiçbir ağ hayati öneme sahip olmadığından diğer ağ çeşitleri gibi hassas değildir. Bu sebeple içlerinden en güçlüsü dağıtık ağ seçilmiştir (Brendon, 2010: 79-80). Bu ağın seçilmesinde önemli olan etkenlerden biri, Küba füze kriziyle gün yüzüne çıkan olası bir nükleer saldırıda iletişim hatlarının işlerliğinin kesilmesi sorunu idi. Saldırı sonucunda elektrik bağlantısını sağlayabilen bu ağ tasarımı sonrasında ARPANET, İngiltere ve Fransa'daki ağlarla birleştirilerek "Bilgisayar Ağlarının Uluslararası Ağını" -İnterneti- ortaya çıkarmıştır. Giderek kullanıcı sayısı artan sistem, FTP (*File Transfer Protocal*) ile dosya gönderim imkanlarının da gelişmesini sağlamıştır. İnternetin sınırlılığının kalkması ve kişisel bilgisayarların oluşturulması ise 1975 yılında IBM 5100 ile başlamıştır (Bıçakçı, 2013: 6-8). 80'ler ile artık hem IP adresleriyle bütün cihazların birbirleriyle bağlantı kurması sağlanarak hem de DNS (*Domain Name System*) ile daha akılda kalıcı alan adları oluşturulmaya başlanarak iletişim güçlendirilmiştir (Akyeşilmen, 2018: 29). Son durumda hem kullanıcı sayısı artan hem ağları genişleyen ARPANET artık kontrol edilemez bir alan olmaya başlayınca bazı sorunları da beraberinde getirmiştir. İlk etapta insanların mutluluk kaynağı olarak tanıtılan internetin aslında kıskançlık ve rekabet duygusuyla yaygınlaştırıldığını belirten Kyong Chun (2006: 256), 11 Eylül saldırılarında da terörist gruplar tarafından kolayca ele geçirilebilen hesaplar ile internetin nasıl sömürüldüğünü ve nasıl kontrol

edilemediğini değerlendirmektedir. Herkesin kolayca erişebildiği ve kontrol edilemeyen bu sanal alan ise siber uzay kavramıyla tanımlanmaktadır. Temelde siber kavramı elektronik ve bilgisayarla ilişkilendirilen tüm eylemleri kapsayan bir sıfattır ve ilk olarak William Gibson tarafından kullanılmıştır. Gibson (1984: 51)'a göre siber uzay, "*her ulustaki milyarlarca yasal operatörün rızaya dayalı halüsinasyonudur*". Nye (2010: 3)'e göre ise: "*birbirine bağlı sistemler ve onların altyapıları aracılığıyla bilgiyi kullanan tüm elektronik kullanıcıların eylemde bulunduğu operasyonel alan*" olarak tanımlanmaktadır. Siber güvenliği anlamak için, siber uzay kavramının ve siber uzayın katmanlarının anlaşılması gerektiğini belirten Bıçakçı (2013: 10-16) siber uzayı; fiziksel katman, kodlar katmanı, içerik katmanı ve düzenleyici katman olarak dört parçaya ayırmaktadır. Siber uzayın fiziksel katmanı; ana kart, hafıza (RAM), işlemci, disk, Ethernet kartı, kablolar ve yönlendiriciler (*router*) gibi somut bilgisayar ekipmanları ve akıllı telefonlar, televizyon ve uydu sistemleri gibi ağ sistemine entegre olmuş tüm elektronik cihazları kapsamaktadır. Mamafih, fiziksel katman, kodlar katmanı olmadan da çalışamamaktadır. 1 ve 0 olarak oluşturulmuş programlama dilleri sayesinde hem işletim sistemleri hem de internet içerik erişimi mümkün kılınmaktadır. Fiziksel katman ve kodlar katmanı sayesinde internette bilgi erişimine izin veren içerik katmanı oluşturulmakta ve düzenleyici katman ile bu içeriğin ulusal hukuki düzenlemelerle sınırlanması mümkün kılınmaktadır.

Aslında bir Soğuk Savaş ürünü olan, dört katmandan oluşan ve temelde fiziksel güvenliği sağlamak için çok-merkezli olarak inşa edilen siber uzay, zamanla kontrol edilemeyen ve birçok güvenlik problemine yol açan bir alana dönüşmüştür. Öyle ki Uluslararası İlişkiler disiplininde birçok teori tarafından benimsenen uluslararası sistemin anarşik doğasının, belli bir merkezi yönetimi olmadığından siber uzay için de geçerli olduğu düşünülmektedir (Akyeşilmen, 2018: 59). Bu yaklaşıma sebep olan ilk güvenlik problemi ise 1980'lere tekabül etmektedir. İlk bilgisayar virüsü 15 yaşında olan Richard Skrenta'nın Floopy diskleriyle bilgisayarlar arasında kendi kendine çoğalan 'Elk Cloner' adlı virüsü bulmasıyla başlamıştır (Haberler, 2013). İnternete büyük zararlar veren 'Moris Kurtçuğu' ise 1987 yılında gerçekleşmiştir. Robert Tappan Morris tarafından oluşturulan ve DDoS saldırısı olan kurtçuk, NASA, Pentagon ve Stanford Üniversitesi gibi önemli kurumların bilgisayarlarına da zarar verdiğinden tarihte deneyimlenen en kapsamlı saldırı olarak belirtilmiştir (Akyeşilmen, 2018: 236). Aynı dönemlerde John Badham yönetmenliğinde çekilmiş 1983 tarihli 'War Games' Amerikan bilim kurgu filmi, 17 yaşındaki bir çocuğun (hacker) kendi evinde kurmuş olduğu bilgisayar sistemiyle, ABD ve SSCB arasında termonükleer bir savaş başlatabileceğini konu

