Erciyes İletişim Dergisi / Journal of Erciyes Communication
e-ISSN: 2667-5811 | ISSN: 1308-3198

Araştırma Makalesi | Research Article

Sinemada Sibergüvenlikleştirme Söylemi: İnternetle İlgili Popüler Korku ve Gerilim Filmlerinin Analizi

Cyber Securitization Discourse in Cinema: Analysis of Popular Horror and Thriller Movies Related to The Internet

Umur BEDİR (Asst. Prof. Dr.)
Istanbul Aydın University, Faculty of Communication
Istanbul/Turkey
umurbedir@aydin.edu.tr

Başvuru Tarihi | Date Received: 17.08.2021
Yayına Kabul Tarihi | Date Accepted: 03.12.2021
Yayınlanma Tarihi | Date Published: 31.01.2022
https://doi.org/10.17680/erciyesiletisim.983854

Öz

Kophenag Okulu tarafından geliştirilen 'güvenlikleştirme teorisi' bir sorunun söylem yoluyla güvenlik sorunu olarak inşa edilmesi süreciyle ilgilenir. Bu araştırmada güvenlikleştirme teorisi ve bu teoriyi siber alana uyarlayan Hansen ve Nissenbaum'un yaklaşımından hareketle, popüler korku ve gerilim filmlerindeki siber güvenlikleştirme söylemi incelenmektedir. Bu bağlamda, farklı ülke sinemalarından internetin risklerine odaklanan 13 adet korku/gerilim filmi seçilmiştir. Bu filmlerde internet ve siber alandan kaynaklı bireysel ve toplumsal güvenlik tehditlerinin nasıl tanımlandığı, referans nesneleri, güvenlikleştirici aktörler gibi unsurların nasıl konumlandığı içerik analizi yöntemiyle incelenmiştir. Filmlerde internetin her türlü kontrol ve denetimden azade, tehlikeli ve kuralsız bir alan olarak sunulduğu, internet aracılığıyla tehdit unsurlarının kılık değiştirerek gündelik hayatın içerisine kadar sızabildiği ve kişisel mahremiyetin ihlal edildiği yolundaki argümanların öne çıktığı görülmektedir. Öte yandan gençler siber güvenlik söyleminin en temel referans nesnesi olarak sunulmakta ve siber alanın denetim altına alınması için devletin, uzmanların, bireylerin ve/veya ailenin vakit kaybetmeksizin harekete geçmesi gerektiği savunulmaktadır.

Anahtar Kelimeler: İletişim Bilimleri, Siber Güvenlikleştirme, Güvenlikleştirme Söylemi, İnternet, Korku Sineması.

Abstract

'Securitization theory' developed by the Copenhagen School deals with the process of construction of an issue as a security problem through discourse. In this research, based on the theory of securitization and the approach of Hansen and Nissenbaum, who adapted this theory to cyberspace, cyber securitization discourses in popular horror and thriller movies are examined. In this context, 13 horror/thriller films focusing on the risks of the internet were selected from cinemas from different countries.. In these films, how the individual and social security threats originating from internet and cyberspace are defined, how the elements such as referent objects and securitizing actors positioned are examined by using method of content analysis. In those movies, it is seen that the internet is presented as a dangerous and lawless area free from any control and supervision and the arguments that threat elements can infiltrate into daily life by disguising and that personal privacy is violated through the internet become prominent. On the other hand, young people are presented as the main referent object of the cyber security discourse and it is argued that the state, experts, individuals and/or family should take action without wasting time in order to control the cyberspace.

Keywords: Communication Sciences, Cyber Securitization, Securitization Discourse, Internet, Horror Movies.

Giriş

Kophenag Okulu ve en önemli temsilcilerinden biri olan Ole Weaver tarafından, soğuk savaş sonrası dönemde temelleri atılan güvenlikleştirme teorisi, geleneksel güvenlik anlayışının tersine, güvenlik kavramının ve buna paralel olarak güvenlik tehdidinin mutlak ve somut realiteden kaynaklanan bir tanımının ve içeriğinin olmadığı varsayımına dayanır. Toplumsal bir konunun nasıl, neden ve hangi aktörler tarafından bir güvenlik sorunu olarak tanımlandığını anlamak açısından uygun bir çerçeve sunar. Bu yaklaşıma göre, nelerin güvenlik tehdidi olduğu siyasal ve toplumsal olarak ve söylemsel edim aracılığıyla 'inşa' edilir. Güvenlikleştirme, kamusal bir sorunun devlet ve yönetici elitler tarafından acil, normal prosedürlerin dışında istisnai uygulamalar ve olağanüstü önlemler gerektiren bir mesele olarak çerçevelenmesiyle gerçekleşir (Waever, 1995, s. 7). Böylelikle konu, normal siyasetin alanından çıkarılarak güvenliğin alanına aktarılır ve tehdide karşı alınacak aşırı önlemler kamusal bir müzakereye ve haklı çıkarmaya gerek duyulmaksızın meşrulaştırılmış olur (Buzan, Waever, & Wilde, 1998, s. 23). Bu noktada, güvenlikleştirme teorisinin, kamusal meselelerin güvenlik alanının dışına taşınarak (*desecuritization)*, demokratik siyaset zeminde ve katılımcı bir şekilde müzakere edilmesi gerektiğini savunan normatif bir ideale dayandığını vurgulamak gerekir (Buzan & Hansen, 2009, s. 1). Güvenliğe inşacı bir perspektiften yaklaşması ve demokratik ideale dayanması gibi tüm bu özellikleri, güvenlikleştirme teorisini mevcut güvenlik paradigmalarına ve uygulamalarına yönelik eleştirel perspektife dayanan araştırmalar için de uygun bir zemin haline getirir.

Güvenlikleştirme analizi bir konunun öznelerarası olarak güvenlik sorunu olarak inşa edilmesi sürecini, bu sürecin nasıl işlediğini ve sonuçlandığını anlamaya dönük bir dizi analitik araç sunar (Baysal & Lüleci, 2015, s. 76). Bu bağlamda 'güvenlikleştiriciler' (herhangi bir tehdidin var olduğunu ilan eden aktörler), 'güvenlik sorunu' (tehdit olarak ilan edilen konu), 'referans nesnesi' (korunması gereken kişi, değer ya da obje), 'işlevsel aktörler' (referans nesnesi veya güvenlikleştirici olmaksızın referans nesnesi yerine güvenlik talep ederek süreci etkileyen birimler) gibi güvenlikleştirme sürecinin tüm unsurlarının nasıl konumlandığı ve söylem içerisinde nasıl tanımlandığı sorularını merkeze alır (Buzan, Waever, & Wilde, 1998, s. 36).

Geleneksel paradigmada yalnızca ulusal güvenlik ekseninde ve askeri sektör ile bağlantılı olarak tanımlanan güvenlik anlayışının, güvenlikleştirme teorisi çerçevesinde kapsamı da genişlemiştir. Bu anlamda, Kophenag Okulu kuramcıları çağdaş yaşamı güvenlik sorunu olarak tanımlanabilecek risklerin yalnızca askeri kaynaklı olmadığını, güvenlik olgusunun ayrıca siyasi güvenlik, ekonomik güvenlik, toplumsal güvenlik ve çevresel güvenlik gibi farklı sektörler üzerinden incelenmesi gerektiği tezini savunmuşlardır. Söz konusu sektörlerden her birinin tehdit algıları ve referans nesneleri bağlamında karakteristik özellikleri bulunmaktadır (Buzan, Waever, & Wilde, 1998, s. 7). Kophenag Okulunun erken dönemlerinde siber güvenlik ayrı bir sektör olarak tanımlanmamıştı. Ancak internetin ve yeni iletişim teknolojilerinin ekonomik, siyasal, toplumsal ve kültürel süreçlere giderek daha fazla eklemlenmesiyle siber güvenlik söylemine yönelik eleştirel ve inşacı yaklaşımlar geliştirilmeye başlanmış (Bendrath, 2001; Eriksson, 2002) ve siber güvenlik konusu da güvenlikleştirme kuramının alanına girerek ayrı bir sektör olarak tanımlanmıştır (Hansen & Nissenbaum, 2009).

Literatürde siber güvenlikleştirme söylemi konusunda yapılan araştırmaların pek çoğu, uzmanlar veya siyasal karar alıcılar gibi elit aktörlerin (Cavelty & Egloff, 2021; Gorr & Schünemann, 2013; Hill & Marion, 2017), çeşitli politika belgelerinin veya siyasal

faaliyetlerin (Lobato & Kenkel, 2015) analizine odaklanmaktadır. Buna karşın görsel temsiller (Cavelty, 2019) medya içerikleri (Hart, 2012; Lawson & Middleton, 2019) veya filmler (Viganò, 2020) gibi popüler kültür ürünlerinde siber güvenlikleştirme söyleminin nasıl çerçevelendiğini inceleyen görece daha sınırlı sayıda araştırma vardır. Diğer taraftan, siber güvenlikleştirme kuramı çerçevesinde yapılan araştırmalardan pek çoğu, referans nesnesi olarak ulusal güvenlik, ekonomi ve devlet fonksiyonları için kritik önemdeki enformasyon alt yapılarının korunması gibi konuları merkeze alan süreç ve söylemleri incelemektedir. Bu anlamda Batılı gelişmiş ülkelerin yanında (Cavelty, 2008; Jantunen & Huhtinen, 2011; Kasper, 2014; Lawson, 2013), az gelişmiş ve gelişmekte olan ülkeler veya otoriter rejimler üzerine de çeşitli araştırmaların yapıldığı görülmektedir (Kallender & Hughes, 2017; Shad, 2019; Yau, 2020; Virgy, Destianira, & Mustofa, 2020; Gessler, 2017). Buna karşın siber güvenlikleştirmeyi gündelik yaşamdaki yansımaları bakımından inceleyen ve internetin sosyal ve bireysel risklerine dair söylemleri ele alan araştırmalar literatürde daha az yer kaplamaktadır (Hill & Marion, 2017).

