GÜVENLİK YAZILARI
https://trguvenlikportali.com/guvenlik-yazilari/
Seri Editörü: Prof.Dr. Mustafa Aydın, Kadir Has Üniversitesi
No. 42, KASIM 2019

SİBER GÜVENLİK VE SAVUNMA

Doç.Dr. Salih Bıçakcı
Kadir Has Üniversitesi
asbicakci@khas.edu.tr

ÖZET

Siber güvenlik, en sade anlamıyla siber uzayın her türlü tehditten korunmasını esas alır. Bütüncül ve derleyici bir kavramdır. En küçük siber suçtan en büyük ve karmaşık saldırıya kadar bütün katmanları içine alan birleştirici bir unsurdur. Siber güvenlik en temel haliyle verinin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunmasıdır. Siber tehditleri başlıca üç ana başlık altında toplayabiliriz: hatalar, kazalar, saldırılar. Bunların ulusal güvenlik açısından organize edilmesi gereklidir. Siber suçlar ve bunlarla mücadele, askeri siber organizasyon ve operasyonlar, istihbarat ve karşı istihbarat, kritik altyapı koruması ve ulusal kriz yönetimi, siber diplomasi ve İnternet yönetişimi başlıkları ulusal siber güvenliğin temellerini oluşturmaktadır. Bu yazıda siber tehditlerin bu beş temel alanda nasıl güvenliği etkilediğini anlamaya çalışacağız.

ATIF İÇİN: Bıçakcı, Salih, "Siber Güvenlik ve Savunma", *Güvenlik Yazıları Serisi*, No.42, Kasım 2019. *https://trguvenlikportali.com/wp-content/uploads/2019/11/SiberGuvenlik_SalihBicakci_v.1.pdf*
DOI: 10.13140/RG.2.2.21435.77601

Siber uzayı esas alan siber güvenlik kendi başına sanal bir alan değildir. Siber uzay fiziksel ve sanal alanın etkileşiminden oluşan bir alandır.

Siber güvenlik İnternet'in yaygınlaşması ve gündelik veri iletişiminin hızlıca dijitalleşmesi neticesinde ortaya çıkmış bir kavramdır. 1991'de İnternet'in sivil kullanıma yaygın olarak açılması ve gelişen bilgisayar teknolojisi bireylerin fiziksel dünyadaki bağlantılarına dijital ve sanal ortamı eklemiştir. Bugünlerde 'siber uzay' adını verdiğimiz bu alan 2000'li yıllarda gelişen telekomünikasyon teknolojisiyle birlikte etkili biçimde hayatımıza girmiştir. İletişim teknolojilerinin yaygınlığındaki artış dijital verilerin üretimini de teşvik etmiştir. Artık sadece kurumların, şirketlerin, siyasi yapının ve ekonomik unsurların değil, onlara temel teşkil eden bireylerin (vatandaşların) verilerinin de güvenli şekilde kullanılması gündemdedir.

Günümüzde sıkça kullanılmaya başlayan siber güvenlik kavramı en temel anlamıyla, siber uzay alanındaki güvenlik sorunlarıyla ilgilenen bir tanımdır. Siber güvenlik, en sade anlamıyla siber uzayın her türlü tehditten korunmasını esas alır. Bütüncül ve derleyici bir kavramdır. En küçük siber suçtan en büyük ve karmaşık saldırıya kadar bütün katmanları içine alan birleştirici bir unsurdur. Uluslararası ilişkiler perspektifinden bakıldığında devletin bireyi koruması gerektiği ilkesi burada da esastır. Ancak 1990'larda bu kavramın kullanımı için esas alınan tanım ve sahadaki dinamikler ile günümüzdeki etkenler arasında devasa farklılıklar olduğunun da altı çizilmelidir.

