SİBER TERÖRİZM VE ULUSAL GÜVENLİK: ÖRNEK ÜLKE İRAN

Seyedmohammad SEYEDI ASL
Gazi Üniversitesi

Giriş

Teknolojik gelişim, iletişim ve ulaşım imkanlarının gelişmesi günümüz dünyasında yeni tehditlerin ortaya çıkmasına, var olan tehditlerin şekil değiştirmesine ya da daha etkili hale gelmesine neden olmaktadır. Bu bağlamda tehdit türlerinin artması ve şekil değiştirmesi ve Soğuk Savaş sonrası oluşan yeni dünya düzeninin yeni bir güvenlik konseptine ihtiyaç duyması, güvenlik alanında yeni bir yaklaşımın gelişmesini de tetiklemiştir[1].

Bilişim teknolojisindeki gelişmelerin belki de en buyuk ironisi yonetimlerin (hükumetlerin) her yerde ciddi güvenlik sorunlarıyla yüz yüze gelmelerine neden olmasıdır. Coğu toplum ve yonetimler siber savaşlar, siber terorizm ve sanal suçların potansiyel tehditlerini anlamaya başlamışlar, ancak bu sorunlarla ilgili kapsayıcı onlemleri tam olarak geliştirememişlerdir[2]. Siber terörizmin tehdit potansiyeli her geçen gün biraz daha artmaktadır. Özellikle son yıllar içerisinde yaşanan İran nükleer tesislerinin hedef alındığı Stuxnet saldırısı ile başlayan ve onun türevleri olduğu idda edilen, daha gelişmiş DuQU solucanı, Ortadoğu sistemleri hedef alınan Flame virüsü Gauss zaralı yazılımı siber savaşların şiddetinin zamanla daha da artacağını, kullanılan saldırı teknolojilerin daha da gelişmekte olduğunu göstermektedir. Bu bağlamda bu makale; İran'ı örnek göstererek siber terörizm bir ülkenin ulusal güvenliğini nasıl tehdit edip veya güvensiz hale getire bilmesini incelemektedir.

1 AKSU Muharrem, TURHAN Faruk, YENİ TEHDİTLER, GÜVENLİĞİN GENİŞLEME BOYUTLARI VE İNSANİ GÜVENLİK, Uluslararası Alanya İşletme Fakültesi Dergisi, Yıl:2012, C:4, S.69.

2 AKTEL M, GÜRKAYNAK M, KÜRESELLEŞEN TERÖRİZM: BİR ETKİLEŞİM ÇALIŞMASI. 38. ICANAS (Uluslararası Asya ve Kuzey Afrika Çalışmaları Kongresi), 10-15 Eylül 2007 - Ankara / Türkiye, Bildiriler: Uluslararası İlişkiler, 2011, C. 1,S.80.

Metodoloji: Bu makalenin metodolojisi tanımlayıcı- analitik olarak, siber terörizmin ulusal güvenliğe günümüzde en büyük tehditlerden birisi olmasını İran ülkesin örnek göstererek inceleyecek.

Siber Terörizm

Terör sözcügü Latince "terrere" sözcüğünden türemistir. Korku salmak, dehşete düşürmek, yıldırmak anlamına gelmektedir. Türkçemizde aynı anlamda Arapça kökenli "tedhis" sözcüğü de kullanılmaktadır. Ancak bu korkutma, yıldırma ve tedhis, yogunluk olarak oldukça büyük çaplı ve birey ya da bireylerin ruhsal yapılarını birden bire kaplayan korku durumunu ve şiddet halini ifade etmektedir. Bugünkü anlamıyla ise terör kelimesi ilk kez Fransa'da, Fransız Devriminden sonra kullanılmıstır. Devrimden sonra 1793 Mart'ından 1794 Temmuz'una kadar süren dönem "terör rejimi, terör dönemi" olarak adlandırılmıstır. Günümüzde çokça kullanılan bir terim olmasına rağmen terörün ortak kabul görmüş bir tanımı bulunmamaktadır. Konu ile ilgili birçok tanım yapılmış, ancak uluslar arası arenada ortak bir kavram üzerinde birleşlememiştir. Bunun nedeni de bir tarafın terörist ilan ettigini, diger tarafın özgürlük savasçısı olarak nitelemesidir[3]. Terör ve terörizm kavramsal olarak farklı bir anlam ve öneme sahiptir; şiddet terörizmin hem amacı hem de ön şartı olmakla beraber terörizmi tamamlayan şiddetin "siyasî amaçlı" olmasıdır. Genel anlamda şiddet, siyasî amaç taşımayan, buna karşılık yok etmeye kadar varan zarar verici saldırıların tümünü kapsamaktadır. Terör, hem şiddet yoluyla yaratılan korku ortamını, hem de bu ortamı yaratan şiddet eylemini ifade etmektedir. Terörizm ise, uzun süreli korku ve dehşet durumunu ifade eden terörden farklı olarak, siyasî amaçlar için örgütlü, sistemli ve sürekli terör kullanmayı yöntem olarak benimseyen bir strateji anlayışıdır[4].

Terörizm, uluslararası ve ulusal güvenlik ortamını ciddi derecede tehdit eden bir olgu olarak yoğun incelemelere konu olmaktadır. Terörizm konusunda uluslararası alanda halen ortak bir anlayışa bağlı olarak tek bir tanım geliştirilememiş olması önemli bir eksiklik olarak karşımıza çıkmaktadır. Doktrinsel tartışmada, terörizm" ile "yabancı işgaline karşı" ve "kendi kaderini tayin amaçlı meşru mücadele" arasında bir ayrıma gidilmesi hususunda mutabakat yoktur. Ülkelerin yaklaşımındaki farklılıklar tanımı zorlaştıran en önemli etkenlerin başında gelmektedir[5]. Bağımsız Devletler Topluluğu da terörizmi şöy-

3 KILIÇ Zafer, KÜRESELLEŞME İLE İVME KAZANAN ULUSLARARASI TERÖRİZM VE BUNA KARSI ALINAN TEDBİRLER, Süleyman demrel Üniversitesi/ Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi ISPARTA, 2007, S.4.