edinmektedir. Filmde özellikle makinaların insanları ele geçirebilmesi ve ortaya çıkabilecek olan güvenlik problemleri titizlikle vurgulanmaktadır. Filmle birlikte popülerleşen 'hacker' kültürü siber uzay çalışmalarında da literatürdeki yerini almaktadır. Kelime anlamı olarak 'bilgisayar teknolojisinde yetenekli olan kişi' olarak çevrilse de genellikle olumsuz manada (güvenliği aşarak bilgisayarlara/ağlara izinsiz giren kişi -cracker) tanımlanmaktadır. Yaptıkları eylemlere göre (iyi niyetli, kötü niyetli vs.) sınıflara ayrıldıktan sonra yaptıkları işlemin türüne göre de ayrılmaktadırlar; beyaz şapkalı (iyi niyetli), siyah şapkalı (kötü niyetli), gri şapkalı (genellikle iyi niyetli), mavi ve kırmızı şapkalı (genellikle hükümet ve şirket ağlarını 'heckleyenler') ve hacktivistler (siyasi, ideolojik, dini ve sosyal amaçlı eylem yapanlar) (Tutorialpoint, 2016: 3)… Tüm bu veriler ışığında 1980'lerde siber uzay artık siber güvenlik kavramıyla birlikte ele alınmaya başlanmıştır.

Siber Güvenlik ve Ulus-Devlet

Elk Cloner virüsüyle endişeleri artıran siber uzay, Soğuk Savaş'ın sona ermesiyle birlikte daha da girift bir hal almaktadır. Aynı dönemde ortaya çıkan 'world wide web' (www) formatı ile farklı bilgisayarlar arası bağlantının daha hızlı ve daha kolay bir şekilde sağlanması ve kişisel bilgisayarların yaygınlaşması, bilgisayarın gündelik hayatta daha çok kullanılmasına yol açmaktadır (Bıçakçı, 2013: 32-38). Kamusal işlemlerini, haberleşme sistemlerini ve hatta güvenliklerini siber uzayda yürüten devletler tehditlere ve saldırılara açık sanal bir gerçeklik içerisinde yaşamaktadır. Bu minvalde; 1994'te Rus birliklerinin Grozni'ye saldırısının ardından Çeçenlerin interneti savaş alanı olarak kullanması, NATO birliklerinin 1999'da Sırp hedefleri bombalamasıyla Sırp hackerların NATO ve üye ülke askeri haberleşme sistemlerine DDoS (sunucu işlemcilerini cevap veremez hale getirme yöntemi) siber saldırı düzenlemeleri ve nihayetinde Rusya ve Çin'in Sırp saldırılarını desteklemeleri, 11 Eylül saldırılarında teröristlerin internet üzerinden haberleştiklerinin saptanması, 2007 Estonya-Rus anlaşmazlığının Estonya'daki resmi kurumların hacklenmesine sebep olması ve 2008 Gürcistan-Rusya anlaşmazlığının hibrid savaşa (hem geleneksel savaş yöntemi hem de siber saldırı) dönüşmesi gibi tüm örnekler, uluslararası ilişkilerdeki güç mücadelelerinin siber uzaya da taşınarak güvenlik problemleri yarattığı şeklinde yorumlanabilmektedir (Bıçakçı, 2013: 32-38). Bu bağlamda bilgisayar güvenlik firması McAffee'nin kötücül hacktivist eylemlerin artışının ileriki yıllarda katlanarak devam edeceğini; çünkü çoğu endüstriyel ve ulusal altyapıların modern bağlantılarla dizayn edilmediğinden saldırılara karşı korunmasız kaldığını, öyle ki kendi firmalarının bile 2012 yılında 'Anonymous' haktivistleri tarafından saldırıya uğradığını beyan etmesi önemlidir (Geers, 2013: 465).

Siber güvenlik son yıllarda siber uzayın ekonomik, sosyal ve siyasal birçok alanını ilgilendirecek kadar genişlemiştir. Farklı ülkelerde ve farklı ülkelerdeki siber güvenlik strateji belgelerinde farklı tanımlanan siber güvenlik, "*siber uzayı ve siber uzay kaynaklı sistemleri korumak için kullanılan kaynakların, süreçlerin ve yapıların organizasyonu ve bir araya getirilmesi*" olarak tanımlanmaktadır (Craigen vd., 2014: 17). Bu bağlamda Uluslararası İlişkiler disiplini de siber güvenliği içerecek yeni yaklaşımlar ve kavramlar (siber güç, siber çatışma, siber suç, siber saldırı, siber savaş gibi) geliştirmektedir. Siber güvenlik probleminin ortaya çıkmasında; çeşitli amaçları olan kötücül hackerler, internet yapısının saldırılara açık olması, siber güvenlik problemlerine yol açabilecek unsurlar hakkında bilgi paylaşımının yetersiz olması, saldırıların çoğu zaman tespit edilememesi ve failin bulunamaması, siber güvenliğe karşı koyabilecek araçların zayıf ve yetersiz olması ve uluslararası işbirliğinin eksik olması gibi sebepler etkili olabilmektedir (Akyeşilmen, 2018: 109). Bu noktada siber güvenliğin amaçları ise bilginin gizliliği, bütünlüğü ve erişilebilirliği olarak ifade edilmektedir. Bilginin gizliliği yetkisiz kişilerce kullanılmasını belirtirken, bütünlüğü ise bilginin içeriğinin çoğaltılması, dönüştürülmesi ve yanlış bilgi eklenmesi gibi uygulamalarla değiştirilmesi olarak tanımlanmaktadır. Erişilebilirlik ise bilginin 'DoS', 'DDoS', 'Blackhole', 'Broadcast Tampering', 'Malware' ve 'Spamming' gibi isimlerce adlandırılan çeşitli siber saldırı yöntemleriyle bilginin elde edilebilmesini belirtmektedir (Sumra vd., 2014).