Bu araştırmanın amacı ise güvenlikleştirme teorisi çerçevesinde popüler korku ve gerilim sinemasında internetin nasıl ve hangi bağlamlarda bir güvenlik sorunu olarak inşa edildiğine dair ortak temaları tespit etmek ve bunları yorumlamaktır. Araştırma, filmlerde internet ve siber alanın yaratabileceği özellikle bireysel ve toplumsal tehditlere ilişkin nasıl bir güvenlikleştirme söylemi inşa edildiğine odaklanmaktadır. Bu anlamda ulusal, uluslararası, siyasal ve makro ekonomik boyuttaki riskler araştırma kapsamının dışında tutulmuştur. Araştırma ayrıca, siber güvenlik söylemini politika belgelerden veya teknik uzmanlar, siyasal karar alıcılar ve çıkar grupları gibi elit aktörlerden ziyade filmler gibi popüler içeriklerdeki yansımaları üzerinden inceliyor olması bakımından da özgün bir içeriğe sahiptir. Literatürde çevre felaketleri (Maertens, 2015) veya küresel terör (Coşkun, 2012) gibi farklı güvenlik sektörlerine ilişkin olarak popüler sinema ve televizyon dizilerindeki güvenlikleştirme söylemlerini inceleyen araştırmalara rastlamak mümkündür. Diğer taraftan filmlerde internet ve siber alan korkusunu (cyberphobia) tetikleyen abartılı çerçeveleme biçimlerine odaklanan araştırmalar bulunsa da (Viganò, 2020; Rosewarne, 2016) bunlar sistematik bir saha çalışmasına dayanmamaktadır.

Filmlerde ve popüler medya metinlerindeki siber güvenlikleştirme söylemleri ve bu tarz içeriklerde internetin (ağırlıkla olumsuz) çerçevelenme biçiminin eleştirel bir perspektiften incelenmesi oldukça önemlidir. Zira bu türden popüler mitler ve anlatı kalıpları aynı zamanda siber güvenlik uzmanlarının ve alanda güç ve denetim sahibi olmak isteyen siyasal ve ekonomik elitlerin kendi konumlarını ve faaliyetlerini meşrulaştırmak adına kullanabilecekleri bir söylemsel repertuvarın de ana unsurlarını oluşturmaktadır (Hill & Marion, 2017). Öte yandan siber güvenlik söyleminin oluşmasında ve topluma benimsetilmesinde de popüler kültürün önemli bir etkisinin olduğundan bahsedilebilir (Shires, 2020, s. 86). Bu kapsamda, araştırmanın ilk bölümünde Hansen ve Nissenbaum'un yaklaşımından ve konuya ilişkin literatürdeki diğer araştırmalardan hareketle siber güvenlik sektörünün karakteristik özellikleri ve siber güvenlikleştirmenin temel söylem kalıpları ortaya konulacaktır. Ardından örneklem olarak seçilen 13 adet filmin içerik analizine yer verilecektir.

Siber Güvenlikleştirme Söylemi

Siber güvenlik siber alan tarafından veya onun aracılığıyla yaratılan tehditler ve bu tehditleri ortadan kaldıracak veya azaltacak pratikleri ve süreçleri içeren bir kavramdır. Teknik veya teknik olmayan bir dizi önleme ve faaliyete vurgu yapar (Cavelty, 2010, s. 401). Soğuk savaş sonrası değişen güvenlik paradigmasının ve enformasyon devriminin

etkisini de yansıtan siber güvenlik kavramının temelleri 1970'lerde ABD'de atılmış ve 80'lerde önemli bir ivme kazanmış, diğer ülkelere yayılması ise 1990'ları bulmuştur. Siber güvenlik, statik bir kavram değildir. Gerek referans nesneleri, gerekse de temel aktörler, tehdit algısı ve bunlarla baş etme yöntemleri/araçları/stratejileri bağlamında kısa sayılabilecek tarihi içerisinde önemli dönüşümler geçirmiştir. Siber güvenlik ilk başta bazı özel sektör kuruluşlar veya devlete ait sistemler ile ilgili bir kavramken, bilgisayar ağlarının hayatın neredeyse tüm alanlarına yayılması ve yeni özellikler kazanmasıyla referans nesnelerinin tanımı genişlemiş ve kavram ulusal güvenliğin yanı sıra, devletin ve ekonominin fonksiyonlarını da ilgilendirir hale gelmiştir (Cavelty, 2010, s. 403). Zamanla farklı güvenlik sektörleri arasındaki sınırları bulanıklaştıran siber güvenlik yalnızca 'kritik önemdeki enformasyon altyapılarının' savunulmasının dışına çıkarak, ulusal güvenlik, devlet güvenliği, bireysel güvenlik ve ağ güvenliği gibi alanları da kapsamıştır (Diebert, 2002). Hansen ve Nissenbaum'a göre siber güvenlikleştirmenin dinamiklerini kavrayabilmek için alanı her biri birbiriyle bağlantılı bir dizi bireysel veya kolektif referans nesnesine sahip çoklu söylemler arasındaki rekabet olarak görmek gerekir (2009, s. 1163). Siber güvenlik ulusal veya uluslararası hiçbir düzeyde ortak anlayış ve terminolojiye dayanmamaktadır ve fazlasıyla fragmanlaşmıştır (Kasper, 2014, s. 185). Örneğin otoriter devletlerin ulusal güvenliği, rejimi, aileyi, bireyi, gençleri, ulusal kültürü ve kimliği korumak gibi gerekçeler öne sürerek ulus ötesi enformasyon akışını güvenlikleştirdiğine, interneti sınırlandırma veya gözetim altına alma yoluna gidebildiğine dair sayısız örnek bulunmaktadır. Buna karşın siber özgürlükçüler ise söz konusu uygulamaları bireysel mahremiyete, ifade özgürlüğü ve basın özgürlüğü gibi sivil haklara veya küresel ekonomiye yönelik bir tehdit olarak değerlendirebilmektedir. Ya da toplumun bilgiye erişim hakkı çerçevesinde yapılan hacktivist faaliyetler, liberal devletler tarafından fikri mülkiyet, ulusal güvenlik ve hatta terörle mücadele gibi gerekçelerle güvenlikleştirilmektedir.

Referans nesnelerini, tehditleri ve güvenlikleştirici aktörleri birbirine bağlayan güvenlikleştirme biçimleri ve kullandıkları gramer açısından her bir güvenlik sektörü kendine has bazı özellikler göstermektedir. Siber güvenlik sektörü için de bu durum geçerlidir. Hansen ve Nissenbaum'a göre siber güvenliğe özgü üç tür söylem kalıbı bulunmaktadır; Bunlardan ilki olan '*Hipergüvenlikleştirme*' kavramı, güvenlikleştirmenin normal tehdit düzeyinin ötesine taşınması, tehdidin abartılması ve bunun sonucunda aşırı-orantısız tedbir alma eğiliminde kendisini gösterir. Olası siber tehditlere yönelik çok boyutlu ve hipotetik siber felaket senaryoları oluşturulur (2009, s. 1164). Bu felaket senaryoları ağda bir sorun ortaya çıkması durumunda finansal, sosyal, askeri alanda ve diğer sektörlerde eş zamanlı olarak nasıl kırılmalar yaşanabileceğine ilişkin çeşitli projeksiyonlar sunar. Bireysel boyutta ise siber güvenlik söylemi, isimsiz ve tehlikeli yabancıların ağın sunduğu olanaklardan yararlanarak masum insanların özel yaşamına kılık değiştirmek suretiyle sızmasına dair sayısız imaj ve senaryo üretir (Sandywell, 2006, s. 50).

'*G*ündelik güvenlik pratikleri' olarak tanımlanan ikinci söylem modeli ise, güvenlikleştirici aktörlerin, argümanlarını hedef kitle nezdinde inandırıcı hale getirmek ve bireyleri ağ güvenliğini sağlamaya dönük olarak harekete geçirmek amacıyla, felaket senaryolarını bireylerin gündelik yaşamıyla bağlantılandırma çabasıdır. Güvenlikleştirmenin başarısı, güvenlikleştiricinin hedef kitlesinin hissiyatı, ihtiyaçları ve çıkarlarıyla özdeşlik kurmasına, söylemini onun gündelik, somut deneyimlerine göre şekillendirmesine bağlıdır. Gündelik hayatta siber güvenlikleştirmenin en önemli ayrıcı özelliği, bireyi

yalnızca güvenlik sorunlarıyla baş etmekle ve gerekli tedbirleri almakla sorumlu bir partner değil, aynı zamanda tehdidin sorumlusu ve hatta bizzat kendisi olarak görmesidir (Hansen & Nissenbaum, 2009, s. 1165). Bu çerçevede bireye yönelik eğitici ve güvenlikleştirici söylemler aynı esnada devreye girer, çeşitli klişeleşmiş metaforlar (viral bir hastalık gibi yayılan siber tehdit), algılamada kolaylık yaratan stereotip temsiller (dijital oyun bağımlısı asosyal ergen) sıklıkla kullanılır.