4 TAŞDEMİR Fatma, ULUSLARARASI TERÖRİZME KARŞI DEVLETLERİN KUVVETE BAŞVURMA YETKİSİ, Doktora tezi, Ankara, 2005, S. 25.

5 YAYLA Mehmet, SİBER SAVAŞ VE SİBER ORTAMDAKI KÖTÜ NİYETLİ HAREKETLERDEN FARKI , HFD, 4(2) 2014, S.194.

le tanımlamıştır: "Kamu güvenliğine zarar veren, otoriteler tarafından karar alınmasını etkilemek ya da halkı terörize etmek amacıyla işlenen ceza hukukuna göre cezalandırılan ve aşağıdaki şekillerde gerçekleşen hukuka aykırı fiiller:

- Gerçek ya da tüzel kişilere karşı şiddet veya şiddet tehdidi;

- Kişilerin hayatını tehlikeye atacak şekilde mülk ve diğer maddi nesneleri yok etme ve bunları yok etme tehdidinde bulunma;

- Mülkiyete ciddi zarar verme ve topluma zararlı neticelere yol açma;

- Bir devlet adamı veya kamu yetkilisine görevini sona erdirme amaclı veya ondan öc almaya yönelik tehditte bulunma;

- Bir yabancı devlet temsilcisine veya uluslararası örgütün uluslararası korunan personeline ve bunlann işyerleri veya araçlarına saldırma;

- Taraf devletlerin ulusal hukuklarında veya terörle mücadeleyi amaç edinmis evrensel olarak tanınan hukuki enstrümanlarda terör olarak nitelenen diğer eylemler[6].

Siber Terör

Siber terörizm, belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin bireylere ve mallara karşı bir hükümeti veya toplumu yıldırma, baskı altında tutma amacıyla kullanılmasıdır. Terör örgütleri internet ortamında propaganda ve eğitim, aberleşme, bilgi toplama ve sanal saldırı faaliyetleri gerçekleştirmektedir. Kısaca, terör eylemlerinin internet üzerinden yürütülmesi işlemidir. Siber terörizmi diğer internet yoluyla islenen suçlardan ayıran başlıca fark, suçun mağdurunun devlet olması ya da devlet dışındaki bir yapı olduğunda bile bu mağdurun siyasi bir sebeple mağdur durumunda kalmasıdır[7]. Günümüzde birçok bilgi sistemi ülkeler açısından kritik bilgiler barındırmaktadır. Bu kritik bilgilerin güvenlik zafiyetlerinden ötürü siber teröristler tarafından kötüye kullanılması durumunda ülkeler açısından felaketler meydana gelebilir. Siber teröristlerin kabiliyetleri ve ulusal bilgi sistemlerimizin korunmasızlığına bağlı olarak anayurt güvenliğini tehdit eden birçok saldırıyla karşılaşılabilir. Bir barajın kapaklarının istenmeyen bir zamanda açılması, askeri haberleşme sistemlerinin engellenmesi, kentin bütün trafik ışıklarını durdurulması, telefon santrallerinin kullanılamaz duruma getirilmesi, elektrik ve doğalgaz santrallerinin kullanılmaz hale getirilmesi, ulaşım

6 SARAÇLI Murat, ULUSLARARASI HUKUKTA TERÖRİZM, Gazi Üniversitesi Hukuk Fakültesi Dergisi C. XI, Sa.1-2, Y.2007.S.1061.

7 KEÇECİ ORÇUN, SİBER SUÇLAR VE SİBER TERÖRİZM, (https://www.academia.edu/2333087/Siber_Su%C3%A7lar_ve_Ter%C3%B6rizm).

ve su sistemlerini durdurulması, finans sektörünün çökertilmesi, acil yardım, polis, hastaneler ve itfaiyelere ait bilgi sistemlerinin çalışamaz duruma getirilmesi, anayurt güvenliğini tehdit eden bilgi sistemleri odaklı saldırılara örnek olarak gösterilebilir[8].

Federal Acil Durum Yönetim Ajansı (Federal Emergency Management Agency) siber terörizmi böyle tarif ediyor: bilgisayar, ağ ve gizili saklanmış bilgilere, yasa dışı tehdit ve saldırı olmasi, halki veya hukumet korkutarak veya zorlayarak kendi siyasal ya sosyal amaçlara ulaşmak[9]. Terör faaliyetlerinin siber uzay kullanılarak gerçekleştirilmesi siber terörizm olarak adlandırılmaktadır. Burada siber terör kavramı terör örgütlerinin siber alanı araç olarak kullanmaları söz konusudur[10]. Siber terör, bilgisayar ağlarını kullanarak kritik öneme sahip ulusal altyapılara (enerji, ulaşım ve devlet işlemleri) zarar vermeyi ya da tamamen kullanılamaz hale getirmeyi amaçlayan saldırılar biçiminde kendini göstermektedir. Siyasal bir amaç uğruna insanlara zarar vermek veya acı çektirmek için devlet tarafından iyi korunan alanlardaki (telekomünikasyon, ulusal güvenlik ağları vs) bilgileri elde etmek, değiştirmek veya terörist amaçlar için kullanmak siber terörün önemli hedefleri arasında yer almaktadır[11].

Uzman politik, ekonomik ve psikolojik birimler bir araya gelerek siber terörizm tehdidini araştırmaktadır. Psikolojik perspektife göre modern dönemlerin en buyuk iki korkusu "siber terörizm" adı altında birleşmiştir. Modern araçlardan ve alışkanlıklardan kaynaklanan mağduriyet korkusu, bilgisayar teknolojilerine olan güvensizlik ve endişe ile birleşerek siber terörizm korkusunu yaratmıştır. Bilinmeyen bir tehdidin bilinenden daha korkutucu olduğu açıktır. Buna rağmen siber terörizm doğrudan bir şiddet tehdidi sunmamaktadır; fakat tedirgin toplumlara yapacağı psikolojik darbe, terörist bir bombanın etkisi kadar zarar verici olabilir. Daha da ötesi siber saldırılara karşı mucadele çalışmaları, en büyük ve gerçek tehdidin bilinmezlikten, bilgi eksikliğinden ve daha da kötüsü yanlış bilgilerden kaynaklandığını ortaya çıkarmıştır. Siber

8 YILMAZ Vural, BAYINDIR Mustafa, TAMER Onur, ANAYURT GÜVENLİĞİNİN SAĞLANMASINDA BİLGİ SİSTEMLERİ GÜVENLİĞİNİN ÖNEMİ, Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri 11-13 Şubat 2009 Harran Üniversitesi, Şanlıurfa.S.809.

9 DHANASHREE Nagre & PRIYANKA Warade, "CYBER TERRORISM VULNERABILITIES AND POLICY ISSUES "FACTS BEHIND THE MYTH**",** 2008 (http://www.andrew.cmu.edu/user/dnagre/).S.8.

10 MİL Halil İbrahim, SOSYAL GÜVENLİK KURUMUNDAKİ SİBER GÜVENLİK YÖNETİMİ UYGULAMALARININ İNCELENMESİ VE DEĞERLENDİRİLMESİ, Dicle Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Nisan 2015 YIL-7 S.13,S.400.