Siber uzayın siber güvenlik problemleri Uluslararası İlişkiler disiplini içerisinde iki şekilde değerlendirilmektedir. Siber güvenliği uluslararası ilişkilerde yüksek politika olarak tanımlayarak ulusal güvenlik bağlamında değerlendiren çalışmalar ki bunlar savaş ve çatışma teorileri bağlamında siber güvenliği ele almaktadırlar. Örneğin Arquilla, siber savaşı yeni bir çatışma türü olarak nitelendirmektedir ve Stuxnet kurtçuğunu da stratejik siber saldırı olarak ele almaktadır (Arquilla, 2012). İkinci olarak da siber güven (siz) lik problemleri olarak tanımlanan yahut 'siber savaş' olarak nitelendirilen olayların abartıldığını, askeri doğasının olmadığını fakat siber suç kapsamında ele alınabileceğini değerlendirenler ki Schneiler bu kapsamda değerlendirilmektedir. Schneiler, "*ABD siber savaşa karşı mücadele ediyor ve biz kaybediyoruz*" diyen Mike McConnel'in ve "*9/11 son on yıl içinde gerçekleşti ve biz onu fark edemedik*" diyen Amit Yoran'ın cümlelerini retorik olarak ifade etmiş ve 'siber savaş' söylemlerinin aşırı hevesli hükümet yetkilileri tarafından abartıldığını dile getirmiştir (Schneiner, 2010). Akyeşilmen ise siber saldırıları çatışma teorileri kapsamında değerlendirmekte ve dört gruba ayırmaktadır; görünmez çatışma, görünür çatışma, kriz ve şiddetli kriz (sınırlı savaş) ... Şiddet içermeyen görünmez çatışmaları; spamlar, dolandırıcılık

işlemleri, zararlı yazılımlar, sahte e-posta olarak örneklendirirken görünür çatışmaları ise bilgisayar sabotajları, pornografi, mali suçlar, reklam yazılımları olarak örneklendirmektedir. Şiddet içeren kriz çatışma türlerini ise siber terörizm, kritik altyapı saldırıları ve Stuxnet gibi fiziksel olarak da zarar veren yazılımlar olarak nitelendirirken, şiddetli kriz için sürekli ve yoğun olarak yapılan kritik altyapı saldırılarını (Estonya olayı) örnek vermektedir. Bu bağlamda kronolojik olarak bir sınıflandırma yapıldığında, 1980 ve 1990 yıllarındaki siber güvenlik problemleri daha çok bireysel siber güvenlik problemlerini içerirken, 2000'lerde referans obje sınıflandırmasına dijital kurumlar ve şirketler girmektedir; fakat 2007 Estonya DDoS saldırıları ve 2010 Stuxnet ile siber güvenlik hem uluslararası bir nitelik kazanmakta hem de ulus-devletlerin önemli bir problemi haline gelmektedir (Akyeşilmen, 2018: 221-227).

Ulus-devletler siber güvenliği uzun bir süre alçak politika (*low politics*) alanı olarak değerlendirerek çoğu zaman özel sektörün eylemde bulunduğu bir alan olarak nitelendirmekteydi; fakat yukarıda da ifade edildiği gibi özellikle 2007 Estonya DDoS saldırılarıyla ulusal güvenlik meselesi olarak görülmeye başlandığından yüksek politika (*high politics*) alanı olarak dillendirilmeye başlanmıştır. Siber güvenliğin bu denli ulusal güvenliğin bir parçası haline gelmesinde; genellikle kritik altyapıları hedefleyen saldırıların yapılması, kişisel yahut kamusal gizli bilgilerin ele geçirilmesi, hactivist eylemlerle kurumsal bilgilerin çalınması, ticaret ve hizmet sektörünün faaliyetlerinin duraklatılması ve ticari bilgilerin çalınması gibi çeşitli faktörlerin etkili olduğu söylenebilmektedir. Bu bağlamda devletler egemenlik alanlarını koruyabilmek için siber güvenlik problemleriyle mücadele etmede çeşitli yöntemlere başvurmuştur. Ulusal düzeyde siber güvenlik strateji belgeleri ve eylem planları bu amaçlar doğrultusunda hazırlansa da savunma araçlarının yetersiz olması, çoğu zaman failin bilinememesi ve kesin kanıtlarla saldırının tanımlanamaması gibi etkenler ulus-devletler açısından siber problemleri önemli bir güvenlik problemi olarak gün yüzünde tutmaktadır (Akyeşilmen, 2018: 129). Bu konuda operasyonel siber çatışma kapsamında değerlendirilebilecek Stuxnet'in İran nükleer kapasitesine nasıl zarar verdiği önem arz etmektedir.