Son olarak '*Teknikleştirme*' ise, siber güvenlikleştirme söz konusu olduğunda, diğer sektörlerden daha baskın biçimde öne çıkan en önemli söylemsel stratejilerden biridir. Bu söylem biçimi tekniği "sıradan insanların ve politikacıların sahip olmadığı düzeyde uzmanlık gerektiren bir alan olarak görür ve bu durum uzmanların –bilgisayar bilimciler, enformasyon bilimciler veya siber güvenlik şirketlerine- siyasal aktörlerden kendilerini ayırarak güvenlikleştirici olarak konumlanmalarına olanak verir" (2009, s. 1167). Güvenlikleştirme mantığı içerisinde işleyen teknikleştirme siyasal meşruiyeti ve epistemik otoriteyi inşa eder. Güvenlikleştirmenin siyasal ve ideolojik köklerini teknik rasyonalitenin arkasında gizleyerek, söz konusu söylemin siyasal ve normatif olarak tarafsız bir ajandaya hizmet ettiği illüzyonunu yaratır. Bu söylem biçimi siber güvenliği, siyasal ve toplumsal bir müzakere konusu olmaktan çok profesyonel ve uzman müdahalesi gerektiren bir alan olarak çerçeveler.

Yöntem

Araştırmanın evrenini, internet ve sosyal medyayı konu alan 39 adet korku ve gerilim filmi oluşturmaktadır. Araştırma kapsamında bu filmlerden 13 tanesi örneklem olarak seçilmiştir (bknz. Tablo 1). Örneklemlerin belirlenmesinde, öncelikle seçilen filmlerin birer popüler sinema örneği olması, internet ve sosyal ağları güvenlik sorunu olarak çerçevelemesi, söz konusu teknolojilerin siyasal, makro-ekonomik, ulusal ve uluslararası etkilerinden ziyade toplumsal ve bireysel risklerine odaklanması gibi kriterler göz önünde bulundurulmuştur. Popüler sinema kavramı ile kast edilen, filmlerin geniş kitleler tarafından izlenmesi ve beğenilmesinden ziyade, klasik anlatı yapısına dayanması, egemen ideolojik kodları ve ahlaki değerleri ifade etmesidir (Bedir, 2014, s. 105). Bu bağlamda araştırmada amaçlı örnekleme tekniklerinden biri olan 'ölçüt örnekleme' kullanılmıştır. Öte yandan bu özelliklere sahip filmlerin çoğunlukla ABD (ve kısmen de İngiltere) menşeli olmasına rağmen, olası söylemsel farklılaşmaları analiz edebilmek açısından farklı ülke sinemalarından da örneklem seçmeye özen gösterilmiştir.

Tablo 1. *Örneklem Seçilen Filmler (Yapım Yılı ve Menşei)*

	FİLM	Yapım Yılı	Menşei	IMDB
1	Death Tube: Broadcast Murder Show	2010	Japonya	4.8
2	Cyberbully	2015	Birleşik Krallık	6.8
3	Friend Request	2016	Almanya	5.3
4	Untraceable	2008	ABD	6.2
5	Chatroom	2010	Birleşik Krallık	5.5
6	Suicide Room	2011	Polonya	6.6
7	Girlhouse	2014	Kanada	5.5
8	Disconnect	2012	ABD	7.5
9	The Den	2013	ABD	6.0
10	Unfriended: Cybernatural	2014	ABD-Rusya	5.5
11	Host	2020	Birleşik Krallık	6.5
12	U Want Me 2 Kill Him?	2013	ABD	6.3
13	Dabbe	2006	Türkiye	4.4

Araştırma kapsamında seçilen filmler içerik analizi yöntemiyle incelenmiştir. İçerik analizi "bir mesajın içeriğindeki verilerden yinelenebilir ve değerli çıkarımlar yapan bir araştırma tekniğidir" (Krippendorff'dan aktaran Aziz, 2017, s. 131). Daha ziyade nicel araştırmalarda kullanılan bu veri toplama tekniği, araştırmacının ele aldığı konuya bağlı olarak belirlediği birimler üzerinden, metin içerisinde belirli örüntülerin hangi sıklıkla (*frekans*) tekrar ettiğinin incelenmesini amaçlar. Bu çerçevede öncelikle her bir filmin künye bilgilerinin, temel hikaye örgüsünün ve filmde temsil edilen ana karakterlerin psiko-sosyal, demografik ve kişisel özelliklerinin ayrıntılı dökümü yapılmıştır.[1] Ardından örnekleme dahil edilen filmler aşağıdaki birimler bağlamında değerlendirilip kodlanarak, elde edilen bulgular güvenlikleştirme teorisi çerçevesinde yorumlanmıştır:

1. İnternet ve sosyal medya ile bağlantılandırılan güvenlik tehditlerinin neler olduğu,
2. Güvenlik tehdidini ortaya çıkaran faillerin kimler veya neler olduğu,
3. Referans nesnelerinin kimler veya neler olduğu,
4. Filmlerde güvenlikleştirici aktörlerin veya güvenlik sorunuyla başa çıkma görevini üstlenen kişi veya kurumların neler/kimler olduğu,
5. Filmlerde güvenlikleştirme sürecinin nasıl bir sonuca bağlandığı.

Analiz

Filmlerde internetin bireyler açısından, hangi özellikleri bağlamında ve nasıl güvenlik tehdidi olarak çerçevelendiği önemli bir sorudur. Bu bağlamda filmlerde en sık tekrarlanan güvenlik sorunları Tablo 2'de sıralanmıştır. Bunların en başında, internetin bireylerin sanal kimlikler inşa ederek kendilerini olduklarından farklı gösterebilmelerine ve anonim kalabilmelerine olanak sağlayan yapısı gelmektedir. İncelenen filmlerin anlatısına bakıldığında, bu özellik çoğunlukla art niyetli kişilerin ve 'tehlikeli yabancıların', gerçek kimliklerini açık etmeksizin, farklı sunucuları ve IP adresleri kullanarak bireylerin yaşamına sızmasına ve hiçbir ceza almaksızın kötü emellerini gerçekleştirebilmesine neden olduğu görülmektedir. Unfriended, U Want Me 2 Kill Him?, Cyberbully, Untraceable, The Den ve Chatroom filmleri, internet üzerinden irtibat kurulan kişinin gerçekten kim olduğunu ve niyetini asla bilemeyeceğimize dair bir endişeyi körüklemektedir. Esasında güvenlik tehdidi olarak sıralanan diğer unsurların temelinde de söz konusu durumun yattığından bahsedilebilir. Zira siber zorbalık, kimlik hırsızlığı, siber pornografi ve diğer siber suçların işlenmesi ve faillerin kolaylıkla izini kaybettirebilmesi için de uygun zemin yaratır. Ayrıca faillerin kendilerini sanal kimlikler ve anonim hesaplar ardında gizleyebiliyor oluşu, siber alanın devlet, kolluk kuvvetleri ve otorite mercileri tarafından etkin şekilde denetlenebilmesinin önüne geçtiği vurgulanmaktadır.

İncelenen filmlerde sıklıkla vurgulanan diğer bir tema ise kişilerin mahrem bilgilerinin kötü niyetli kişilerin eline geçmesi ve ifşa edilmesi sorunudur. İnternette verilerin tam olarak silinememesi, bireysel ağ güvenliği açıklarının tam olarak ortadan kaldırılamaması, bu açıklardan yararlanarak kişisel verileri ele geçiren ve bunu kötü amaçlar için kullanan bilgisayar korsanları için geniş bir hareket alanı sağlamaktadır. Özellikle Chatroom, Cyberbully, Suicide Room, The Den, Unfriended, Disconnect gibi filmlerde yoğun olarak işlenen bu tema çerçevesinde, bilgisayar korsanlığı yoluyla elde edilen kişisel verilerin çoğunlukla siber zorbalık, mağduru intihara veya psikolojik bunalıma sürüklemek için kullanıldığı görülmektedir. Ayrıca filmlerin içerisinde izleyiciye yönelik, bilmediği sitelere girmemeleri, emin olmadıkları bağlantılara tıklamamaları veya tanımadıkları kişilerle sanal ortamda bilgi paylaşmamaları gerektiği türünden öğretici mesajların da serpiştirildiği görülmektedir. Diğer taraftan sosyal medyada popüler olmak veya

kazanç elde etmek amacıyla gönüllü olarak kendi mahremiyetlerini ifşa eden karakterler de bulunmaktadır. Bunlar ise film anlatısı içerisinde çoğunlukla ağır bir şekilde cezalandırılmaktadır (bknz. Friend Request, Girl House).