11 GÜRKAYNAK Muharrem, İREN Adem Ali , REEL DÜNYADA SANAL AÇMAZ: SİBER ALANDA ULUSLARARASI İLİŞKİLER, Süleyman Demirel Üniversitesi, İktisadi ve İdari Bilimler, Fakültesi Dergisi, Y.2011, C.16, S.2, S.268.

terörizme odaklanmanın bir de politik boyutu vardı. Siber terörizm ile ilgili güvenlik tartişmaları her zaman için siyasi aktörlerin ilgisini cekmiş ve indirgemeci bir yaklaşımla değerlendirilmiştir. Bu açıdan bakıldığında siber terörizm zaman zaman küresel siyasetin ve "güç" unsurunun önemli bir parçası haline getirilmiştir[12]. Siber terör eylemlerini kimler ne için yaparlar;

- Devletler: Düşmanı zayıflatmak ve çökertmek, istihbarat ve sabotaj yapmak

- Politik örgütler: Ekonomik ve psikolojik çöküntü yaratmak, sosyal yapıyı ve düzeni yapmak, propaganda amaçlarıyla

- Kurum içi ve dışı düşmanlar: Haksız rekabet gücü sağlamak, sanayi casusluğu amaçlarıyla

- Kiralık saldırganlar ve suç örgütleri: Para ve güç amacıyla

- Kriminaller: Kendilerini ispatlamak amacıyla siber terör eylemlerini yaparlar[13].

Siber terörün hedefleri**;**

• Bir telekomünikasyon yönetimine yerleşmek
• Banka ve finans yönetimine yapılan müdahaleler
• Posta yönetim merkezine yapılan müdahaleler
• Enerji dağıtım merkezlerine yapılan müdahaleler
• Ulaşım sisteminin işleyişine yapılan müdahaleler
• Petrol üreten ve dağıtımına yapılan müdahaleler
• Su dağıtım sistemlerine ve sitelerine yapılan müdahaleler
• Medya
• Sosyal servislere yapılan müdahaleler
• Toplumun ve yaşamın sembolüne
• Kamu güvenliği, sağlığı ve acil servislere yapılan müdahaleler[14].

Ulusal Güvenlik

Güvenlik olgusu, insanoğlunun var oluşundan günümüze kadar sahip olmaya çalıştığı en temel değerlerden biridir. İlk insandan günümüze, güven-

12 http://www.tasam.org/files/pdf/raporlar/siber_teror__639c0ad9-f639-4c64-9220-3bbc07f81993.pdf

13 http://www.21yyte.org/tr/arastirma/terorizm-ve-terorizmle-mucadele/2011/09/23/6309/siber-teror-ve-siber-istihbarat

14 http://akademikperspektif.com/2014/03/01/terorizm-ve-siber-teror.

lik hep arzu edilen ve elde etmek adına mücadele verilen bir değer olmuştur. Toplumsal yaşam biçimi ve ihtiyaçları arasında öncelikli sıralarda güvenlik ihtiyacı yer almaktadır[15]. Her dilde bu anlamı içeren bir kavram olmasına karşın güvenlik kelimesinin uluslararası alanda kullanılan İngilizce karşılığı "security" kelimesidir. Latince "securus" kelimesinden türeyen kelime kaygıdan üzüntüden emin olma, emniyet hali gibi anlamlara gelmektedir. "Se" ve "cura" eklerinin bileşiminden oluşan kelimede "se" eki Latince'de "free from" yani bir şeyden emin olma ya da özgür olma anlamına gelir, "cura" ise "care" yani kaygı üzüntü anlamına gelmektedir. Yine Latince "securitas" ya da "securus"-den türetilen "security" kelimesinin yazında kullanımına 1432 tarihinden itibaren rastlamak mümkündür[16].

Dünyaya gelen her canlının öncelikli amacı varlığını korumak ve sürdürmektir. Bir canlı olarak insanlar için geçerli olan bu durum insanlardan meydana gelen devletler için de geçerlidir. Varlığını korumak ve sürdürmek güvenlik kavramının da özünü oluşturmaktadır. Günlük hayatta ifadelerimizde sıklıkla yer bulan ve uluslararası ilişkilerde de yaygın bir kullanım alanı olan güvenlik kavramının bu yaygın kullanımına karşılık, üzerinde uzlaşılan bir tanımı yapılabilmiş değildir. Kavramın tanımına yönelik yapılan açıklamalar muğlaktır ve bu muğlaklığın temel nedeni de söz konusu alanda yapılan çalışmaların yetersizliği değil, aksine güvenliğin türetilmiş bir kavram olmasından kaynaklanmaktadır. Söz konusu üretilme, kişilerin ve toplumların kendi siyasi ve ideolojik düşüncelerinin bir ürünüdür[17]. Avrupa Birliği Standardizasyon Komitesi 2005 yılında güvenliğin tanımon şu şekilde kabul etmiştir: ''Güvenlik, bir kişi, toplum, örgüt, sosyal kuruluş, devlet ve onların vasıtalarını (eşyalar, altyapı vb.); suç faaliyetleri, terörizm ve diğer saldırı veya düşmanca hareketler, afetler (doğal veya insan terefınden) gibi tehlike veya tehditlere karşı korunulasının gerekli olduğu sanılan veya teyit edilen durumdur''[18].

Güvenlik, tek fertten devlete kadar bütün toplumu ilgilendiren bir olgudur. Var olma ile ilgili olduğundan konu doğrudan çıkarlarla ilgili alana işaret etmektedir. Bu durumda, her türlü menfaatin güvenlik çemberi içerisine sokulabileceği veya çıkartılabileceği söylenebilir. Ancak var olmaya yönelik risk ve

15 ATEŞ Hasan, KAMU GÜVENLİĞİNDE İSTİHBARAT SİSTEMİNİN DEĞERLENDİRİLMESİ, Atilim Üniversitesi/Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, 2012, Ankara, S.14.

16 BİRDİŞLİ Fikret, ULUSAL GÜVENLİK KAVRAMININ TARİHSEL VE DÜŞÜNSEL TEMELLERİ, Sosyal Bilimler Enstitüsü Dergisi Sayı: 31, Yıl:2011, S.150.

17 SANCAK Kadir, GÜVENLİK KAVRAMI ETRAFINDAKİ TARTIŞMALAR VE ULUSLARARASI GÜVENLİĞİN DÖNÜŞÜMÜ, KTÜ/ Sosyal Bilimler Enstitüsü DergisiSayı: 6 – 2013, S.124.

18 YILMAZ Sait, GÜÇ VE POLİTİKA, Alfa Yayınları, 1.Basım: Mayıs 2008.S.96.

sel" bir kavram değildir. Ulusal güvenlik sosyal bilimler alanında uzun süre üzerinde çalışılarak geliştirilmiş ve yerleşmiş bir kavram ya da zamanaşımı, sözleşme, tazminat gibi teknik anlamda hukukî bir kavram da değildir. Ulusal güvenliğin "siyasî-hukukî" bir kavram olduğu düşünülebilir. Kavramın siyasî niteliği genel olarak açık bir tanımının yapılmamış (veya yapılamamış) olmasından ve kapsamının bir ülkenin siyasî koşullarına bağlı olarak değişmesinden ileri gelmektedir. Kavramın hukukî yönü ise uluslararası sözleşmelerde, anayasalarda ve kanunlarda yer almasından ortaya çıkmaktadır[23].