İran Nükleer Tehdidi ve Stuxnet Olayı

1979 İslam devrimi ile İran'ın büyüyen gücünün Batı değerleri için bir tehdit oluşturmaya başlamasıyla uluslararası toplumun İran üzerinde yaptırımları artmıştır. 1979-2002 yıllarını kapsayan yaptırımlar özellikle İran'ın terörizme verdiği destekle ve insan hakları ihlalleriyle ilintili olsa da 2002 yılından itibaren İran'da gizli nükleer tesislerinin ortaya çıkması ve nükleer

tehdit olarak algılanmaya başlanmasıyla yeni yaptırımlar getirilmiştir. Bu bağlamda, Birleşmiş Milletler Güvenlik Konseyi'nin 2006 yılında uygulamaya koyduğu yaptırımlar ve 2010'da Avrupa Birliği ekonomik ve siyasi yaptırımları İran'ın nükleer tehdit olarak görülmesindeki algıları kanıtlar niteliktedir (Bayar, 2016: 88 & Küpeli, 2016: 106-111). Netice itibariyle 2010'da uluslararası toplum, BMGK'nın 1929 sayılı kararıyla İran'dan, nükleer silahların yayılmasını durdurmak için uranyum zenginleştirme programını askıya almasını istemekteydi (Mehta, 2015: 101 & Seyrafi ve Ranjbarian, 2018: 270). Bu bağlamda, İran'ın silah üretimini sağlayabilecek olan uranyum zenginleştirme programının engellenmesi kapsamında İran, ABD, Rusya, Çin, Fransa, İngiltere ve Almanya arasında 'Kapsamlı Ortak Eylem Planı' (*Joint Comprehensive Plan of Action*) 2015'te imzalanmıştır. Anlaşma İran'ı uranyum zenginleştirme düzeyi, miktarı, nükleer reaktör çeşidi ve santrifüj sayısı gibi birçok noktada sınırlamıştır. İran'ın olası anlaşmayı ihlal etme ihtimaline karşılık ise (özellikle Natanz ve Fordo tesislerinde), anlaşmaya uyup uymaması Uluslararası Atom Enerji Ajansı'nın (UAEA) kontrolüne bırakılmıştır; fakat nihayetinde bu sınırlamalar yeterli olmamış, İran'ın el altından nükleer silah üretimine devam edebileceği (çünkü UAEA askeri tesisleri gözlemleyememekte) şüpheleri hem bölge ülkelerince hem de ABD'deki bazı kesimler tarafından (Cumhuriyetçi kanat) dillendirilmeye devam edilmiştir. (Rezaei, 2017 & Mehta, 2015: 108). Özellikle bölge ülkelerinden gelen şikayetlerin bir kaçına değinecek olursak; İsrail Başbakanı'nın İran nükleer kapasitesine dikkat çekmesi üzerine, Suudi Arabistan Kralı Abdullah bin Abdulaziz'in ABD'ye "*yılanın başını kesmeliyiz*" söylemleri, Mısır Cumhurbaşkanı Hüsnü Mübarek'in İranlıları "*tam bir yalancı*" olarak itham etmesi, Birleşik Arap Emirlikleri Savunma Bakanı'nın İran Cumhurbaşkanı Mahmut Ahmedinejat'ı Adolf Hitler'e benzetmesi, Bahreyn'in "*İran nükleer programı durdurulmalıdır*" çağrısı ve Ürdün Kralı Abdullah'ın İran'a doğrudan saldırıyı değil de, İran'ın gücünü engellemeyi ima etmesi bu örneklerden birkaçını oluşturmaktadır (Farwell ve Rohozinski, 2011: 28).

Şimdiye kadar saldırı ile ilgili çeşitli görüşler ileri sürülse de saldırı öncesi ve sonrası durum değerlendirildiğinde Haziran 2010'da Stuxnet olarak isimlendirilen siber solucanın İran'daki Natanz nükleer tesislere yönelik bir saldırı olduğu iddia edilmiştir. 60.000 bilgisayara bulaştırılan solucanın yarısından fazlası İran'da bulunmakla birlikte, bu durum Hindistan, Endonezya, Çin, ABD gibi diğer ülkeleri de etkilemektedir (Farwell ve Rohozinski, 2011: 23). Alman Uzman Langner (2010), Stuxnet'i hem İran nükleer programlarını hem de Bushehr Nükleer santralini hedef alan askeri siber füze/savaş başlığı olarak tanımlarken, daha önce dünya üzerinde böyle bir saldırının olmadığını beyan etmiştir. Uzaktan belirli hedeflere karşı

kurulan karmaşık bir bilgisayar programı olarak tanımlanan Stuxnet, yeni bir tür "ateşle ve unut" yazılımıyla kurgulanmıştır. Stuxnet'in hedef sahası internet erişiminden arındırılmış ve USB gibi aracı aygıtlarla erişimi ve kontrolü sağlanmıştır. Saldırıda yazılımın ilk oluşturulduğunda var olan açıkların süreç içerisinde fark edilip, açıklık olan yerlerden bilgi sızdırma işleminin yapılması yöntemi (Sıfır/İlk Gün Açıkları-Zero-day Exploit) kullanılmıştır (Farwell ve Rohozinski, 2011: 24). Bu şekilde oluşturulmuş bilgisayar solucanının özellikle İran uranyum zenginleştirme programını hedeflediği dillendirilmiştir.