Filmlerde yoğun olarak verilen bir diğer mesaj ise internetin kontrol edilmesi mümkün olmayan bir alan olduğudur. Siber dünya çoğunlukla anarşist, kontrol dışı, kanunsuz ve hatta yeni kurallara ve denetime ihtiyaç duyan bir alan olarak resmedilir (Cavelty, 2013, s. 112). Bu durum siber alanın dinamik yapısından, bilgi akışı ve etkileşimlerin hızlı ve viral olarak gerçekleşmesinden ve kişilerin anonim kalmasına olanak tanımasından ileri gelmektedir. Filmlerde kullanılan güvenlikleştirme söyleminin dayandığı bir diğer argüman ise 'Dark Web' adı verilen, girmek için özel yetkilendirme gereken ve güçlü şekilde şifrelenmiş yasa dışı ağlardır. Bu ağlar üzerinden siber pornografi (Bknz. Girl House), çocuk pornografisi, gerçek şiddet görüntüleri (Bknz. The Den, Death Tube) veya intihara yönlendiren içerikler (bknz. Suicide Room) gibi her türlü siber suç unsuru dolaşıma sokulabilmektedir. Bu anlamda filmlerin neredeyse tamamında geleneksel güvenlik tedbirlerinin siber suçlarla mücadelede yetersiz kaldığı, polis teşkilatının failleri ancak birkaç adım geriden takip etmekle yetindiği görülmektedir2. Öte yandan filmlerin birçoğunda devlet ve toplumsal kurumlar tarafından, internetin yol açtığı güvenlik sorunlarıyla daha etkin bir şekilde mücadele edebilecek ve siber alanın ruhuna uygun yeni yöntem ve araçların 'acil olarak' geliştirilmesi gerektiğine dair güçlü alt metinler görmek mümkündür3. Güvenliği sağlamakla görevli aktörlerin başarı sağladığı az sayıda filmde ise, bunun standart güvenlik prosedürlerinin ve güvenlik bürokrasinin dışında hareket eden bir polis komiserinin bireysel çabası sayesinde başarılmış olması önemli bir detaydır (Bknz. Untraceable).

Filmlerde sıklıkla tekrar edilen bir diğer klişe ise internet ve sanal dünyanın bireyleri (özellikle de gençleri) yalnızlaştırdığı, asosyal hale getirdiği, toplumsal ilişkileri ve aile ilişkilerini zayıflattığı ve bu yolla kişiyi daha savunmasız hale getirdiği yönündedir (bknz: Disconnect). Buna göre, internetin sunduğu sanal ilişki biçimleri ve siber fanteziler karşısında gerçek dünya ve gerçek ilişkiler önemsizleşmektedir. Filmlerin pek çoğunda çevrimiçi oyunlar, sanal sohbet uygulamaları ve sosyal medyayı yoğun şekilde kullanmaya başlayan karakterlerin, adım adım gerçek dünyadan ve gerçek ilişkilerden geri çekildiği, 'bilgisayar kurdu asosyal genç' stereotipinin birçok filmde yeniden üretildiği görülmektedir. Bunun tam tersi bir şekilde, kişiler sosyal bağları ve ebeveynleriyle ilişkileri zayıfladığı için de kendilerini sanal ilişkilere daha fazla adayabilmektedir (bknz. Suicide Room). Ancak her iki durumda da filmlerin anlatı kalıplarının sosyal ilişkiler ile çevrimiçi ilişkiler arasında yapay bir karşıtlık inşa ettiği söylenebilir.

Filmlerde güvenlik sorunu olarak çerçevelenen bir diğer önemli tema ise cinler, kötü ruhlar veya lanetler gibi doğaüstü unsurların insanları rahatsız etmesi ve felakete sürüklemesidir. Bu anlatı kalıbı çerçevesinde, doğaüstü varlıklar internet ve sosyal ağları kullanarak 'yaşayanların' hayatına sızabilmektedir. Tanrısal düzen ile şeytanın ini arasında, biz ve öteki arasında, id ile süper ego arasında kültürel olarak inşa edilmiş sınırları ihlal eden internetin söz konusu temsilleri muhafazakar bir teknoloji karşıtlığını beslemektedir. Arkaik mitlerde de sıklıkla tekrar edilen söz konusu anlatı kalıbı, 'Dabbe'[4], 'Host'[5] ve Friend Request gibi filmlerde aynı zamanda öteki olandan ve 'tehlikeli yabancıdan' duyulan korkunun metaforik bir dışa vurumu olarak da okunabilir.

Tablo 2'de yer alan internet temelli bağımlılıklar (oyun, sosyal medya bağımlılıkları), siber suçlar (bknz. Disconnect), siber pornografi, bireyin gerçeklik algısının bozulması

(gerçek ile sanal olanı birbirinden ayırmanın zorlaşması) gibi diğer güvenlik tehditlerinin birer yan tema olarak işlendiği görülmektedir (bknz: U Want M 2 Kill Him?).

Tablo 2. *Filmlerde Güvenlik Tehdidi ve Faillerin Frekansı*

Güvenlik Tehdidi	**Fr.**	**Failler**	**Fr.**
Sanal Kimlikler ve Anonimlik	10	Psikopat ruhlu kişiler	8
Bireysel mahremiyetin ihlali	9	Siber zorbalar	5
Siber zorbalık ve İntihara sürükleme	8	Gerçek hayattan tanıdık kişiler	4
Devlet denetimi ve otorite eksikliği	7	Doğaüstü varlıklar	4
Sosyal İlişkilerin zayıflaması ve yalnızlaşma	6	Siber pornografi ve şiddet endüstrisi	3
Şiddetin Eğlence Unsuruna Dönüşmesi	5	Seri Katiller	3
İnternet temelli bağımlılıklar	4	Siber dolandırıcılar	2
Doğaüstü varlıkların insanları rahatsız etmesi	4	Sapkın cinsel eğilimlere sahip kişiler	2
Siber suçlar	3		
Siber pornografi	3		
Gerçeklik algısının bozulması	3		

Filmlerde güvenlik sorununu yaratan failler incelendiğinde ise bunların çoğunlukla rasyonel bir amacı veya maddi çıkarı olmaksızın, sadece haz, eğlence veya intikam gibi kişisel duygularını tatmin etmek için kötülük yapan psikopat ruhlu (veya sıra dışı ruh haline sahip) kişiler oldukları görülmektedir. (Siber pornografi ve siber şiddet endüstrisi veya siber dolandırıcılık gibi çıkar amaçlı suçlar görece daha nadirdir). Söz konusu kişiler, gerçekleştirdikleri siber zorbalık, cinayet gibi fiillerin sonucunda herhangi bir vicdan azabı ve sorumluluk duygusu hissetmemektedir. Tamamen irrasyonel saiklerle hareket ederler. Mağdurdan talep ettikleri hiçbir şey yoktur. Her an her yerdedirler ve her türlü güvenlik önlemine rağmen onlardan kurtulmanın bir yolu yoktur. Bilgisayarı ve yeni iletişim teknolojilerini bu fiilleri gerçekleştirmek adına çok etkin bir şekilde kullanmakta ve izlerini kolaylıkla kaybettirmektedirler. Siber güvenlikleştirme söyleminin dayanağı olan tehdidin her an ve her yerdeliği, öngörülemezliği, kontrol edilemezliği, rasyonel bir şekilde tanımlanamaz oluşu filmlerdeki faillerin resmediliş biçiminde de karşımıza çıkmaktadır. Unfriended, U Want Me 2 Kill Him?, Cyberbully, Untraceable, Girlhouse, Suicide Room, Chatroom gibi pek çok filmde bu tür amaçsız ve irrasyonel faillerle karşılaşmak mümkündür. Diğer taraftan faillerin büyük bir kısmının bireyin gerçek hayattan değil sanal ortamda tanıştığı kişiler olması çevrimiçi ilişkilere dair şüpheci bir yaklaşıma işret etmektedir.

Bu noktada vurgulanması gereken bir diğer husus ise filmlerin çoğunda failler ile mağdurlar arasında keskin sınırların bulunmayışıdır. Yani failler aynı zamanda mağdur, mağdurlar ise fail olabilmektedir. Örneğin Death Tube isimli filmde, mağdur karakterlerin tümü kurbanı oldukları şiddetin daha önceden izleyicisi olmuşlardır. Untraceable filmindeki seri katil, aynı zamanda babasını şiddete kurban vermiş bir mağdurdur ve intikam amacıyla cinayetler işlemektedir. İşlediği cinayetleri canlı olarak yayımlamakta ve izlenme sayısı arttıkça, kurbanlarını da daha hızlı şekilde öldürmektedir. Bu anlamda film, şiddeti pasif şekilde izlemenin de ahlaki bir sorun olduğuna ve kimsenin tam anlamıyla masum olmadığına dair bir toplumsal eleştiri getirmektedir. Unfriended örneğinde ise failin, siber zorbalık yoluyla genç bir kızın intiharına yol açan bir grup arkadaştan intikam aldığı görülmekte, siber alanda kimsenin dürüst ve masum olmadığına, ilişkilerin sahteliğine, çok yakın dostların bile birbirinin kuyusunu kazabildiğine dair mesajlar verilmektedir. Dolayısıyla filmler aracılığıyla kurulan siber güvenlikleştirici söylem, bireyi hem potansiyel mağdur hem de bizzat tehdidin kaynağı olarak çerçevelemektedir.