Devletin zaralı tehdidlerden uzak kalma özgürlüğü tanımlanabilecek olan ulusal güvenlik kavramı, bir devletin fiziki güvenliği, toprak bütünlüğü, milli egemenliği ile politik, ekonomik ve sosyal istikrarı gibi öğelere işaret etmektedir. Ulusal güvenlik kavramı ayrıca milli değerlerin, sosyal ilişki kalıplarının ve yaşam biçimlerin korunması ve sürdürülmesini öngörür[24]. Ulusal güvenlik polilitikasının üç temel unsuru bulunmaktadır; ulusal güvenliğini sağlanması, ulusal hedeflere ulaşılması ve bu iki unsur için; iç, dış ve savunma hareket tarzlarına ait esasların (politika esasları) tesbit edilmesidir[25]. Diğer bir tarife göre ulusal güvenlik; ülkenin fiziki bütünlüğünün muhafaza ve korunmasıyla birlikte, yabancı ülkelerle olan ekonomik, siyasi ve diğer münasebetlerin makul ölçüler içinde devam ettirilmesi, yönetimin, kurumların iç ve dış olumsuz etkilere karşı korunması ve sınırların kontrol altında bulundurulmasıdır[26].

Güvenlik algılamalarında meydana gelen değişimin en önemli sebeplerinden birisi, artık tehdidin tek boyutlu, devletten devlete olma klasik konumundan çıkarak, asimetrik ve çok boyutlu bir konuma ulaşmasıdır. Bu durum, günümüz tehditleri ile mücadelede geleneksel yapılanma ve anlayışların geçerliliğini tamamen yitirdiğine işaret etmektedir. Bunun yanında risk ve tehditlerin kaynağının, zamanının ve şeklinin önceden tahmin edilmesinin Soğuk Savaş döneminin aksine imkansız bir hale geldiği yeni güvenlik ortamında, mücadele alanı bütün dünya olarak ortaya çıkmıştır[27]. Yeni dönemde güvenlik gündemi, askeri ve siyasi gündemden ibaret olan geleneksel güvenlik yaklaşımından daha geniş bir alanı kapsamaktadır. Fakat, güvenlik gündeminin

23 HAZAR Zeynep, BASIN ÖZGÜRLÜĞÜ VE ULUSAL GÜVENLİK, Gazi Üniversitesi Hukuk Fakültesi Dergisi C. XVII, Y. 2013, Sa. 1-2, S.1530.

24 KARABULUT Bilal, GÜVENLİK, ULUSLARARASI İLİŞKİLERDE ANAHTAR KAVRAMLAR SERİSİ: II, BARIŞ KİTABEVİ, 2. Bskı, 2015 ANKARA.S.22.

25 YILMAZ Sait, GÜÇ VE POLİTİKA, Alfa Yayınları, 1.Basım: Mayıs 2008.S.99.

26 ÇALIK Zuhal, YENİ GÜVENLİK KAVRAMI, ULUSLARARASI GÜVENLIK KONGRESI, Bildiriler Kitabı, Nisan 2014, Kocaeli , S.639.

27 ŞÖHRET Mesut, KOPENHAG VE ABERYSTWYTH EKOLLERİ ÇERÇEVESİNDE 21. YÜZYILDA GÜVENLİĞİN DEĞİŞEN KAPSAMI VE BOYUTU, Uluslararası Güvenlik Kongresi, Bildiriler Kitabı, Nisan 2014, Kocaeli, S.662.

genişlemesi basit ve önemsiz veya politik sonuçları olmayan bir gelişme değildir. Nitekim Buzan ve Waever'in ortaya koydukları yeni güvenlik yaklaşımı geleneksel güvenlik anlayışını dışlamamaktadır. Bununla birlikte geleneksel güvenlik anlayışı ile yeni güvenlik yaklaşımı arasında önemli fark vardır. Genişletilmiş güvenlik yaklaşımı katı iç ve dış system farkını esas almamaktadır, çünkü sorunların çoğu devlete göre tanımlanmamaktadır, geleneksel güvenlik yaklaşımının gündemi dardır (monosectoral), oysa, yeni güvenlik yaklaşımı geniş bir alanı içine almaktadır, yani çok-sektöreldir (multisectoral). Yeni yaklaşım, sektörler arasındaki denge, tehdit, aktörler, değerli referent object ve farklı dönemlerde bunlardan hangisinin ağır bastığına dikkat etmektedir. Oysa geleneksel güvenlik yaklaşımında yalnız tek bir sektörün (askeri) ve tek aktörün (devlet) kesintisiz bir şekilde üstünlüğü sözkonusudur[28].

İran

İslam Devrimi zaferi ile ve İran İslam Cumhuriyeti kurulmasıyla beraber güvenlik konularında ciddi değişiklikler oldmuş. Geçmişten tamamen farklı olarak yeni sistem insan, devlet ve uluslararası sistemi farklı tanımlamıştır. İran İslam Cumhuriyeti ulusal güvenliğinde beş boyut vardır Askeri, ekonomik, siyasi, sosyal ve çevresel buyut.

1. Askeri güvenliği:

İran İslam Cumhuriyeti güvenliliğini, maddi ve manevi değerlere dış ve iç askeri tehditler olmaksızın ve korku hissetmeksizin tanımlayabilirz. Bu değerler, milli egemenlik, istiklal, toprak bütünlüğü, halk sağlık ve güvenliliği, siyasi sistemin hayatta kalması, ekonomi ve kültürel-dini, refah ve halkın geçimini içerir. Bu değerler karşı askeri tehditler görsel veya zihinsel olabilir. Ayrıca askeri güvenliliği sağlamak için en uygun mekanizma, askeri eylem ve saldırılara yanıt verecek verimli ve yeterli askeri kuvvetlere ve güce sahip olmaktır[29].

2. Ekonomik Güvenlik:

Ekonomik gücün bağımsız fonksiyon ve araç niteliğine ve yapısal ve aracılık tehditlerine göre İran İslam Cumhuriyeti ekonomik güvenliliği şu şekilde açıklayabilirz; İslam Cumhuriyeti ekonomik güvenliliği, toplumun ve halkın hayat gereksinimlerini temin etme, ekonomik refah ve geçim, endüstriyel kalkınma, organizatör usulleri koruyarak ekonomik ve ticari teknoloji gelişimi ve

28 ZHYLKYSHYBAYEVA Meruyert, BÖLGESEL GÜÇ DENGESİ IŞIĞINDA KAZAKİSTAN'IN GÜVENLİĞİ, ANKARA ÜNİVERSİTESİ/ SOSYAL BLİMLİER ENSTİTÜSÜ, doktora Tezi, 2008 ANKARA.S.48.