Siber uzayı esas alan siber güvenlik kendi başına sanal bir alan değildir. Siber uzay fiziksel ve sanal alanın etkileşiminden oluşan bir alandır. Her iki alanın etkileşimi siber güvenlik kavramını daha da önemli hale getirmektedir. Eğer sanal alanda yapılan işlemlerin fiziksel dünyada etkisi olmasaydı, muhtemelen siber güvenlik diye bir kavramdan bahsetmezdik. Bir diğer ifadeyle, siber alanda yapılan saldırılar ya da hamleler fiziksel alanda etki oluşturduğu için siber güvenlik kavramı ortaya çıkmaktadır. Bu yüzden de siber güvenlik alanında kullanılan terminoloji ister istemez ulusal güvenlik kavramlarını temel almaktadır.

Günden güne gelişen bilişim ve iletişim teknolojileri (BİT) insanların hayatına farklı ekipmanlarla hızlı bir şekilde girmiştir. İlk atılım bilgisayar ve iletişim teknolojilerinin önde gelen cihazı telefonun hızlıca yaygınlaşmasıyla başladı. İlk yıllarda daha az gelişmiş ve pahalı olan teknoloji 2000'li yılların başında nispeten ucuzlayarak erişilebilir hale geldi. Herkes hızlıca bu iletişim ağına dahil olmak için çabaladı. İnternetin hızlı yükselişi ve Castells'in (2010) tanımladığı ağ toplumunun oluşumu da bu yıllara denk gelmektedir. Sadece ülkelerin nüfusunun değil, dünya nüfusunun bu anlamda ağ toplumu oluşturması, takip eden dönemde ortaya çıkan yeni tehlikelerin ve tehditlerin

NATO sadece saldırılara karşı üyelerini savunmak amacıyla tasarladığı siber savunma stratejisinden, siber saldırıyı da içine alan bir yaklaşıma doğru evrildi.

yankısının büyük olmasına sebep olmuştur. Bağlanmış bir toplumda siber tehditlerin en temellerinden olan virüsler ve kötücül yazılımlar böylece hızlıca yayılabilmiştir.

Siber güvenlik kavramının ilk kullanılmaya başlandığı yıllarda tehditler ve bunların bilgisayar sistemlerine erişimi daha temel güvenlik açıklarını hedef alıyordu. Güvenlik yaklaşımı ile dizayn edilmemiş donanım ve yazılımların oluşturduğu açıkların da bu dönemde saldırganların işini kolaylaştırdığı belirtilmelidir. Bugün gelinen noktada, siber güvenlik kavramının temelde donanım, yazılım, insan, değerler katmanı ve politik katman olarak beş ana katmandan oluştuğu söylenebilir. Bu katmanların hepsi gizlilik, bütünlük ve erişilebilirlik ilkesi altında yer almaktadır.

Siber güvenliğin en temel prensibi üretilen veri ile en küçük veri parçasının gizliliğinin korunabilmesidir. Böylece her isteyen veriye ulaşamaz. Ayrıca verinin bir noktadan diğer noktaya giderken bütünlüğü de bozulmamalıdır. Siber güvenlik sadece gizlilik ve bütünlük esaslı olsaydı, çözümü bulmak daha kolay olurdu. Fakat günümüzde verilerin birden fazla program ya da sunucu veya kullanıcı tarafından aynı anda korunması gerekliliği, siber güvenlik kavramını daha zorlu hale getirmektedir.

Siber tehditleri başlıca üç ana başlık altında toplayabiliriz: hatalar, kazalar, saldırılar. Hatalar genellikle bilgi sistemlerinin içinde çalışan kişilerin bilinçsizce yaptıkları kusurlardır. Bu kusurlar sistemin güvenliğini tehdit eder. Kazalar daha ziyade insanların kontrollerinin dışında belirsiz bir zaman takvimi izleyerek gelişen -tabii afetler bu kategoride ele alınabilir- ve sistemlere zarar veren olaylar için kullanılır. Saldırılar ise aktif ya da pasif olarak bilgi işlem sistemlerine zarar vermeyi amaçlayan ve organize şekilde insan-düşman tarafından tasarlanmış eylemlerdir. Siber güvenlik tesis edilmeye çalışırken alınan önlemlerin hatalara mı, kazalara mı yoksa saldırılara mı çözüm olmayı hedeflediği önemlidir.