Güvenlik tehdidinden etkilenen mağdurlara, yani referans nesnelerine bakıldığında ise, ağırlıklı olarak genç/ergen kadınlar (benzer bir frekansta da erkekler) olduğu görülmektedir. Dolayısıyla gençlik ve gençlik alt kültürleri bir yandan güvenlik sorunu olarak ele alınırken, diğer yandan bu güvenlik tehditlerinden korunması gereken, savunmasız kurbanlar olarak resmedilmektedir. Filmlerdeki siber güvenlikleştirme söyleminin dayandığı referans nesnelerine dair dikkat çeken bir diğer öğe ise, bu gençlerin ağırlıklı olarak orta sınıf ailelere mensup olmasıdır. Kendilerini tutumluluk, saygınlık ve güvenlik gibi değerler çerçevesinde ahlaki ve ideolojik olarak var olan toplumsal sistemle bağlantılandıran orta sınıflar (Hall, Critcher, Jefferson, Clarke, & Roberts, 1982, s. 255), farklı türden ahlaki paniklere ve risk algısına en duyarlı toplumsal katmandır. Referans nesnesi olarak orta sınıfların tercih edilmesi, aynı zamanda farklı toplumsal katmanların da kendilerini güvenlikleştirici söylemle özdeşleştirebilmeleri açısından uygun bir zemin sağlar. Bu anlamda toplumun en temel birimi olarak ailenin ve aile değerlerinin/bütünlüğünün de önemli bir referans nesnesi olduğu görülebilir. Zira çevrimiçi ilişkilere kendisini adayan gençlerin giderek aileden ve aile ilişkilerinden de uzaklaşarak yalnızlaşması filmlerde sıkça tekrarlanan bir temadır.

Tablo 3. *Filmlerde Referans Nesnesi ve Güvenliği Sağlamakla Görevli Aktörlerin Frekansı*

Referans Nesnesi	**Fr.**	**Güvenliği Sağlamakla Görevli Aktörler**	**Fr.**
Kadın	11	Polis/Asker gibi kolluk kuvvetleri	10
Erkek	10	Mağdurların kendisi	7
Genç/Ergen	10	Bilgisayar ve IT konusunda uzman kişiler	5
Orta Sınıf	10	Akrabalar/aile bireyleri	4
Yetişkin/Orta Yaşlı	5	Spritüal Kişiler/Din adamları	2
Varlıklı	4	Yargı Kurumları	1
Yoksul	3		
Çocuk	1		

Filmlerde güvenlik sorununu tanımlamak, ele almak ve güvenlik tehdidini bertaraf etmekle sorumlu aktörlerin en başında polis/asker gibi silahlı kolluk kuvvetleri ve bunlara bağlı dedektifler, siber güvenlik uzmanları veya siber güvenlik birimleri gelmektedir. Ancak filmlerdeki genel bakış açısı, bu türden bürokrasiye ve katı hiyerarşiye dayalı geleneksel kurumların, hızlı, esnek ve dinamik yapıda olan internet kaynaklı tehditlerle baş etmek konusunda kaçınılmaz olarak yetersiz kalacağı yönündedir. Dolayısıyla filmlerde güvenlik tehdidinin ortadan kaldırılmasına yönelik genellikle kötümser bir bakış açısı hakimdir. Bu nedenle iki tanesi hariç ('Chatroom' ve 'U Want Me 2 Kill Him?') tüm filmlerde polisin güvenliği sağlamada yetersiz kaldığı görülmekte, hatta bizzat polisler cinayete kurban gitmektedir (Untraceable, The Den). Polisler genellikle güvenlik sorununun içeriğini, boyutunu, kaynağını ve aciliyetini kavramakta veya soruna etkin müdahalede geç kalmakta, bunları yaptığında ise iş işten geçmektedir.

Güvenlikleştirici söylemin temel dayanağı olan, aciliyet vurgusuna filmlerde sıklıkla rastlanmaktadır. Söz konusu vurgu, varoluşsal bir tehdit olarak tanımlanan konunun, hızlı bir şekilde, siyasetin ve normal prosedürlerin dışına çıkılarak ele alınmasını meşrulaştırır. Örneğin filmlerin neredeyse tamamında suç unsuru olabilecek fiiller (cinayet, intihara özendirme, çocuk pornografisi, siber zorbalık vs.) bulunmasına rağmen, bu konularda polis gücünü de yönlendiren temel yetkili merci olarak yargı kurumlarının devreye girdiği yalnızca bir film bulunmaktadır.[6] Sorunlar standart yargı prosedürlerinin dışına çıkılarak, doğrudan polis gücüyle ve olağanüstü yöntemlerle çözülmeye çalışılmaktadır. Zira tehdit viral olarak (yani hızı katlanarak) yayılmakta, kaybedilen her dakika yeni mağdurlar zarar

görmektedir. Örneğin Chatroom filminin finalinde sanal sohbet platformunu cisimleştiren metruk binaya özel harekat birlikleri tarafından ağır silahlarla baskın yapılmakta ve bir anlamda olağanüstü yöntemler kullanılarak güvenlik sağlanmaktadır.

Yargı kurumlarının ve asker/polis gücünün yetersiz kaldığı siber güvenlik sorunları karşısında, mağdurlar çoğunlukla kendi başının çaresine bakmak zorunda kalmaktadır (bknz: Unfriended, Dabbe, Host, Girlhouse, Friend Request, The Den, Death Tube). Adalet arayanlar ise, yine devlet olmadığı için bu adaleti kendi elleriyle sağlamak zorundadır (bknz: Girl House, Cyberbully, Untraceable). Bu durum, Rosewarne'in de işaret ettiği üzere, popüler kültür ürünlerinde siber alanın avcılar ve kurbanlardan müteşekkil bir 'vahşi Batı' metaforu çerçevesinde simgeleştirilmesinin bir örneğidir (Rosewarne, 2016, s. 41). Güvenliği sağlama rolü mağdurların yanında, onun tanıdığı diğer kişilere de düşebilmektedir. Bu anlamda filmlerin önemli bir kısmında (Friend Request, Untraceable, Girlhouse, Chatroom, Unfriended) bilgisayar ve iletişim teknolojilerinden iyi anlayan ve güvenlik sorunu karşısında mağdura yardım eden bir karakter bulunur. Dolayısıyla siber güvenlik sorunlarıyla başa çıkmanın ancak teknik beceriyle ve uzmanlıkla mümkün olabileceğine yönelik bir mesaj verilmiş olur ve bu durum Hansen ve Nissenbaum'un 'Teknikleştirme' adı verdiği bağlama denk düşer. Tehdidin doğaüstü varlıklar olması durumunda ise, konunun uzmanları olarak medyumlar (bknz. Host) ve din adamları (bknz. Dabbe)[7] devreye girebilmektedir.

Polis gücü, teknik uzmanlar ve mağdurların bizzat kendisinin dışında, güvenlik tehdidini ortadan kaldırmak adına sorumluluğa davet edilen bir diğer önemli unsur ise ailelerdir. Filmlerde yer verilen siber güvenlikleştirici söylem, ailelerin çocuklarıyla yeterince ilgilenmediği, onların ihtiyaçlarını ve beklentilerini gözetmediği, onlarla yeterince iletişim kurmadığı durumlarda çocukların bu türden çevrimiçi tehditlere daha açık olacağını vurgulamaktadır. Bu anlamda filmler ailelere yönelik olarak çocuklarıyla iletişim halinde olmaları, onların çevrimiçi ve çevrimdışı yaşamlarını denetim altına almaları yönünde açık veya örtük mesajlar vermektedir. Örnekleme dahil edilen filmlerin altısında, ailesi tarafından yeterli düzeyde ilgi görmeyen veya aile ilişkileri sorunlu olan en az bir çocuk veya genç karakter bulunmaktadır. Özellikle kendi kariyerleriyle meşgul oldukları için çocuklarıyla yeterli düzeyde ilgilenemeyen anne-babaların[8] eleştirisini (bknz. Disconnect, Suicide Room, Chatroom) yoğun bir şekilde görmek mümkündür. Ayrıca gençlere ise, sanal ilişkilere değil, yalnızca ailelerine güvenebilecekleri mesajı verilmektedir (bknz: Cyberbully). Dolayısıyla filmlerde, sorumluluğun kurumsal aktörlerden ziyade, bireylere, uzman kişilere ve ailelere yüklendiği görülmektedir.