29 DEHGHANI Seyed Jalal, , CONCEPTUAL FRAMEWORK FOR EVALUATING THE FOREIGN POLICY OF THE ISLAMIC REPUBLIC OF IRAN, Center for Strategic Research, 2008, *(In Persian)*.S.87-88.

ulusal ekonomi yapısı ve kaynaklara serbest erişim, sermaye ve küresel pazar ve ekonomi birimleri ve yapısal tehditlere karşı güvenlilik açığı olmayan bir tanımdır[30].

3. Sosyal güvenlilik:

İran İslam Cumhuriyeti sosyal güvenliliği şöyle tanımlanabilir, İran halkının değişken şartlar altında ve potansiyel ve gerçek tehditler yanısıra ulusal doğa ve kimliklerini koruma ve sürdürme yeteneği.daha doğrusu İran İslam Cumhuriyeti sosyal güvenliliği; dilin geleneksel desen stabilitesi ve Sürekliliği, kültür, gelenek ve adetler, inançlar, sünnetler, geleneksel yaşam tarzı istikrarı ve İran halkının milli ve dini kimliğinin korunma ve hayatta kalması, makbul bütün şartlar altına evrim ve sosyal gelişim için[31].

4. Çevre güvenlik:

İran ulusal güvenliğinin bir başka boyutu ise, çevre güvenliliğidir. Ama diğer üçüncü dünya ülkeleri gibi güvenliliğin bu boyutu pek önemsenmiyor, Bununla birlikte İran İslam Cumhuriyeti'nin çevre güvenliliği aşağıdaki gibi tanımlanabilir: hükümetin iç ve dış çevresi, İran medeniyeti ve halkının doğal yaşam yerlerinin Doğal ve beşeri tehditler karşısında güvenliliği, sürekliliği, istikrar ve hayatta kalması[32].

5. Siyasi Güvenlik:

İran İslam Cumhuriyeti Ulusal Siyasi Güvenliliği, ülkenin örgütsel ve yapısal kararlılığı, hükümet sistemi, devlet ve hükümet sistemini meşrulaştırıcı ideolojiden ibarettir. Bu yüzden siyasi güvenlilik farklı katmanlar ve boyutlardan oluşmaktadır. Bu boyutların bazısı ulusal düzeyde devlet ve millet arasındaki ilişkileri denetlemektedir[33].

İran'ın Siber Güvenliği

İran'ın siber güvenliği askeri boyutu olarak ülke güvenliğinde önemli yere sahipdir. İran'ın İletişim bakanığı bu saldırıların sayısın on dört bin olbuğu söyledi. Bu saldırılardan bazileri:

30 ABOLFATHI Mohammad, NOORI Mukhtar, REVOLUTION MOVEMENTS IN MIDDLE EAST AND THE NATIONAL SECURITY OF IRAN, Studies of Islamic Awakening in the Second Year Spring and Summer 1392 (3), (In Persian).S.14.

31 DEHGHANI Seyed Jalal, , CONCEPTUAL FRAMEWORK FOR EVALUATING THE FOREIGN POLICY OF THE ISLAMIC REPUBLIC OF IRAN, Center for Strategic Research, 2008, *(In Persian)*.S.95-96.

32 İbid.S109.

33 ABOLFATHI Mohammad, NOORI Mukhtar, REVOLUTION MOVEMENTS IN MIDDLE EAST AND THE NATIONAL SECURITY OF IRAN, Studies of Islamic Awakening in the Second Year Spring and Summer 1392 (3), (In Persian).S.15.

1. STUXNET ve Sanat bölümüne saldırısı:

Özellikle SCADA (Supervisory Control and Data Acquisition) sistemlerine saldırmak üzere yazılmış, bilinen ilk ve en karmaşık yazılımdır. 2010 yılının Haziran ayında Beyaz Rusya'daki küçük bir firma olan Virüs BlokAda tarafından tespit edilmiştir. İncelemeler sonunda yazılımın karışık yapısı, basit bir solucan olmadığını göstermiştir. Farklı alanlarda uzmanların uzun zaman ve büyük bir bütçe harcayarak gerçekleştirilebileceği bir yazılım olduğu anlaşılmıştır. Bu yazılımın en korkutucu tarafı ise Windows tabanlı bilgisayarlardan endüstriyel takım donanımlarının kontrolünde kullanılan özel bir sisteme atlamaya yönelik tasarlanmış olmasıdır. Hedefi kritik alt yapılardır. 2010 Kasım ayında İran'ın yüksek düzeyde güvenlikle korunan nükleer yakıt tesisinde tespit edilen virüs çok sayıda santrefüjün arızalanmasına sebep olmuştur. İran'ın uranyum zenginleştirme programına vurduğu darbe ile stuxnet asıl hedefinin ne olduğunu ortaya koymuştur. İran nükleer tesisinden içeri girmeyi başaran stuxnet virüsü, yavaş ve emin adımlarla zarar vermeye başlamıştır[34].

2. Flame:

Stuxnet virüsünden 20 kat daha karmaşık bir kodla yazılan ve özellikle Ortadoğu'yu hedef alan Flame virüsü very sızdırma amacı taşımaktadır. Flame'de diğer virüsler gibi uzunca bir sure keşfedilememiştir. Flame virüsü 43 farklı antivirüs tarafından tanımlanmadı ve bu sebep Flame virüsün daha fazla yaşamasına izin verdi. İran, Flame'in tespit edildiği ülkeler içerisinde en çok etkilenen alan olarak görülmektedir. İran'dan sonra Filistin, Macaristan, Lübnan, Avustralya, Suriye, Rusya, Hong Kong ve Birleşik Arap virüsten etkilenen bölgeler arasındadır[35]. Buna karşılık, İran, bir devlet kurumunun "Flame" yok etmek kötü amaçlı yazılım aracı geliştirdi iddia etti. Merkezi, bir "uzman" olarak bilinir ekler: "Mevcut fazla 43 antivirüs yazılımı tarafından kötü amaçlı yazılım bileşenlerinin Şimdi hiçbiri kabul edilmeyecektir[36].