Stuxnet'in en belirgin özelliği belirli bir anakartı (PLC-Programlanabilir Kontrol Cihazı) hedef seçmesidir. Microsoft Windows işletim sistemleri ile programlanan kurtçuk, Siemens'in S7 300 modülünü hedef seçmiştir. Hedef seçerken yukarıda da belirttiğimiz gibi Windows'un ilk gün açığını kullanmıştır. Stuxnet'in diğer önemli bir özelliği ise, hedefine (Siemens PLC) ulaşıncaya kadar çalıntı imzalar kullanması ve bulaştığı hiçbir bilgisayara zarar vermeyerek kendi ömrünü de uzatmasıdır (Çahmutoğlu, 2021: 11; Bıçakçı, 2013: 41-42). İran nükleer tesislerine hangi yollardan bulaştığı konusunda kesin bir kanıt olmamasına rağmen, İran'ın nükleer tesislerinin kapalı ağ (air-gapped) ile yürütüldüğü bilindiğinden (küresel internete bağlı olmayan), nükleer tesislerde çalışan birinin USB yoluyla kurtçuğu bulaştırdığı iddia edilmiştir. Stuxnet kurtçuğu bulaştığı hedefte makina ile kontrol bilgisayarı arasındaki bağlantıyı koparmış ve işlevini gizlenerek gerçekleştirmiştir (Akyeşilmen, 2018: 243). Bu yöntemle dışarıda herhangi bir sorun yokmuş algısı oluşturan kurtçuk, nükleer reaktörleri maksimum hıza ulaştırıp (1410Hz) sonra da ani fren yaptırarak 2Hz'ye düşürüp sonra tekrar 1064 Hz'ye çıkarıp tahrip olmasına sebep olmuştur (Halliday, 2010). Bu süre zarfında onu kullananların istedikleri bilgileri de sistem üzerinden sızdırabilmiştir. Ek olarak kendi kendini yok edebilme özelliği de barındırdığından failinin bulunmasını imkânsız kılmıştır (Akyeşilmen, 2018: 244).

Nihai olarak Stuxnet gerçekten İran nükleer programını engelledi mi sorusu sorulduğunda farklı cevaplar alınmıştır. İran İletişim Bakanı Reza Taghipour'un, casus solucanın etkilerinin ve zararlarının ciddi olmadığını ve bulaştığı her yerin temizlendiğini bildirmesi; fakat Sanayi ve Maden Bakanı Mahmut Liai'nin 300.000 bilgisayarın etkilendiğini ve solucanın İran'a karşı bir elektronik savaş olduğunu belirtmesi önemlidir (Sanger, 2010). Ek olarak Cumhurbaşkanı Ahmedinejat'ın Stuxnet'in İran nükleer programını hedef aldığını, uranyum zenginleştirme santrifüjlerinin bir kısmını yavaşlattığını; fakat sadece belirli santrifüjlere zarar verdiğini ve durumun uzmanlar tarafından kontrol altına alındığını bildirmesi çelişki doğurmaktadır (Nagesh, 2010). İran her ne kadar pek fazla zarar görmediklerini ve hiçbir tesisin etkilenmediğini belirtse de Siemens'ten gelen bilgilere göre 14 endüstriyel tesis ciddi bir

şekilde zarar görmüştür (Farwell ve Rohozinski, 2011: 29). Bu durumun önemli bir kanıtı da Uluslararası Atom Enerji Ajansı'ndan gelen bilgilerdedir. Buna göre İran, Natanz'daki santrifüjlere bir hafta uranyum takviye etmeyi durdurmuştur ki bu aslında İran'ın saldırıdan ciddi zarar gördüğünün belirtisidir (Broad, 2010). Daha sayısal olarak ifade edilecek olursa İran'da 2009 ile 2010 arasında faaliyet gösteren santrifüj sayısı 4920'den 3772'e düşmüş ve %23 gerilemiştir (Markoff ve Singer, 2010). İran'daki resmî açıklamalarda Natanz tesislerine saldırının olmadığı beyan edilse de ISIS raporunda, 2010'un başında Natanz'daki Yakıt Zenginleştirme Tesisi'ndeki (FEP-Fuel Enrichment Plants) 1000 IR-1 santrifüjünün devre dışı bırakıldığı saptanmış; fakat Stuxnet'in gerçek etkisinin bilinmediği belirtilmiştir. UAEA'nın üç ayda bir yayınlanan raporunda Natanz'daki kaskad sayılarına göre saptamalarda bulunulmuştur. FEP'lerdeki A24, A26, A28 modüllerini belirli sınıflandırmalar altında değerlendiren raporda özellikle A26 modülündeki 6 kaskadın devre dışı bırakıldığı ki her kaskadda 164 IR-1 santrifüjü bulunduğundan yaklaşık 1000 santrifüjün devre dışı bırakıldığı tespit edilmiştir. Netice itibariyle, Stuxnet'in amacı eğer FEP'teki tüm santrifüjlerin devre dışı bırakılmasıysa bunun gerçekleşmediği ama eğer amaç belirli sayıdaki santrifüje zarar verip İran'ın FEP üretimini yavaşlatmaksa bunun başarıya ulaştığı belirtilmiştir. Aşağıda santrifüj kaskad sayılarındaki değişim detaylıca gösterilmektedir (Albright vd., 2010: 2-8).