Sonuç

Filmler internetin tamamıyla kontrolsüz biçimde kötüye kullanıldığı durumda bireylerin ve toplumların başına nelerin gelebileceğine dair hipotetik felaket senaryoları üretmektedir. Üretilen bu senaryolardaki ortak temalara bakıldığında, internetin her türlü kontrol ve denetimden azade tehlikeli ve kuralsız bir alan olarak sunulduğu, internet aracılığıyla tehdit unsurlarının kılık değiştirerek gündelik hayatın içerisine kadar sızabildiği ve kişisel mahremiyetin ihlal edildiği yolundaki argümanların öne çıktığı görülmektedir. Dolayısıyla üretilen felaket senaryolarının internetin yalnızca fiziksel-maddi boyutundan kaynaklanmadığı, hali hazırda var olan korkuların (tehlikeli yabancıdan ve öteki olandan duyulan korku) internetin sunduğu yeni alanda tekrar filizlendiği söylenebilir (Furedi, 2017, s. 66). Öte yandan gençlerin siber güvenlik söyleminin en temel referans nesnesi olduğu ve bu anlamda internetin yol açabileceği güvenlik riskleri karşısında toplumdaki en savunmasız kesimlerin başında geldiği

görülmektedir. Ayrıca filmlerin siber güvenlik sorunlarının çözümüne yönelik karamsar bir bakış açısı ortaya koyduğu ve bu yönüyle toplumda güvenlik paranoyasını, korkuyu ve ahlaki paniği kışkırtan bir anlatım tarzı benimsediği görülmektedir. İnternetin yol açtığı güvenlik sorunlarının üstesinden gelinebilmesi için devletin geleneksel güvenlik bürokrasisinin ve prosedürlerinin yetersiz ve etkisiz kalacağı, daha hızlı ve esnek şekilde hareket edebilen uzman kişilerin sorumluluk alması gerektiği savunulmaktadır. Öte yandan çevrimiçi güvenliğin sağlanabilmesi için bireylerin kendisine ve aileye de önemli roller düşmektedir. Dolayısıyla Hansen ve Nissenbaum'un siber güvenlik söyleminin modelleri olarak tanımladığı hipergüvenlikleştirme, gündelik güvenlik pratikleri ve teknikleştirmenin filmlerde iç içe geçtiği görülmektedir. Öte yandan güvenlikleştirme söyleminin temel dayanağı olan tehdide karşı –politik tartışmayı, temel yurttaş haklarını ve standart kuralları göz ardı etmek pahasına da olsa- hızlı bir şekilde harekete geçilmesi gerektiğine yönelik vurgu da filmlerde yoğun bir şekilde işlenmektedir.

Araştırmanın aynı zamanda önemli bir takım sınırlılıkları bulunmaktadır; Bunlardan en önemlisi siber güvenliğin özellikle bireysel ve toplumsal boyutuna odaklanması, ulusal ve uluslararası güvenlik veya devlet güvenliği boyutunun konunun dışında tutulmasıdır[9]. Dolayısıyla konunun bu ikinci boyutunu ele alan filmleri incelemek üzere yeni araştırmalar yapılabilir. Diğer taraftan popüler siber güvenlikleştirme söyleminin, toplumdaki internete yönelik tehdit algısını nasıl etkilediği, siyasal karar süreçlerine, alandaki karar alıcıların, uzman ve elitlerin yaklaşımlarına hangi bağlamlarda nüfuz ettiği gibi önemli sorulara cevap arayan yeni araştırmalar yapılabilir.

İkinci sınırlılık ise, araştırmanın korku ve gerilim filmlerinde siber güvenlikleştirme söyleminin nasıl inşa edildiğine odaklanmakla birlikte, ele alınan söylemlerin ne derece nesnel ve tutarlı bir temele dayandığı sorusunu dışarıda bırakmasıdır. Postyapısalcı bir perspektiften hareket eden ve dolayısıyla her türlü söylemsel edimin en nihayetinde gerçekliği yeniden kurgulanması olarak gören Hansen ve Nissenbaum'a göre, bir tehdidin abartıldığını veya gerçek dışı olduğunu savunmak, aynı zamanda gerçek bir tehdidin var olduğunu savunmak anlamına geleceğinden anlamsızdır. Ancak kuramcıların savunduğu bu radikal görelilik anlayışı da eleştiriye açıktır. Zira siber güvenlikle ilişkili uluslararası veya ulusal kurum/kuruluşlar tarafından üretilen çeşitli istatistiksel verilerden yararlanarak ya da eleştirel çözümlemeye dayanarak popüler medya içeriklerinde dolaşıma sokulan internet ve siber alanla ilgili kalıplaşmış temsillerin, korkuların ve felaket senaryolarının zemini ve dayandığı ideolojik saikler sorgulanabilir (ve tabi ki bu türden araştırmalara da ihtiyaç vardır).

Örneğin Paker, çağdaş bireyin evinin, kendisinin ve hatta ülkesinin güvenliğini sağlayabilmek için bu kadar çok imkan, fırsat ve ürün ile karşı karşıya olduğu bir çağda, tehdidin öngörülemezliğine, bilinemezliğine ve tam olarak kontrol altına alınamaz oluşuna dair popüler mitlerin bu derece yaygınlaşmasının ve güvenlik paranoyasının tüm kamusal hayatın temel belirleyici ilkesi haline gelmesinin yarattığı paradoksun nedenini anlamaya çalışır. Bu durumu ise "güvenlik alanındaki somut tehditlerin artmasından ziyade güvenlik piyasasının kapitalist pazar ilişkilerine entegre olması süreciyle" ve bu sürece eşlik eden yeni güvenlik söylemiyle ilişkilendirir (2009, s. 205). Bu bağlamda, devletin güvenlik bürokrasinin yetersizliğine vurgu yaparak siber güvenliği bireylere ve uzmanlara tahvil eden bu türden popüler mitlerin, neoliberal kapitalist devletlerde giderek yükselen siber güvenlik endüstrisinin çıkarlarıyla doğrudan paralellik taşıması tesadüf değildir. Diğer yandan, çevrimdışı alanda da vuku bulabilen çocuk istismarı, şiddet, dolandırıcılık gibi pek çok suçun internet ile özdeşleştiren siber güvenlikleştirme

söylemi, internet erişimini ve içeriğini rejim çıkarları çerçevesinde denetim altına almayı amaçlayan otoriter devletler açısından oldukça kullanışlı bir söylemsel cephanelik sunar. Bu türden devletler 'çocukları ve gençleri zararlı içeriklerden korumak', 'ulusal değerlerin ve ailenin korunması', 'genel ahlak' veya 'müstehcenlik' gibi muğlak ifadeler üzerinden uluslararası enformasyon dolaşımının, yurttaşların bilgiye erişiminin, ifade özgürlüğünün, kişisel verilerin gizliliğinin ihlali veya muhafazakar ve patriarkal değerlerin dayatılması anlamına gelebilecek yasaların ve idari yaptırımların hayata geçirilmesini meşrulaştırırlar (Bedir, 2020, s. 329). Korku, toplumdaki egemenlik ilişkilerinin yeniden üretilmesi için uygun bir ideolojik araçtır. "Sistem bireye, onu korkusundan kurtaracağı vaadini aşıladığı oranda, birey duygusal ve varoluş koşulları bakımından sisteme daha bağlı hale gelir" (Duhm, 1996, s. 204).

Korku ve gerilim filmlerinde üretilen siber güvenlikleştirici söylemin eleştirisi, internet aracılığıyla işlenen suçlar veya ortaya çıkabilecek bireysel ve toplumsal risklerin kamusal tartışmaların konusu olmasının önemini ve gerekliliğini yadsımak anlamına gelmemelidir. Ancak Oskay'ın 'çağdaş fantazyalar' olarak tanımladığı bilim kurgu ve korku sineması, "çağdaş toplumsal ve beşeri sorunlardan bilim ve teknolojiyi sorumlu göstererek bu sorunların gerçekliğini gitgide daha çok bulandırmakta ve insanın dış gerçekliğini mistifiye etmektedir" (Oskay, 1994, s. 80). Bu nedenle sorunların temelinde yatan siyasal, ekonomik ve sosyo-kültürel etkenler görünmez hale gelebilmektedir. Bu anlamda medyanın, siyasal karar alıcıların, uzmanların ve akademinin bu konulara dair toplumla etkileşime geçerken, meseleleri güvenlik dışı bir bağlamda ve siyaset alanı içerisinde ele almaları, toplumsal paranoyayı tetikleyecek abartılı söylemlerden ve stereotiplerden kaçınmaları önem arz etmektedir. Meseleye dair çözüm önerileri geliştirilirken, özgürlük ve güvenlik dengesinin gözetilmesi, gerek otoriter ideolojiler, gerekse de güvenlik endüstrisi açısından kullanışlı söylemler üretmekten imtina edilmesi ve çok boyutlu bir kamusal müzakereye alan açılması gerekmektedir.

Notlar

1 Araştırma, her biri tek bir filmden sorumlu olan 13 kişilik bir proje ekibi ve bir proje yöneticisi tarafından gerçekleştirilmiştir. 13 Kişilik araştırma ekibi arasında ortak bakış açısı oluşturulabilmesini sağlamak maksadıyla projenin amacı, yöntemi ve kuramsal çerçevesinin yanında, kodlama işleminin nasıl gerçekleştirileceği ekibe ayrıntılarıyla aktarılmıştır. Öte yandan her bir film özelinde elde edilen bulgular tartışılmıştır.