Siber güvenliğin ulusal seviyede gerçekleştirilmesi için beş zorunlu alanda çalışmalar yapmak gerekir (Klimburg, 2012). Bu alanlar siber güvenliğin tesis edilmesi için de gereklidir.

Siber Suçlar ve Mücadele

Siber uzayın güvenliğinin en temel unsuru siber suçlardır. Bu suçlar büyük çaplı saldırıların da temelini teşkil etmektedir. Ulus devletlerin vatandaşlarını korumak için etkin bir 'siber suçlarla mücadele organizasyon yapısı' kurması zorunludur. Kritik altyapıları hedef olan saldırılar bile çoğunlukla siber suç olarak kişisel erişim bilgisinin çalınması suretiyle başlamaktadır. Günümüzde artan miktarda organize suç örgütlerinin siber suçlar yoluyla para kazandığını ve bu sahada aktif olduklarını görüyoruz. Bunların belirli bir plan ve taktik çerçevesinde geliştikleri ve siber suçlar sayesinde dikkate değer miktarlarda paralar kazandıkları gözlenmektedir.

Bu örgütler son yıllarda özellikle 'fidye yazılımları' (*Ransomware*) kullanarak birçok küçük ve orta ölçekli işletmeyi zora sokmuştur. Fidye yazılımlar, temelde erişebildiği bilgisayardaki bilgileri hızlıca şifreleyerek, açılabilmesi için gerekli bir şifreye (anahtara) bağlar. Kullanıcıya bilgisayar ekranından belirli bir zamana kadar istenilen miktarda dijital parayı ödemezse bütün bilgilerinin silineceğini ifade eden bir uyarı çıkar.

2018 yılında bu tür yazılımların ticari sektöre maliyeti 8,5 milyar ABD Doları olmuştur. 2019 içinse bu rakamın 11,5 milyar ABD Dolarına çıkması beklenmektedir. Siber güvenlik alanında çok açıklanmasa da sadece ticari şirketlerin değil, kamu kurumlarının da fidye yazılımlar yüzünden büyük zararlar gördüğü ve hizmetlerinin kesintiye uğradığı bilinmektedir. Özellikle saldırı sonrasında bilgisayar sistemlerinin güvenliği için yatırımların maliyeti zaman zaman saldırganlara ödenenden çok daha fazla olabilmektedir.

Fidye yazılımlar bu tür güvenlik sorunlarının sadece bir örneğidir. Bu nedenle siber suçlar siber güvenliğin temel unsuru olarak çok önemlidir, dikkate alınmaması genelde daha büyük zararların ortaya çıkmasına sebep olmaktadır. Kritik altyapıyı hedef alan saldırganlar da siber suçlarla başlayarak hedefine ulaşmaktadırlar. Bu kapsamda siber suçlarla mücadele, polisiye tedbirlerin yanı sıra siber suçları anlayan kanunların çıkarılması ve gerekli düzenlemelerin yapılması ile siber suçlarda uzmanlaşmış hâkim ve savcıların varlığını da içermektedir. Konunun teknik içeriği yasama, yürütme ve yargının ortak bir hareket planı izlemesini gerektirmektedir.

Askeri Siber Organizasyon ve Operasyonlar

Her ne kadar şimdiye kadar ölümcül sonuçları olan siber savaş olmamışsa da, siber güvenliğin önemli bir kısmını askeri siber güvenlik önlemleri

Siber güvenlik alanında çok açıklanmasa da sadece ticari şirketlerin değil, kamu kurumlarının da fidye yazılımlar yüzünden büyük zararlar gördüğü ve hizmetlerinin kesintiye uğradığı bilinmektedir.