Tablo 1

Kaskad Sayılarındaki Değişim (31 Ocak 2010)

Table 1: Number of Centrifuge Cascades enriching, under vacuum, installed, or with centrifuges disconnected, January 31, 2010

	Fed with UF_6	Under Vacuum	Installed, not Under vacuum	With Centrifuges Disconnected	Total
Module A24					
Aug. 12, 2009	18	0	0	0	18
Nov. 2, 2009	18	0	0	0	18
Jan. 31, 2010	17	1	0	0	18
May 24, 2010	18	0	0	0	18
Aug. 28, 2010	17	0	1?	0	18
Module A26					
Aug. 12, 2009	10	8	0	0	18
Nov. 2, 2009	6	12	0	0	18
Jan. 31, 2010	6	1	0	11	18
May 24, 2010	6	7	0	5	18
Aug. 28, 2010	6	6	6	6	18
Module A28					
Aug. 12, 2009	0	0	14-15	0	14-15
Nov. 2, 2009	0	0	17 (1 being installed)	0	18
Jan. 31, 2010	0	0	16	2*	18
May 24, 2010	0	0	16	2?	18
Aug. 28, 2010	0	0	18	0	18

Kaynak: Albright, D., Brannan, P., Walrond, C. (2010). "Did Stuxnet Take Out 1000 Centrifuges at the Natanz Enrichment Plant?", *Institute for Science and International Security (ISIS)* (Aralık 2020), *8.*

Stuxnet, İran'ın nükleer kapasitesine verdiği zararın yanında, rejimin siyasi olarak sorgulanmasına da sebep olmuştur. Bu konuda kanıtlar yeterli olmamakla birlikte, siber alan

doğası gereği rejimlerin otoritesini zayıflatabilen bir araç olarak kolayca kullanılabilmektedir. Geleneksel askeri araçları kullanmaktan daha az riskli olan ve düşmanı alaşağı etmede öneme haiz olan siber saldırılar, aynı zamanda geleneksel askeri yöntemlere/araçlara göre daha az maliyetli olduğundan ulusal güç rekabetlerinde başat rol oynayabilmektedir (Farwell ve Rohozinski, 2011: 35). Stuxnet'in ulus-devlet kapasitelerine zarar vermede başarılı olduğunun bir diğer kanıtı da Stuxnet'ten sonra aynı işlevlere sahip çeşitli kötücül yazılımların ortaya çıktığının görülmesidir. 2011 yılındaki Macaristan'da ilan edilen 'Duqu' yazılımı, Stuxnet'ten sonra İran Ulusal Bilgisayar Acil Müdahale Ekibi'nin (Maher) istihbarat toplama amacıyla oluşturduğu 'Flame' kötücül yazılımı ve Lübnan'daki bankalarda ortaya çıkan Gauss, Stuxnet'ten ilham alındığına örnek gösterilmektedir (Bıçakçı, 2013: 42-43).

Verdiği zarar dikkate alındığında Stuxnet saldırısının bir silahlı saldırı yahut güç kullanma aracı olarak değerlendirilebilmesi hususunda, literatürdeki çoğunluk böyle bir değerlendirmenin yapılabilmesi için siber saldırıların geleneksel savaştaki gibi insanlara fiziksel bir zarar vermesi kriterinin alınması gerektiğini belirtmekte; fakat bu görüş örneğin kritik altyapılara verilen zararlarla insanların ekonomik ve finansal olarak çöküntüye girmesine sebep olunmasını görmezden gelmektedir (Farwell ve Rohozinski, 2011:35). Bu açıdan bakıldığında Farwell ve Rohozinski (2011: 35) Stuxnet'i ilk siber silah olarak tanımlamaktadırlar. Stuxnet'in bu şekilde nitelendirilmesindeki önemli nokta, sadece bilgisayar programlarına zarar vermeyip, aynı zamanda makinalara fiziksel olarak da zarar verebilme kapasitesine sahip olmasıdır (Akyeşilmen, 2018: 244). Literatürde ise siber saldırılar; siber terörizm, hacktivizm, hackleme, siber suç, siber casusluk ve devlet temelli bilgi savaşları olmak üzere altı kategoriye ayrılmaktadır; fakat kategoriler arasında sınır belirsizdir ve tek bir aktör birçok farklı eylemde bulunabilmektedir. Stuxnet bu kategoriler içerisinde çeşitli yazarlarca çeşitli şekillerde adlandırılmaktadır (Lachow, 2009: 439-441). Örneğin; Stuxnet'i devlet-tabanlı siber casusluk ve sabotaj hareketi olarak tanımlayan Rudner, bu şekilde üretilmiş bir siber silahın dünya genelinde hükümetlere, organizasyonlara ve kritik altyapılara kolayca zarar vereceğini belirtmiş ve siber saldırılara karşı küresel işbirliğinin geliştirilmesi gerektiğini önermiştir. Bu şekilde değerlendirildiğinde; küresel işbirliği, uygun eğitim ve nitelikli güvenlik çalışanları olmadan hiçbir stratejinin böyle etkili bir silaha karşı koyamayacağını ve ulus-devletlerin tehlike altında olacağını belirtmiştir (Rudner, 2013: 460, 472-473). Öte yandan Lunker (2018), siber uzayın hukuki olarak düzenlenişinde dört yaklaşım öne sürmüştür; Ulus-devletlerin kendi nüfusu üzerinde etkin olan İnternet'in düzenlenebilmesi için yeni yasalar çıkarması; Internet üzerindeki düzenlemelerin gerçekleştirilebilmesi için devletlerin çok taraflı