3. Gauss ve bankacılık sistemi:

Siber güvenlik firması Kaspersky Lab yeni keşfettiği Gauss isimli virüsün, daha önce İran'ın nükleer programına saldırarak gündeme gelen Stuxnet ile aynı elden çıktığını açıkladı. Gauss, sosyal medya hesapları, emailler gibi kişisel veriler dışında, banka hesaplarına ait bilgileri de ele geçirmeyi hedefliyor. Bu nedenle Gauss daha önceki benzerleri olan Flame ve Stuxnet'ten

34 KARA Mahruze, SİBER SALDIRILAR - SİBER SAVAŞLAR VE ETKİLERİ, İSTANBUL BİLGİ ÜNİVERSİTESİ SOSYAL BİLİMLER ENSTİTÜSÜ, YÜKSEK LİSANS PROGRAMI, 2013, S.34.

35 http://www.momtaznews.com-

36 http://fa.rfi.fr/%D8%A7

ayrılıyor çünkü onlar sadece sanayi casusluğu odaklı hazırlanmış virüslerdi. Lübnan, Filistin ve İsrail olmak üzere ortadoğu'daki yaklaşık 2500 kullanıcıyı etkilediği düşünülmwktidir[37]. Bu saldırılar İran'ın ulusal güvenliğine tehdit olmuş ve bu saldırılara karşı İran askeri buyutda karşi tavır almaya başlamış.

İran'ın dini lideri: düşmanın saldirisina hemen düzeyde saldırmak bizim siber ulusal güvenlik stratejimiz olmalıdı[38]. İran'ın da siber harp dünyasına gelişen ve iddialı bir aktör olarak girdiği söylenebilir. Diğer birçok otoriter rejim gibi, İran'ın siber adımlarının ilk olarak iç güvenlik odaklı başladığı görülmektedir. Daha sonra, Stuxnet'in etkisiyle siber teknolojinin yıkıcı sonuçlarını gören rejim, Dini Lider Ayetullah Ali Hamaney'in onayı ile 2011 yılında Yüksek Siber-uzay Konseyi'ni kurmuştur. Söz konusu birim, hem müdafi hem de taarruzi siber yeteneklerin yönetiminden sorumludur. Konsey, çeşitli istihbarat ve güvenlik kurumları ile kültür ve haberleşme bakanlıklarını da çalışmalarına dahil etmektedir. İran siber güvenlik mekanizmasında Devrim Muhafızları'nın da önemli bir rol oynadığı görülmektedir. Ayrıca, İran 2012 yılında ilk siber tatbikatını icra etmiştir ve Ruhani'nin devlet başkanlığına gelmesi ile siber operasyonlar bütçesini 20 milyon dolar artmıştır[39].

İran bir milyard dolardan fazla siber ve sibere bağlı teknoloji para harc ederek 100 bin uzman eğitmiş. İran yetkilileri biliyorlar siber bilimi askeri savavaşla bir araya gelerek birleşmişler. İran'ın bazi komşulari gelişmiş askeri savaş vitesi alarak İran'a büyük bir tehdid ola bilirler, bunun üzünden İran siber bilimimnde çok iyi olması gerekiyor. Muhafizkar devriçi Kara Kuvvetleri Komutan Yardımcısı Abdullh IRAKİ Daha önce söylemişti siber savaşlar klasik savaşlardan çok tehlikeli ola bilir. İran yetkilileri yakın zamanda siber konusunda dünyada dördüncu güç olmaya çalışıyorlar[40]. Defense tech enstitüsü ABD'nin Merkezi İstihbarat Teşkilatı (Central Intelligence Agency) aldığı istatistiklere göre İran siber güçde dünyada 5. sırada yer alıyor ve İran'ın siber kuvvetlerinde 2400 kişi çalışmaktadır ve 12 bin kişidende fazla yedek kuvvet olarak hazır sakalnmaktadır. Defense tech enstitüsü bu kuvvetin buçesin 76 milyon dolar olarak Muhafızakar Devrimçilere bağlı olduğunu yazıyor[41]. Amerika'nın İstihbaratının yeni tahminlere göre İran'ın siber gücünün iki yönü

37 http://www.kigem.com/banka-hesaplarimiz-tehlikede-mit.html

38 HALEDI Mohammad, İRAN'IN SİBER ULUSAL GÜVENLİK STRATEJİSİ NEREDE (http://nahad.ir/index.jsp?siteid=51&pageid=2835&newsview=139788).

39 SINAN Ülgen, TÜRKİYE'DE SİBER GÜVENLİK VE NÜKLEER ENERJİ, 1. Baskı, İstanbul, Şubat 2016.S.8.

40 http://www.afkarnews.ir.

41 PEYMANFER Semira, İRAN'IN SİBER YETENEKLERİNE KISABAKIŞ, (http://nahad.ir/index.jsp?siteid=51&pageid=21028&newsview=128226).

vardır. biri Tahran'ın saldırılar karşı siber güçüne Itiraf da bulunmak ve diğer yönü siber saldırının karşi tarafa önemli olmak. Savaş kı birinin Burun kanamıyor ama sonuç olarak on kere geleneksel savaşlardan çok insan ölmeğe yol açıyor[42].

İran, yaptığı nükleer çalışmalar neticesinde stuxnet gibi güçlü bir siber saldırıya maruz kalmıştır. Saldırı neticesinde nükleer çalışmalarına darbe vurulmuştur. Siber güvenlik stratejisi konusunda geniş bilgi vermemektedir. Siber güç konusunda ABD, Rusya ve Çin'den sonra İran'ın dördüncü büyük güç olduğu düşünülmektedir. Silahlı kuvvetler, savunma sanayisi ve üniversitelerden oluşan üçlü işbirliği ile güçlü bir mekanizma şekillenmiştir. Siber savunma ve gerektiğinde siber saldırı yeteneğini geliştirmiştir. İran Savunma Bakanı, ABD'nin siber terörün başında bulunduğunu, çeşitli suçlamalarla siber terörün arttırılması için ortam sağladığını belirtmiştir. İran gençlerinin dahi bilgisine güvenen İran Savunma Bakanı, İran'ın dahi bilgisinin siber alanda alt edilemeyeceğini belirtmiştir. Siber savunma organizasyonu, ordu tarafından koordine edilmektedir. Askeri siber savunma takımları siber saldırıları önlemek amacıyla sürekli bilgisayar ağlarını kontrol ederek, saldırı söz konusu olduğunda anında savunmaya geçmektedir. Genellikle saldırılara maruz kalan İran'ın, siber saldırılarda, bilgisayarlardaki bilgilerinin hacklenmesi amaçlanmıştır. İran, stuxnet virüsünden sonra savunma sistemini geliştirmeye yönlenmiştir. İran, Velayet tatbikatları adı altında deniz ve hava kuvvetlerinin askeri gücünü tatbik etmektedir[43].