2 Araştırma kapsamında incelenen 13 filmin 7'sinde güvenliği sağlama görevini üstlenen kişilerin başarısız olduğu, mağdurların kurtarılamadığı ve güvenlik sorununun devam ettiği görülmektedir. Filmlerden 4 tanesinde ise söz konusu aktörlerin kısmen başarılı olduğu, yani mağdurlar kurtarılsa da faillerin bulunamadığı, failler bulunsa da güvenlik sorununun devam ettiği veya güvenlik sağlanana kadar failler hedefledikleri zararı zaten yarattığı görülmektedir. Geriye kalan 2 filmde ise güvenliği sağlamakla görevli kişiler tam anlamıyla başarı sağlamaktadır.

3 Örneğin Chatroom isimli filmde ağırlıklı olarak gençlerin kullandığı sanal sohbet odası, metruk bir bina olarak temsil edilmiştir. Binanın odalarına şifre ile girilmekte ve her bir odada pedofililer, siber zorbalar, intihara yönlendirenler, dolandırıcılık, yasa dışı bahis gibi kriminal faaliyetlere bulaşmış kişiler ve her türlü 'sapkın' gençlik alt kültürü cirit atmaktadır. Bu türden bir tasvir, siber alana (ve bir anlamda gençlik alt kültürlerine) yönelik olarak toplumda ahlaki paniği körükleme ve devletin bu alana hızlı ve etkin şekilde müdahil olması gerektiği yönünde hipergüvenlikleştirici söylem biçiminin yansımasıdır.

4 Dabbe filminde İnternet bir kıyamet alameti olarak tanımlanmaktadır. Dabbe isimli bu ağ sayesinde, cinlerin yaşadığı boyut ile insanların yaşadığı boyut arasındaki perde ortadan kalkmıştır. Cinler insanların akıllarını kaybetmelerine ve intihar etmelerine neden olmaktadır. Öte yandan 'cin' etimolojik kökeni itibariyle görünmeyen ve bize yabancı olan varlıkların genel ismidir (Düzgün, 2012, s. 12). Dabbe aynı zamanda Japonya yapımı Kairo ve ABD yapımı Pulse isimli filmlerinin Türkiye uyarlamasıdır. Dolayısıyla benzer temaların örnekleme dahil olmayan bu filmlerde de tekrar edildiği söylenebilir.

5 Host filminde ise bir grup arkadaş, pandemi döneminde zoom isimli görüntülü sohbet uygulaması üzerinden ruh çağırma seansı gerçekleştirmektedir. Ancak gruptaki kişilerden birinin durumu alaya alması ruhları kızdırmış ve olaylar kontrolden çıkmıştır. Ruhlar ağ üzerinden viral olarak yayılarak arkadaş grubunu ağır bir şekilde cezalandırmıştır. Filmde ruhları kızdıran

kişinin bir Çinli olması da bir tesadüf değildir. ABD'de aşırı sağ siyasetin pandemiden dolayı Çin'i sorumlu göstermesi (hatta Donald Turmp'ın COVID-19 virüsünü 'Çin virüsü' olarak isimlendirmesi) ile filmde kötü ruhların gazabından bir Çinlinin sorumlu olması arasında kayda değer bir paralellik vardır. Dolayısıyla filmde 'yabancı düşmanlığının' kötü ruhlar metaforunun arkasına gizlendiği söylenebilir.

6 Yalnızca 'U Want Me 2 Kill Him?' isimli filmde yargı kurumlarının devreye girdiği görülür. Bunun aynı zamanda, örneklemeler arasında yaşanmış bir olaydan esinlenerek senaryolaştırılan tek film olması önemlidir.

7 Dabbe filminde ülkede ve dünyada salgın gibi yayılan şüpheli intiharları araştırmakla görevlendirilen polis Komiseri, başlangıçta olayın virüs yoluyla bilgisayarları ele geçirerek insanları intihara yönlendiren sapkın bir grubun işi olduğu görüşündedir. Ancak din adamı olduğu düşünülen biri, Kuran'dan alıntı yaparak olayların internet ağı üzerinden insanlara musallat olan cinler tarafından gerçekleştirildiği ve kıyametin yakın olduğu düşüncesini öne sürer. Din adamının düşüncesi filmin devamında doğru çıksa da şarlatan muamelesi görüp akıl hastanesine kapatılmaktan kurtulamaz. Bu bağlamda geleneksel güvenlik önlemlerinin olduğu gibi, rasyonel akıl yürütmenin de internetin yaratabileceği tehditler karşısında çaresiz kaldığı görülmektedir.

8 Bazı filmlerde babanın kariyerist bir karakter olması sorun yaratmazken, annenin çalışıyor olması ve mesleğine yoğunlaşması çocuğun tehlike altında olmasının en önemli nedeni olarak görülmektedir. Söz konusu filmler çocukla ilgilenmeyi temelde annenin sorumluluğu olarak görmekte ve bu anlamda kalıplaşmış toplumsal cinsiyet rollerini örtük biçimde yeniden üretmektedir.

9 Siber güvenlik söz konusu olduğunda, güvenlikleştirmenin bu iki boyutu arasında keskin sınırlar çizmek mümkün değildir. Araştırmada bazı filmlerde siber güvenliğin ulusal, uluslararası güvenlik ve devlet güvenliği boyutuna örtük ya da dolaylı de olsa işaret edildiği görülmüştür. Bu durum Hansen ve Nissenbaum'un işaret ettiği üzere, siber güvenlik söylemlerinin, bireysel, kolektif ve siyasal referans nesnelerini birbiriyle bağlantılandırdığı teziyle paralellik taşır (2009, s. 1163).

Kaynakça

Aziz, A. (2017). *Sosyal Bilimlerde Araştırma Yöntemleri ve Teknikleri.* Ankara: Nobel Yay.

Baysal, B., & Lüleci, Ç. (2015). Kopenhag Okulu ve Güvenlikleştirme Teorisi. *Güvenlik Stratejileri Dergisi, 11*(22), 61-95.

Bedir, U. (2014). Haneke Sinemasında Hazzın Engellenmesi. N. T. Cheviron içinde, *Haneke Huzursuz Seyirler Diler* (s. 103-135). İstanbul: Ekslibris Yay.

Bedir, U. (2020). Güvenlikleştirme Teorisi Bağlamında İnternette Devlet Denetiminin Meşrulaştırmas. M. C. Sadakoğlu, E. Arğın, & E. G. Erol içinde, *Dijital Kültür ve Sosyal medya Okumaları* (s. 306-335). İstanbul: Hiper Yayın.

Bendrath, R. (2001). The cyberwar debate: Perception and politics in US critical infrastructure protection. *Special Issue of Information & Securityl*(65), 80–103.

Buzan, B., & Hansen, L. (2009). *Evolution of International Security Studies.* New York: Cambridge University Press.

Buzan, B., Waever, O., & Wilde, J. d. (1998). *Security: A New Framework for Analysis.* Boulder: Lynne Rienner Pub.

Cavelty, M. D. (2008). Cyber-terror—looming threat or phantom menace? The framing of the US cyber-threat debate. *Journal of Information Technology & Politics, 4*(1), 19–36.

Cavelty, M. D. (2010). Cyber-security. J. P. Burgess içinde, *The routledge handbook of new security studies* (s. 154-162). New York: Routledge.

Cavelty, M. D. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review, 15*(1), 105-122.

Cavelty, M. D. (2019). The materiality of cyberthreats: securitization logics in popular visual culture. *Critical Studies on Security, 7*(2), 138-151.

Cavelty, M. D., & Egloff, F. J. (2021). Hyper-Securitization, Everyday Security Practice and Technification: Cyber-Security Logics in Switzerland. *Swiss Political Science Review, 27*(1), 139-149.

Coşkun, B. B. (2012). Words, images, enemies: Macro-securitization of the Islamic terror, popular TV drama and the war on terror. *Turkish Journal of Politics, 3*(1), 37-51.

Diebert, R. J. (2002). Circuits of power: Security in the internet environment. J. N. Rosenau, & b. P. Singh içinde, *Information technologies and global politics : the changing scope of power and governance* (s. 115-142). New York: State University of New York Press.

Duhm, D. (1996). *Kapitalizmde Korku.* (S. Şölçün, Çev.) Ankara: Ayraç Yay.

Düzgün, Ş. (2012). Dinsel ve Mitolojik Yönleriyle Cin ve Şeytan Algımız. *Kelam Araştırmaları, 10*(2), 11-30.

Eriksson, J. (2002). Cyberplagues, IT, and security: Threat politics in the information age. *Journal of Contingencies and Crisis Management, 9*(4), 211–222.

Furedi, F. (2017). *Korku Kültürü: Risk Almamanın Riskleri.* İstanbul: Ayrıntı Yay.

Gessler, H. A. (2017). Securitizing the Internet: The case of Turkey. *Central and Eastern European eDem and eGov Days*(325), 295-304.

Gorr, D., & Schünemann, W. J. (2013). Creating a secure cyberspace–Securitization in Internet governance discourses and dispositives in Germany and Russia. *The International Review of Information Ethics*(20), 37-51.

Hall, S., Critcher, C., Jefferson, T., Clarke, J., & Roberts, B. (1982). *Policing the crisis: Mugging, the state and law and order.* Hong Kong: The Macmillan Press.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly, 53*(4), 1155–1175.

Hart, C. E. (2012). *Securing Freedom: A media framing analysis of cybersecuritization (Doctoral dissertation).* Fraser University: Communication, Art & Technology: School of Communication.