antlaşmalara taraf olması; Yeni kuralların uygulanabilmesi için uluslararası bir organizasyonun kurulması; ve son olarak yeni kuralların IP adresleri gibi bireysel kararlar sonucu oluşabilme ihtimalini hesaba katarak beklenilmesi… Bu bağlamda son yıllarda siber güvenlik strateji belgeleri ve eylem planları sayısında bir artış gözlense de doğası gereği küresel olan bir problemin tek başına ulusal düzeyde strateji belgeleriyle yahut nitelikli güvenlik personeli yetiştirmekle çözülemeyeceği ve tüm aktörleri kapsayan bir yönetişim mekanizmasına sahip olunması gerektiği aşikardır.

Sonuç

1957'de SSCB'nin Sputnik I uydusunu uzaya göndermesiyle başlayan siyasi rekabet, ABD'nin 1958 yılında ARPA'yı, 1962'de de ARPANET'i kurmasıyla sonuçlanmıştır. Güvenlik endişeleriyle kurulan ARPANET farklı yerlerdeki bilgisayarlar arası iletişimi sağlayarak internetin ilk nüvelerini ortaya çıkarmıştır. İlk etapta sadece dört merkezi birbirine bağlayan ARPANET fiziksel güvenlik dikkate alınarak kurgulansa da çok-merkezli yapısı ve kullanıcı sayısının artmasıyla kontrol edilemez bir alana dönüşmüştür. Herkesin kolayca erişebildiği, kullanabildiği ve kontrol edilemeyen bu sanal alan ise siber uzay kavramıyla tanımlanmaktadır. Fiziksel katman (ana kart, hafıza, disk vs.), kodlar katmanı, içerik katmanı ve düzenleyici katmandan oluşan siber uzay, 1980'lerle birlikte güvenlik problemlerine sebep olunca Uluslararası İlişkiler disiplini içerisinde de yer almaya başlamıştır. Siber güvenlik 1980 ve 1990'larda genellikle bireysel problemlere sebep olurken, 2000'lerde kurumlar ve şirketleri de kapsamıştır. Son yıllarda ise 2007 Estonya DDoS saldırısı, 2008 Gürcistan hibrid savaşı ve 2010 Stuxnet saldırısı ile ulus-devletlerin en büyük problemlerinden biri olmuştur. Uluslararası toplumun 2002'den itibaren nükleer silah üretme şüphesiyle İran üzerinde kurmuş olduğu baskının 2010 yılında artması ve akabinde gerçekleşen Stuxnet saldırısı, Stuxnet'in İran ulusal güvenliğine tehdit oluşturan bir siber silah olduğu yorumlarının yapılmasına sebep olmuştur. Saldırı neticesinde İran'da 2009-2010 yılları arasında faaliyet gösteren santrifüj sayısının %23 gerilemesi ve uranyum zenginleştirme faaliyetlerinin yavaşlatılması, İran'ın saldırıya uğradığı yorumlarının yapılmasını mümkün kılmaktadır. Ek olarak sıfır-gün açıklığını kullanarak kapalı ağ sisteminin aktif olduğu İran nükleer tesislerinde uzun süre varlığını hissettirmeden yerleştirilen Stuxnet solucanı hem santrifüjlere fiziksel hasar vererek hem de uzun süre resmi bilgileri sızdırarak o zamana kadar türünün tek örneği olmuştur ki böyle bir saldırının ancak başka bir ulus-devlet tarafından yapılabileceği söylenebilir. Nihai olarak Stuxnet örneğinde görüldüğü gibi, siber güvenlik problemlerine karşı ulus-devletlerin savunmasız kalması, Uluslararası İlişkiler alanında "başat aktör" olma rollerini de törpülemiştir. Bu bağlamda siber

güvenlik problemlerine karşı küresel iş birliği yapılmasının, bu alanda uluslararası bir örgütün kurulmasının, uluslararası hukukun buna göre düzenlenmesinin ve nitelikli uzmanların istihdam edilmesinin gerekliliği tartışmaya mahal bırakmamaktadır.

KAYNAKÇA

Akyeşilmen, N. (2018). *Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik,* Ankara: Orion.

Albright, D., Brannan, P., Walrond, C. (2010). "Did Stuxnet Take Out 1000 Centrifuges at the Natanz Enrichment Plant?", *Institute for Science and International Security (ISIS)* (Aralık 2020).

Arquilla, J. (2012). "Cyberwar Is Already Upon Us", *Foreign Policy*, 27.02.2012,

https://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/ (24.02.2022)

Baran, P. (1962). "On Distributed Communication Networks", *RAND Corporation*, Eylül 1962.

https://www.rand.org/content/dam/rand/pubs/papers/2005/P2626.pdf

Bayar, M. (2016). "Kapsamlı Ortak Eylem Planı ve İran'ın Nükleer Programının Geleceği", *Uluslararası İlişkiler,* 13 (51), 81-97.