Siber güvenlik alanında çalışan firmaların sunduğu siber tehdit istihbaratı sadece ekonomik gücü yüksek şirketler tarafından yaygın olarak kullanılmaktadır.

oluşturmaktadır. Günümüzde hibrit savaş içinde siber unsurların kullanılması yanında, birçok askeri hedefe yapılan saldırılara siber saldırı unsurlarının da eşlik ettiğini görmekteyiz. Özellikle askeri istihbarat unsurlarının önemli bir kısmının artık siber saldırı ve istihbarat araç ve yöntemleri kullandığı bilinmektedir. Bu nedenle, bir güvenlik ittifakı olarak NATO da, 2007'de Estonya'ya yönelik gerçekleştirilen siber saldırıdan sonra öncelikle siber uzaya dönük savunma odaklı bir strateji geliştirmiştir.

Kritik altyapıların korumalarını esas alan bu yaklaşım, 2008'de Rusya'nın Gürcistan'da ülkenin hem kara askeri güçlerini hem de bilgisayar ve iletişim altyapısını hedef alan saldırısıyla birlikte daha da derinleşti ve bu tür saldırılara karşı önlemler geliştirebilmek amacıyla 14 Mayıs 2008'de Estonya Tallinn'de *Siber Savunma Mükemmeliyet Merkezi* kuruldu. Ardından NATO'nun 2016 Varşova Zirvesi'nde siber uzay kendi başına bir 'askeri operasyon sahası' olarak kabul edildi. Böylece NATO sadece saldırılara karşı üyelerini savunmak amacıyla tasarladığı siber savunma stratejisinden, siber saldırıyı da içine alan bir yaklaşıma doğru evrildi. Bu gelişme sonrasında üye ülkeler de askeri yapıları içinde siber uzayda savaşabilecek birlikler tesis etmeye başladılar.

Siber uzayın ayrı bir operasyon alanı olarak kabul edilmesi, siber saldırılara nasıl karşılık verilebileceği gibi teknik soruları gündeme getirdi. Özellikle ABD'de 'siber saldırılara fiziksel cevap verilip verilmeyeceği' yönünde hararetli tartışmalar olurken, Washington, Amerikan askeri güçlerinin kişisel bilgilerini *Twitter* aracılığıyla duyuran DAEŞ'li bir siber saldırgana (*hacker*) insansız hava araçları ile saldırı düzenleyerek bu konudaki ilk örneği oluşturdu. 6 Mayıs 2019'da da İsrail ordusu, siber saldırı gerçekleştiren HAMAS'a karşı bu saldırıların yapıldığını iddia ettiği Gazze'deki bir binayı bombalayarak karşılık verdi. Böylece siber saldırılara karşı fiziksel cevap verilebileceği konusunda belirgin örnekler ortaya çıkmış oldu.

Askeri siber organizasyonların ve operasyonların hızla gelişmesine karşın uluslararası hukukun bu konuda yetersiz kaldığı ve henüz gelişmekte olduğu görülmektedir. Askeri siber organizasyonların karar vericilerinin bu bağlamda uluslararası hukukun gelişiminde yönlendirici rol oynayabilmek için siber diplomasi sahasında çalışan kurumlarla işbirliği yapmaları gerekmektedir.

İstihbarat ve Karşı İstihbarat

Siber güvenliğin hızla yükselen unsurlarından birisi de siber istihbarat altyapısıdır. Her türlü verinin dijitalleştiği günümüzde devletlerin birçok farklı konuda açık ve gizli bilgiye ulaşmak için istihbarat inşa etmesi gerektiğini biliyoruz. Bu çerçevede siber istihbarat bilgi toplama, işleme, analiz etme ve

Siber güvenliğin temel taşlarından olan birçok konu arasında uluslararası hukukun rolü de unutulmamalıdır.

bilgiyi yayma yöntemleriyle siber alandaki tehditleri, riskleri ve fırsatları tahmin edebilmek ve bunlara karşı nasıl bir yol izleneceğine dair karar verme sürecini desteklemektir.