Hill, J., & Marion, N. E. (2017). The Use of Mythic Narratives in Presidential Rhetoric on Cybercrime. *Journal of Qualitative Criminal Justice & Criminology, 6*(2).

Jantunen, S., & Huhtinen, A.-M. (2011). A Case-Study on American Perspectives on Cyber and Security. *European Conference on Cyber Warfare and Security,* (s. 163). Academic Conferences International Limited.

Kallender, P., & Hughes, C. W. (2017). Japan's emerging trajectory as a 'cyber power': From securitization to militarization of cyberspace. *Journal of Strategic Studies, 40*(1), 118-145.

Kasper, A. (2014). The fragmented securitization of cyber threats. T. Kerikmäe içinde, *Regulating eTechnologies in the European Union: Normative Realities and Trends* (s. 157-187). Cham.: Springer.

Lawson, S. (2013). Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats. *Journal of Information Technology & Politics, 10*(1), 86-103.

Lawson, S., & Middleton, M. K. (2019). Cyber Pearl Harbor: Analogy, fear, and the framing of cyber security threats in the United States, 1991-2016. *First Monday, 24*(3).

Lobato, L. C., & Kenkel, K. M. (2015). Discourses of cyberspace securitization in Brazil and in the United States. *Revista Brasileira de Política Internacional, 58*(2), 23-43.

Maertens, L. (2015). Securitization in Pop Culture: the Environmental Threat According to Hollywood. *Convention Annuelle de l'International Studies Association (ISA).* La Nouvelle Orléans (USA).

Oskay, Ü. (1994). *Popüler Kültür Açısından Çağdaş Fantazya: Bilim-Kurgu ve Korku Sineması.* İstanbul: Der Yayınları.

Paker, E. B. (2009). Güvenlik endüstrisi ve güven(siz)liğin inşası: Bir toplumsal paranoyayı anlamak. *Toplum ve Bilim*(115), 204-225.

Rosewarne, L. (2016). Cinema and cyberphobia: Internet tropes in film and television. *Journal of Telecommunications and the Digital Economy, 4*(1), 36-53.

Sandywell, B. (2006). Monsters in cyberspace cyberphobia and cultural panic in the information age, Information. *Community and Society, 9*(1), 39-61.

Shad, M. R. (2019). Cyber threat landscape and readiness challenge of Pakistan. *Strategic Studies, 39*(1), 1-19.

Shires, J. (2020). Cyber-noir: Cybersecurity and popular culture. *Contemporary Security Policy, 41*(1), 82-107.

Viganò, L. (2020). Explaining Cybersecurity with Films and the Arts. *In Imagine Math 7*, 297-309.

Virgy, M. A., Destianira, C., & Mustofa, M. U. (2020). Social Media Shutdown: A Political and Cyber Securitization of Indonesia's 2019 Presidential Election. *Jurnal Studi Diplomasi Dan Keamanan, 12*(2).

Waever, O. (1995). Securitization and Desecuritization. R. D. Lipschutz içinde, *On Security* (s. 7). New York: Columbia University Press.

Yau, H.-m. (2020). Framing Cyber Security in Taiwan: A Perspective of Discursive Knowledge Production. *Korean journal of defense analysis, 32*(3), 457-474.

Cyber Securitization Discourse in Cinema: Analysis of Popular Horror and Thriller Movies Related to The Internet

Umur BEDİR (Asst. Prof. Dr.)

Extended Abstract

The research focuses on the securitization theory developed by Ole Weaver, one of the Copenhagen School theorists, to describe the new security paradigm that emerged after the cold war. Unlike the traditional security approach, securitization theory takes a constructivist approach to security. According to this theory, there is no clear cut definition of security threat arising from absolute and concrete reality. What constitutes a security threat is 'constructed' politically and intersubjectively and through the speech act. Accordingly, subjects framed as security issues fall outside the realm of normal politics and public debate and excessive measures to be taken by governments would be legitimized. Securitization theorists normatively argue that problems framed as security issues should be 'desecuritized' and negotiated within the normal politics. In this respect, the theory creates a suitable ground for critical approaches to existing security discourses. On the other hand, securitization analysis provides various concept and analytical tools to understand how the securitization process (the process of constructing an issue as a security issue) is works and results. Securitization analysis is concerned with how all elements of securitization process, such as 'securitizers', 'security problems/ threat', 'referent objects', 'functional actors' are positioned within a spesific discourse.

Copenhagen school theorists have also taken security beyond the field of military security and examined it through different 'sectors' such as political security, economic security, social security and environmental security. Each of these sectors has characteristic features in terms of threat perceptions and reference objects. Especially after the 1990s, the importance of the internet and information technologies in economic, political, cultural and social life has made cyber security a separate sector that affect the functioning of economy or governments and also everyday life. Cyber security is a concept that includes threats created by or through cyberspace, and practices processes to eliminate or mitigate these threats. Hansen and Nissenbaum have identified the unique characteristics of the cyber security sector in terms of the forms of securitization and the grammar they use that link reference objects, threats, and securitizing actors. According to them, cyber security is shaped within the framework of three discursive modes, which they define as 'hypersecuritization', 'everyday security practices' and 'techification'.

The main purpose of this research is to explore and interpret the common themes of how and in which contexts the internet is constructed as a security problem in popular horror and thriller movies within the framework of securitization theory and Hansen & Nissenbaum's approach. In this context, 13 horror and thriller movies from different countries, especially the USA, focusing on the individual and social risks of the internet, were analyzed by using the content analysis method. The films were evaluated and coded in the context of the following categories, and the findings were interpreted within the framework of the securitization theory;

- What are the security threats associated with the internet and social media? (Security Problems)

- Who/what are the perpetrators of the security threat?
- What are the people or things that need to be protected from a security threat? (Referent Objects)
- What/who are the persons/institutions that undertake the task of dealing with the security problem? (Securitizing actors)
- How the securitization processes are resulted?

This study shows that, on movies, the internet is presented as a dangerous and lawless area free from any control and supervision. According to such hypothetical disaster scenarios, the anonymity feature of the internet causes threats such as violation of personnel privacy and infiltration of dangerous strangers into daily life by disguising. Online security risks are inherently unpredictable, unpreventable, and irrational, so traditional security bureaucracy and institutions are incapable of dealing with them. On the other hand, young people are the basic referent object of the cyber security discourse and in this sense, they are depicted as the most vulnerable segments in the society against the security risks that the internet may cause. The films also strongly emphasize the need for immediate action by the state, experts, individuals and/or family to control the cyberspace. It can be seen that hypersecuritization, everyday security practices and technification, which Hansen and Nissenbaum defined as three modes of cyber security discourse are intertwined in those films.

This research is important because it is one of the few studies that examines the cyber securitization discourse in popular culture products and movies based on systematic data collection. The limitation of the research is that it focuses on the individual and social aspects of cyber security and excludes the national and international security or state security aspects.

Keywords: Communication Sciences, Cyber Securitization, Securitization Discourse, Internet, Horror Movies.

Bu makale **intihal tespit yazılımlarıyla** taranmıştır. İntihal tespit edilmemiştir.

This article has been scanned by **plagiarism detection softwares.** No plagiarism detected.

Bu çalışmada **"Yükseköğretim Kurumları Bilimsel Araştırma ve Yayın Etiği Yönergesi"** kapsamında uyulması belirtilen kurallara uyulmuştur.

In this study, the rules stated in the **"Higher Education Institutions Scientific Research and Publication Ethics Directive"** were followed.

Araştırma tek bir yazar tarafından yürütülmüştür.

The research was conducted by a single author.

Bu araştırma İstanbul Aydın Üniversitesi, İletişim Fakültesinde, 'Dijital İletişim Araştırmaları ve Çalışmaları' isimli 4. Sınıf Onur Dersi kapsamında, bir uygulama projesi olarak gerçekleştirilmiştir. Araştırmanın verilerinin toplanması, yorumlanması ve analiz aşamaları, dersin öğretim üyesinin yönetiminde Ayşenur Karasu, Batuhan Çulhaoğlu, Gizem Karakaya, Melih Emre Nalbant, Muhammet İpek, Mücessem Çıkıkcı, Semanur Şentürk, Semih Demir, Sevgi Salman, Tamer Cingöz, Yusuf Ulvi Karademir ve Zeynep Aydın isimli öğrencilerin katkılarıyla gerçekleştirilmiştir. Bu kapsamda araştırmanın çalışmaya katkı sağlayan isimlerle **çıkar ilişkisi** bulunmaktadır.

This research was conducted as an application project in Istanbul Aydın University, Faculty of Communication, within the scope of 4th Year Honor Course "Digital Communication Research and Studies". The data collection, interpretation and analysis stages of the research was made by the contributions of students Ayşenur Karasu, Batuhan Çulhaoğlu, Gizem Karakaya, Melih Emre Nalbant, Muhammet İpek, Mücessem Çıkıkcı, Semanur Şentürk, Semih Demir, Sevgi Salman, Tamer Cingöz, Yusuf Ulvi Karademir and Zeynep Aydın under the observation of the lecturer for the related course. In this context, the research has a **conflict of interest** among the names who contributed to the study.