Bıçakcı, S. (2013*). 21.Yüzyılda Siber Güvenlik*, İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2013.

Broad, W. J. (2010). "Report Suggests Problems With Iran's Nuclear Effort", *The New York Times*, 23.11.2010,

https://www.nytimes.com/2010/11/24/world/middleeast/24nuke.html (27.02.2022)

Brendon, L. K. (2010). "Arpanet: An Efficient Machine as Social Discipline", *Science as Culture*, 10 (1), 73-95.

Craigen, D., Diakun-Thibault, N., Purse, R. (2014). "Defining Cybersecurity", *Technology Innovation Management Review*, Ocak 2014, 13-21.

Çahmutoğlu, E. (2021). *İran'ın siber gücü,* İRAM Yayınları Raporu.

Haberler (2013). "Dünyanın İlk Virüsü 31 Yaşında, Onu Yazan Screnta 46, İlk MS Dos Virüsü İse 27" 31.01.2013

https://www.haberler.com/dunyanin-ilk-virusu-31-yasinda-onu-yazan-skrenta-4292566-haberi/ (21.02.2022)

Farwell, J. P. ve Rohozinski, R. (2011). "Stuxnet and the Future of Cyber War", *Survival: Global Politics and Strategy*, 53 (1) (28 Haziran 2011), 23-40.

Geers, K. (2013). "The Cyber Threat to National Critical Infrastructures: Beyond Theory", *International Journal of Intelligence and Counter Intelligence*, 26 (3), 453-481.

Gibson, W. (1984). *Neuromancer,* Ace Books: New York.

Halliday, J. (2010). "Stuxnet Worm is Aimed to Sabotage Iran's Nuclear Ambition, New Rearch Shows", *The Guardian,* 16.11.2010,

https://www.theguardian.com/technology/2010/nov/16/stuxnet-worm-iran-nuclear. (26.02.2022)

Küpeli, M. Ş. (2016). "Dış Politika Aracı Olarak Yaptırımlar: İran'a Uygulanan Yaptırımların Etkileri", *Türkiye Ortadoğu Çalışmaları Dergisi,* 3 (1), 97-135.

Kyong Chun, W. H. (2006). *Control and Freedom: Power and Paranoia in the Age of Fiber Optics*, Cambridge: MIT Press.

Langner, R. (2010). "The Big Picture", 19.11.2010, https://www.langner.com/2010/11/the-big-picture/ (25..2.2022)

Lachow, I. (2009). "Cyber Terrorism: Menace or Myth?", F. D. Kramer ve diğerleri (Ed.), içinde *Cyberpower and National Security (437-464),* Washington: National Defence University Press.

Lunker, M. "Cyber Law: A Global Perspective", Privacy and Cyber Crime Institute Report.

file:///C:/Users/%C5%9Feyma/Downloads/Cyber_Laws_A_Global_Perspective.pdf (24.02. 2022)

Markoff, J. ve Singer, E. D. (2010). "In a Computer Worm, a Possible Biblical Clue", *The*

New York Times, 29.11.2010,

https://www.nytimes.com/2010/09/30/world/middleeast/30worm.html (27.02.2022)

Mehta, S. (2015). "P5+1 Iran Nuclear Agreement: A Silver Lining in US-Iran Relations", *Seton Hall Journal of Diplomacy and International Relations,* 16 (2), 101-116.

Nagesh, G. (2010). "Iran Says Stuxnet Damaged Its Nuclear Program", *The Hill,* 29.11.2010,

https://thehill.com/policy/technology/130965-iran-says-stuxnet-damaged-its-nuclear-program (26.02.2022)

Nye, J. S. (2010). "Cyber Power", *Belfer Center for Science and International Affairs*, Mayıs 2010.

Rezaei, F. (2017). "Iran's Nuclear Agreement: The Three Specific Clusters of Concerns", *Insight Turkey***,** 20 (2), 167-199.

Rudner, M. (2013). "Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge", *International Journal of Intelligence and Counter Intelligence,* 26 (3), 453-481.

Sanger, D. E. (2010). "Iran Fights Malware Attacking Computers", *The New York Times,* 25.09.2010,

https://www.nytimes.com/2010/09/26/world/middleeast/26iran.html (25.02.2022)

Schneier, B. (2010). “Threat of ‘Cyberwar’ Has Been Hugely Hyped”, *CNN*, 07.07.2010,

http://edition.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/index.html?iref=allsearch (21.02.2022)

Seyrafi, S. ve Ranjbarian, A. H. (2018). ”The US’ Withdrawal from the Iran Nuclear Agreement: A Legal Analysis with Special Reference to the Denuclearization of the Korean Peninsula”, *Journal of East Asia and International Law*, 11 (2), 267-291.

Sumra, I. A., Hasbullah, H.B., Ab Manan, J. L. (2014). “Attacks on Security Goals (Confidentiality, Integrity, Availability) in VANET: A Survey”, Saira Andleep Gillani ve diğerleri, içinde *Vehicular Ad-hoc Networks for Smart Cities*, Singapore: Springer.

file:///C:/Users/len/Downloads/iwvsc07.pdf

Tutorialpoint (2016). Ethical Hacking, s.3.

https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_tutorial.pdf (23.02.2022)