Siber güvenlik alanında çalışan firmaların sunduğu siber tehdit istihbaratı sadece ekonomik gücü yüksek şirketler tarafından yaygın olarak kullanılmaktadır. Ulusal anlamda siber güvenliği temin edebilmek içinse istihbarat servislerinin bünyesinde uzun süreden beri siber istihbarat yapılanmalarının oluşturulduğu bilinmektedir. Genellikle farklı kurumların siber istihbarat topladığı gözlemlenen devletlerde bunların iyi bir yönetimle gerekli yerlere zamanında ulaşması siber güvenliğin zaman hassasiyeti açısından önemlidir.

Siber istihbaratın özellikle ulusal anlamda ekonomik kayıpları minimize etmek gibi bir rolü de vardır. Günümüzde teknoloji araştırma ve geliştirme faaliyetleri için yapılan harcamalar ve bu geliştirmeleri kolayca elde etmek isteyen diğer ülkelerin siber saldırılarla bunları ele geçirmelerine en iyi örnek olarak Çinlilerin F-35 askeri uçak projesine yaptıkları saldırıları verebiliriz. Bunun yanında diğer sektörlerde de siber saldırılar firmaların en azından itibar kaybetmesine sebep olmaktadır. Ulusal ekonomik değerlerin tehditlere ve muhtemel saldırılara karşı zamanlıca uyarılmasında siber istihbarat yapılanmalarına büyük bir görev düştüğü açıktır.

Siber istihbaratları son yıllarda zorlayan olayların başında sızıntılar gelmektedir. Julian Assange'ın yayınladığı *Wikileaks* belgeleriyle başlayan süreçte ABD ve müttefiklerinin gizli yazışmalarına kadar pek çok belge İnternete sızmıştır. Ardından, Orta Doğu ülkelerinin gizli yazışmalarından *Stratfor* firmasının hassas e-postlarına kadar birçok bilgi ve belge bütün İnternet kullanıcılarının erişimine açılmıştır. Benzer şekilde Edward Snowden da ortaya çıkardığı belgelerle ABD Milli Güvenlik Ajansı (NSA)'nın kullandığı birçok gizli teknoloji ve takip metodunu bilinir hale getirmiştir. 18 Haziran 2019'da Rusya'nın Federal Güvenlik Ajansı'na (FSB) yapılan saldırı ile 7.5 TB'lık bilgi ve doküman da İnternet'e sızdırıldı. Bunların yanı sıra, Rusya'nın uluslararası alanda devam ettirdiği birçok sosyal medya operasyonu ile *Facebook* ve *Linkedin*'de sürdürdüğü bilgi toplama projeleri açığa çıkmıştır. Uluslararası anlamda bu kadar aktif bir sürecin üstesinden gelebilmek için devletlerin güçlü karşı siber istihbarat yapıları kurarak, kendi güvenlik ihtiyaçlarına göre yapılanmalarının gerekli olduğu ortadadır.

Kritik Altyapı Koruma ve Ulusal Kriz Yönetimi

Siber güvenliğin sağlanması konusunda en hassas noktalardan birisi kritik altyapıların korunması (KAK) konusudur. Her ülke kendi tehdit ve

ihtiyaçlarına göre hangi sektörlerin kritik altyapı olarak sınıflanacağını belirlemektedir. Telekomünikasyon, enerji, bankacılık, ulaşım, sağlık, su dağıtım şebekeleri gibi farklı sektörler bu yapının içinde değerlendirilir. Bu sektörlerin birçoğunun özel işletmeler tarafından yürütülmesi ortak hareket edebilme konusunda sorunlar doğurmaktadır.

Kritik altyapıların korunmasında en çok tartışılan konulardan birisi de bu yapıların içinde çalışan fonksiyon odaklı işlemcilerin güvenlik zafiyetidir. 2010'da siber güvenlik uzmanları tarafından tanımlanan İran nükleer tesislerine saldırmak için dizayn edilmiş *Stuxnet virüsü* bu konuda verilebilecek güzel örneklerden birisidir. Geleneksel savaş stratejileri incelendiğinde ilk saldırının rakibin iletişim ve enerji kaynaklarını zayıflatmak ya da kesmek üzere yapıldığını görürüz. Bu tarihi yaklaşımla değerlendirildiğinde, KAK'nın askeri stratejinin siber uzayı da içerecek şekilde genişlemesi anlamına geldiği rahatlıkla görülür.