Sonuç

Dünyaya gelen her canlının öncelikli amacı varlığını korumak ve sürdürmektir. Bir canlı olarak insanlar için geçerli olan bu durum insanlardan meydana gelen devletler için de geçerlidir. Varlığını korumak ve sürdürmek güvenlik kavramının da özünü oluşturmaktadır. Ama teknolojik gelişim, iletişim ve ulaşım imkanlarının gelişmesi günümüz dünyasında yeni tehditlerin ortaya çıkmasına, var olan tehditlerin şekil değiştirmesine ya da daha etkili hale gelmesine neden olmaktadır. Güvenlik algılamalarında meydana gelen değişimin en önemli sebeplerinden birisi, artık tehdidin tek boyutlu, devletten devlete olma klasik konumundan çıkarak, asimetrik ve çok boyutlu bir konuma ulaşmasıdır. Terörizm, uluslararası ve ulusal güvenlik ortamını ciddi derecede tehdit eden bir olgu olarak yoğun incelemelere konu olmaktadır. Terör

42 TAGADOSI Ihsan, İRAN'IN SİBER GÜÇE NEKADER SAHİP? (http://nahad.ir/index.jsp?siteid=51&pageid=2836&newsview=118018).

43 KARA Mahruze, SİBER SALDIRILAR - SİBER SAVAŞLAR VE ETKİLERİ, İSTANBUL BİLGİ ÜNİVERSİTESİSOSYAL BİLİMLER ENSTİTÜSÜ, YÜKSEK LİSANS PROGRAMI, 2013, İSTANBUL.S.68.

örgütleri internet ortamında propaganda ve eğitim, aberleşme, bilgi toplama ve sanal saldırı faaliyetleri gerçekleştirmektedir. Kısaca, terör eylemlerinin internet üzerinden yürütülmesi işlemidir. Siber terörizmi diğer internet yoluyla islenen suçlardan ayıran başlıca fark, suçun mağdurunun devlet olması ya da devlet dışındaki bir yapı olduğunda bile bu mağdurun siyasi bir sebeple mağdur durumunda kalmasıdır.

İran'da siber terörizmiden etkilenmiş ve farkılı türlerde siber terörizme urayımış bir ülkedir. İran'ın uranyum zenginleştirme programına vurduğu darbe ile stuxnet asıl hedefinin ne olduğunu ortaya koymuştur. İran nükleer tesisinden içeri girmeyi başaran stuxnet virüsü, yavaş ve emin adımlarla zarar vermeye başlamıştır. Stuxnet virüsünden 20 kat daha karmaşık bir kodla yazılan ve özellikle Orta Doğu'yu hedef alan Flame virüsü veri sızdırma amacı taşımaktadır.. İran, Flame'in tespit edildiği ülkeler içerisinde en çok etkilenen alan olarak görülmektedir. Bu durumlardan sonra İran'ın da siber harp dünyasına gelişen ve iddialı bir actor olarak girdiği söylenebilir. Diğer Stuxnet'in etkisiyle siber teknolojinin yıkıcı sonuçlarını gören İran yetkilileri, Dini Lider Ayetullah Ali Hamaney'in onayı ile 2011 yılında Yüksek Siber-uzay Konseyi'ni kurmuştur. Konsey, çeşitli istihbarat ve güvenlik kurumları ile kültür ve haberleşme bakanlıklarını da çalışmalarına dahil etmektedir. İran siber güvenlik mekanizmasında Devrim Muhafızları'nın da önemli bir rol oynadığı görülmektedir. Ayrıca, İran bir milyard dolardan fazla siber ve sibere bağlı teknoloji para harc ederek 100 bin uzman eğitmiş. İran yetkilileri biliyorlar siber bilimi askeri savavaşla bir araya gelerek birleşmişler. İran'ın bazi komşulari gelişmiş askeri savaş vitesi alarak İrana büyük bir tehdid ola bilirler, bunun üzünden İran siber bilimimnde çok iyi olması gerekiyor. Silahlı kuvvetler, savunma sanayisi ve üniversitelerden oluşan üçlü işbirliği ile güçlü bir mekanizma şekillenmiştir.

KAYNAKÇA

1. ABOLFATHI Mohammad, NOORI Mukhtar***, REVOLUTION MOVEMENTS IN MIDDLE EAST AND THE NATIONAL SECURITY OF IRAN***, Studies of Islamic Awakening in the Second Year Spring and Summer 1392 (3), (In Persian).

2. AKSU Muharrem, TURHAN Faruk, ***YENİ TEHDİTLER, GÜVENLİĞİN GENİŞLEME BOYUTLARI VE İNSANİ GÜVENLİK***, Uluslararası Alanya İşletme Fakültesi Dergisi, Yıl:2012, C:4, S:2, s. 69-80.

3. AKTEL, M., GÜRKAYNAK, M., 2011***. KÜRESELLEŞEN TERÖRIZM: BİR ETKİLEŞİM ÇALIŞMASI.*** 38. ICANAS (Uluslararası Asya ve Kuzey Afrika Çalışmaları Kongresi), 10-15 Eylül 2007 - Ankara / Türkiye, Bildiriler: Uluslararası İlişkiler, C. 1, 77-87.

4. TEŞ Hasan, KAMU GÜVENLİĞİNDE ***İSTİHBARAT SİSTEMİNİN DEĞERLENDİRİLMESİ***, ATILIM ÜNİVERSİTESİ/SOSYAL BİLİMLER ENSTİTÜSÜ, YÜKSEK LİSANS TEZİ, 2012, Ankara.

5. BİRDİŞLİ Fikret, ***ULUSAL GÜVENLİK KAVRAMININ TARİHSEL VE DÜŞÜNSEL TMELLERİ***, Sosyal Bilimler Enstitüsü Dergisi Sayı: 31 Yıl:2011/2 s.149-169.

6. Çalık Zuhal, ***YENİ GÜVENLİK KAVRAMI***, Uluslararası Güvenlik Kongresi, Bildiriler Kitabı, Nisan 2014, Kocaeli, S.638-647.

7. DEHGHANI Seyed Jalal, , ***CONCEPTUAL FRAMEWORK FOR EVALUATING THE FOREIGN POLICY OF THE ISLAMIC REPUBLIC OF IRAN***, Center for Strategic Research, 2008.(In Persian).

8. GÜN Çağlar, ***ULUSAL GÜVENLIK POLİTİKALARININ BELİRLENMESİNDE İSTİHBARATIN ROLÜ VE ÖNEMİ***, YÜKSEK LİSANS TEZİ, KARA HARP OKULU, SAVUNMA BİLİMLERİ ENSTİTÜSÜ, 2014– ANKARA.

9. GÜRKAYNAK Muharrem, İREN Adem Ali , ***REEL DÜNYADA SANAL AÇMAZ: SİBER ALANDA ULUSLARARASI İLİŞKİLER***, Süleyman Demirel Üniversitesi, İktisadi ve İdari Bilimler, Fakültesi Dergisi, Y.2011, C.16, S.2, s.263-279.