KAK'nın ve yönetimi için en gerekli yapılardan birisi siber olaylara müdahale etmek için kurulmuş merkezlerdir. Siber güvenliğin sağlanması sürekli takip ve inceleme gerektirdiği için ülkelerin gerek kendi ulusal KAK'na yönelik tehdit ve saldırıları gerekse daha genel ulusal güvenliği tehdit eden olaylara müdahale eden ulusal ekiplerinin oluşturulması zorunludur. Bütün bu yapının üstünde 2007'de Estonya'da yaşanan krize benzer bir olay olduğunda gerekli bilgilendirmeleri yapacak ve ülke çapında koordinasyonu sağlayacak bir kriz yönetim yapısı da kurulmalıdır. Saldırıların psikolojik etkisini azaltarak, küçük ve orta ölçekli işletmelere destek verecek bu yapı, krizin vermeyi planladığı sarsıcı etkiyi kabul edilebilir ölçülere getirmeye de katkı sağlayacaktır.

Siber Diplomasi ve İnternet Yönetişimi

Siber güvenliğin sağlanması, fiziksel güvenlikte olduğu gibi üzerinde uzlaşılmış sözlü ya da yazılı anlaşmalarla gerçekleşmektedir. Siber güvenliğin temelini teşkil eden İnternet altyapısının yönetimi de devletlerin ortak uzlaşısı üzerinden sürdürülmektedir. İnternet'in temel fonksiyonlarının yerine getirmesi için koordinasyon görevini yerine getiren *İnternet Tahsisli Sayılar ve İsimler Kurumu* (*Internet Corporation for Assigned Names and Numbers* - ICANN) ya da İnternet'in teknik altyapısının (protokolleri ve standartlarının) geliştirilmesi için görev alan *İnternet Mühendisliği Görev Grubu* (*Internet Engineering Task Force* - IETF), İnternet yönetimi için önemli kurumlar arasındadır. Bu grupların çalışmasında ve İnternet'in gittiği yönün belirlenmesinde siber diplomasiyi kullanarak devletlerin etkin olması büyük önem taşımaktadır. Özellikle İnternet omurgasına yönelik saldırıların arttığı

günümüzde acil bir durumda müdahale edebilecek ekiplerin oluşturulmasında katılımcı bir tavır izlemek çok önemlidir.

Siber güvenliğin temel taşlarından olan birçok konu arasında uluslararası hukukun rolü de unutulmamalıdır. Uluslararası hukukun siber uzayın askeri amaçlar için kullanımı konusunda büyük ilerlemeler kaydettiği bir dönemde devletlerin bu tartışmalara ilgisiz kalmaları sonunda istenmeyen sonuçlara sebep olacaktır. Bu nedenle ilgili kuralların oluşması aşamasında etkin ve aktif bir diplomasinin devrede olması gerektiği aşikardır.

Özetlemek gerekirse, biz istesek de istemesek de, siber uzay ve bununla ilgili güvenlik alanı günden güne büyümektedir. Her gün daha da dijitalleşen dünya bu alanın büyümesine hizmet etmektedir. Askeri ekipmandan tutun da sağlık araçlarına kadar hemen bütün cihazların dijitalleştiğine ve siber uzayla etkileştiğine şahit oluyoruz. Tüm bu gelişmeler olurken siber güvenliği hafife almanın vereceği zararların yıkıcı olacağı açıktır. Aynı şekilde, güvenlik sektörü, yapay zekâ ve benzeri teknolojilerin yükselişiyle birlikte bu güvenlik sahasının daha da derinleşeceğini öngörmek ve gerekli tedbirleri şimdiden almak zorundadır.