10. HALEDI Mohammad, ***İRAN'IN SİBER ULUSAL GÜVENLİK STRATEJİSİ NEREDE*** (http://nahad.ir/index.jsp?siteid=51&pageid=2835&newsview=139788).

11. HAZAR Zeynep, ***BASIN ÖZGÜRLÜĞÜ ve ULUSAL GÜVENLİK***, Gazi Üniversitesi Hukuk Fakültesi Dergisi C. XVII, Y. 2013, Sa. 1-2,S.1530.

12. KARA Mahruze, ***SİBER SALDIRILAR - SİBER SAVAŞLAR VE ETKİ-***

LERİ, İSTANBUL BİLGİ ÜNİVERSİTESİSOSYAL BİLİMLER ENSTİTÜSÜ, YÜKSEK LİSANS PROGRAMI, 2013, İSTANBUL.

13. KARABULUT Bilal, ***GÜVENLİK, ULUSLARARASI İLİŞKİLERDE ANAHTAR KAVRAMLAR SERİSİ***: II, BARIŞ KİTABEVİ, 2. Bskı, 2015 ANKARA.
14. KEÇECİ ORÇUN, ***SİBER SUÇLAR VE SİBER TERÖRİZM***, (https://www.academia.edu/2333087/Siber_Su%C3%A7lar_ve_Ter%C3%B6rizm).
15. KILIÇ ZAFER, ***KÜRESELLEŞME İLE İVME KAZANAN ULUSLARARASI TERÖRİZM VE BUNA KARSI ALINAN TEDBİRLER***, YÜKSEK LİSANS TEZİ SÜLEYMAN DEMREL ÜNİVERSİTESİ/ SOSYAL BİLİMLER ENSTİTÜSÜ, ISPARTA, 2007.
16. KÜÇÜKŞAHİN Ahmet, UYAR E Önder, TAHMİNCİLER Erçin, DİNÇER Duygu ***TÜRKİYE'NİN GÜVENLİK STRATEJİ BELGESİ NASIL HAZIRLANMALIDIR?,*** STRATEJİK ARAŞTIRMALAR ENSTİTÜSÜ/ GÜVENLİK STRATEJİLERİ DERGİSİ, Yıl 4 Sayı 7 Haziran 2008, s.7-39.
17. MİL Halil İbrahim, ***SOSYAL GÜVENLİK KURUMUNDAKİ SİBER GÜVENLİK YÖNETİMİ UYGULAMALARININ İNCELENMESİ VE DEĞERLENDİRİLMESİ***, Dicle Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Nisan 2015 YIL-7 S.13,S.398-417.
18. Nagre, Dhanashree& Warade, Priyanka; "***CYBER TERRORISM VULNERABILITIES AND POLICY ISSUES "FACTS BEHIND THE MYTH",*** (2008), (http://www.andrew.cmu.edu/user/dnagre/).
19. PEYMANFER Semira, ***İRAN'IN SİBER YETENEKLERİNE KISA BAKIŞ***, (http://nahad.ir/index.jsp?siteid=51&pageid=21028&newsview=128226).
20. SANCAK Kadir, ***GÜVENLİK KAVRAMI ETRAFINDAKİ TARTIŞMALAR VE ULUSLARARASI GÜVENLİĞİN DÖNÜŞÜMÜ***, KTÜ/ Sosyal Bilimler Enstitüsü DergisiSayı: 6 – 2013, S.123-135.
21. SARAÇLI Murat, ***ULUSLARARASI HUKUKTA TERÖRİZM***, Gazi Üniversitesi Hukuk Fakültesi Dergisi C. XI, Sa.1-2, Y.2007.
22. Şöhret Mesut, ***KOPENHAG VE ABERYSTWYTH EKOLLERİ ÇERÇEVESİNDE 21. YÜZYILDA GÜVENLİĞİN DEĞİŞEN KAPSAMI VE BOYUTU***, Uluslararası Güvenlik Kongresi, Bildiriler Kitabı, Nisan 2014, Kocaeli, S.657-713.
23. TAGADOSI Ihsan, ***İRAN'IN SİBER GÜÇE NEKADER SAHİP?*** (http://nahad.ir/index.jsp?siteid=51&pageid=2836&newsview=118018).

24. TAŞDEMİR, Fatma, ***ULUSLARARASI TERÖRİZME KARŞI DEVLETLERİN ÜLKELERİ DIŞINDA MÜNFERİDEN KUVVETE BAŞVURMA YETKİSİ***, Doktora tezi, 2005, Ankara.

25. Ülgen Sinan , ***TÜRKİYE'DE SİBER GÜVENLİK VE NÜKLEER ENERJİ***, 1. Baskı, İstanbul, Şubat 2016.

26. YAYLA Mehmet, ***SİBER SAVAŞ VE SİBER ORTAMDAKI KÖTÜ NİYETLİ HAREKETLERDEN FARKI***, Hacettepe HFD, 4(2) 2014, S.181–200.

27. YILMAZ Sait, ***GÜÇ VE POLİTİKA***, Alfa Yayınları, 1.Basım: Mayıs 2008.

28. YILMAZ Vural, Bayındır Mustafa, Tamer Onur, ***ANAYURT GÜVENLİĞİNİN SAĞLANMASINDA BİLGİ SİSTEMLERİ GÜVENLİĞİNİN ÖNEMİ***, Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri 11-13 Şubat 2009 Harran Üniversitesi, Şanlıurfa.

29. ZHYLKYSHYBAYEVA MERUYERT, ***BÖLGESEL GÜÇ DENGESİ IŞIĞINDA KAZAKİSTAN'IN GÜVENLİĞİ***, Ankara Üniversitesi/ Sosyal Blimlier Enstitüsü Uluslararasi İlşkiler Anablmdali, doktora Tezi, 2008 ANKARA.

30. http://***akademikperspektif.com***/2014/03/01/terorizm-ve-siber-teror/.

31. http://***nahad.ir***/index.jsp?siteid=51&pageid=21028&newsview=128226

32. http://***tabnak.ir***/fa/news/530399/%D8%A2%D9%85%D8%A7%D8%B1

33. http://***www.21yyte.org***/tr/arastirma/terorizm-ve-terorizmle-mucadele/2011/09/23/6309/siber-teror-ve-siber-istihbarat

34. http://***www.afkarnews.ir***/%D8%A8%D8%AE%D8%B4

35. http://***www.kigem.com***/banka-hesaplarimiz-tehlikede-mit.html

36. http://***www.momtaznews.com***/%D9%85%D8%B1%D9%88%D8%-B1%DB%8C-

37. http://***www.tasam.org***/files/pdf/raporlar/siber_teror/639c0ad9-f639-4c64-9220-3bbc07f81993.pdf.

38. http://***fa.rfi.fr***/%D8%A7.