KAYNAKÇA

Castells, Manuel (2010). *The Rise of the Network Society*. Cambridge, M.A:: Wiley-Blackwell.

Klimburg, Alexander (der.), (2012). *National Cyber Security Framework Manual*. Tallinn: NATO CCD COE.

Zetter, Kim (2014). *Countdown to Zero day*. New York: Crown.

EK OKUMA

Bıçakcı, Salih vd. (2015). *Türkiye'de Siber Güvenlik*. İstanbul: EDAM.

Bıçakcı, Salih (2013). *21.yy'da Siber Güvenlik*. İstanbul: Bilgi Üniversitesi Yayınevi.

Bıçakcı, Salih (2012). "Yeni Savaş ve Siber Güvenlik arasında NATO'nun Yeniden Doğuşu", *Uluslararası İlişkiler,* Cilt 9, Sayı 34, ss. 205-226.

"Ulusal Siber Güvenlik Çalışmalarının Yürütülmesine ilişkin karar", https://www.uab.gov.tr/uploads/pages/siber-guvenlik/some-bkk.pdf

"Ulusal Siber Güvenlik Stratejisi 2016 – 2019", https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf

İNTERNET

Siber Kümelenme, https://siberkume.org.tr/birlikten-kuvvet-siber-guvenlik-dogar/

Bir Siber Güvenlik Hikayesi, https://youtu.be/vWPgPsPcA2c

FİLM

The Fallout: Gerçek Bir Siber Güvenlik Hikayesi, https://youtu.be/urmh4CuWv54

Hedefli Bir Siber Saldırının Hikayesi, https://youtu.be/TB1PYwSnz2M

Zero Days (2016). Yönetmen: Alex Gibney. USA: Magnolia Pictures.

Snowden (2016). Yönetmen: Oliver Stone. USA: Endgame Entertainment.

Citizenfour (2014). Yönetmen: Laura Poitras. USA: HBO Films.

The Fifth Estate (2013). Yönetmen: Bill Condon. USA: Dreamworks Pictures.

Official Secrets (2019). Yönetmen: Gavin Hood. ABD: Classified Films, Clear Pictures, The Golden Company.

Mr. Robot (2015). Yönetmen: Sam Esmail. ABD: USA Network.

Uluslararası İlişkiler Konseyi (UİK) Derneği, Türkiye'de uluslararası ilişkiler çalışmalarının gelişimine katkıda bulunmak, ilgili alanlarda çalışanları bir araya getirmek ve çalışmalarını desteklemek amacıyla bir grup akademisyen, medya çalışanı ve dışişleri mensubu tarafından 2004 yılında tarihinde kurulmuştur. 2010 yılından beri *International Studies Association* (ISA) ortak kuruluşu ve 2016'dan beri de *Balkan Political Science Association* (BPSA) üyesi olan UİK, iki yılda bir düzenlediği *Uluslararası İlişkiler Çalışmaları ve Eğitimi Kongresi* ile *Güvenlik Akademisi* ve *Dış Politika Akademisi* eğitim programlarını gerçekleştirmektedir. Uluslararası İlişkiler disiplininin Türkiye'deki gelişimine katkı yapmış öğretim üyelerine yönelik *Ustalara Saygı Ödülü* ile genç akademisyenlere yönelik *Teşvik Ödülü* veren UİK, başta *Uluslararası İlişkiler* dergisi ile *Güvenlik Çalışmaları* serisi olmak üzere kapsamlı bir yayım programı ile *Güvenlik Portalı* (GP), *Türkiye Barışı Koruma Veri Tabanı* (TÜBAKOV), *Kavram Avcıları* ve *Black Sea Young Reformers F*ellowship (BSYRF) projelerini hayata geçirmiştir.

UİK hakkında daha fazla bilgi almak için, lütfen web sayfasını (https:/www.uik.org.tr) ziyaret ediniz.

Güvenlik Yazıları, NATO Kamu Diplomasisi Birimi tarafından desteklenmektedir.

Security Papers are supported by the NATO Public Diplomacy Division.