Türkiye İletişim Araştırmaları Dergisi • Yıl/Year: 2018 • Sayı/Issue: 31 ss/pp. 103-120 • ISSN: 2630-6220
DOI: 10.17829/turcom.415025

"Şebekeleşmiş Otoriteryanizm" ya da Otoriter Rejimlerin Siber Alanla İlişkisi: Rusya ve Çin Üzerine Bir Literatür İncelemesi

"Networked Authoritarianism" or The Relation of Authoritarian Regimes and Cyber Space: A Literature Review on Russia and China

Mustafa Cem OĞUZ*

Öz

Bu makalenin amacı otoriter rejimlerin siber alanla ilişkisini, Çin ve Rusya örnekleri üzerinden incelemektir. Bilindiği üzere bilişim teknolojilerinin ve özellikle internetin yaygınlaşması ile otoriter rejimlerin demokratikleşeceği ve şeffaflık kazanacağı 1990'larda güçlü bir beklentiydi. Buna göre internet bir Truva atı gibi kapalı rejimlerin içine girecek ve burada toplumsal muhalefetin sesi olarak rejimlerin dönüşümünü sağlayacaktı. Ancak 2000'li yılların ortalarından itibaren otoriter rejimlerin bilişim teknolojileri karşısında zayıflamadığı ve hatta dünya ölçeğinde yaygınlık kazandığı gözlemlendi. Bu başarının ardında otoriter rejimlerin ve özellikle Çin ile Rusya'nın internetle girdikleri yeni ilişki formu vardı. "Şebekeleşmiş Otoriteryanizm" (Networked Authoritarianism) olarak adlandırılan bu olguda bu iki ülke, interneti yasaklamamakta ve fakat ona uyum sağlamaktadırlar. İnternet üzerinde örgütlenen demokratik muhalefete karşı aynı platformdan karşıt söylem oluşturup, onunla rekabet etmektedirler. Otoriter rejim yine internet üzerinden kontrollü bir kamusallık yaratarak, toplumun rejimle iletişime girmesine imkan vermekte ve böylece muhalefetin genişlemesini engellemektedir. Neticede internet, otoriter rejimleri içeriden yıkan bir silah değil, onu pekiştiren ve istikrar kazandıran bir niteliğe kavuşmaktadır.

Anahtar Kelimeler: Şebekeleşmiş Otoriteryanizm, Veri Yerelleştirme, Suni Kitle, İnternet, Otoriter Rejimler

Abstract

The aim of this study is to examine the relationship of cyber zone and authoritarian regimes through the cases of China and Russia. It was a big expectation at 1990s that via the widespread use of ICT and especially internet, authoritarian regimes would become democratized and transparent. According to that

* Dr. Öğr. Üye., Niğde Ömer Halisdemir Üniversitesi, İktisadi İdari Bilimler Fakültesi, Niğde, Türkiye, oguzmustafacem@gmail.com, Orcid ID: 0000-0003-3968-350X.

Başvuru Tarihi: 13.04.2018 **Kabul Tarihi:** 06.07.2018

expectation, internet would penetrate to authoritarian state like a Trojan horse and would be the sound of the democratic opposition in there, then facilitate the transforming of the regime. However, from the middle of the 2000s, it was observed that authoritarian regimes did not weaken against information technologies, and even spread across the world scale. Reason of this success was the new relation form that adopted by these regimes, especially Russia and China, against internet. In this new form, called "Networked Authoritarianism", the regimes do not prohibit the internet, but are in compliance with it. They compete with opposition who use the internet as a democratic tool via internet by create counter discourses. Beside these, the states who adopt the networked authoritarianism, create a safe public space via the internet and facilitate the communication of state and public. Through this pseudo communication it prevents the growth of social opposition. After all, it can be concluded that the internet became not a tool that demolishes the authoritarian state from inside, but it consolidates and give strength to it.

Keywords: Networked Authoritarianism, Data Localization, Astroturfing, Internet, Authoritarian Regimes.

Giriş

Portekiz'in 1974'teki Kadife Devrimi'nden bu yana otoriter rejimlerin sonunun geleceği ve her birinin yerini demokratik rejimlerin alacağı genel bir iyimserlik ile bekleniyordu. 1990'ların başında bu iyimserlik artmakla birlikte 2000'lerle birlikte demokratikleşen ülke sayısının beklentinin çok altında kaldığı görüldü. Yüze yakın ülkeden sadece yirmi kadarı demokratikleşirken, büyük çoğunluğu ise ne demokrasi ne de diktatörlük olarak tanımlanamayacak "gri bölgede" kaldı (Carothers, 2002, s.7). Günümüzde açık diktatöryel rejim sayısı azalmakla birlikte, demokrasinin şekilsel şartlarını taşıyan ve fakat özsel şartlarından uzak olan bir dizi melez rejim (*hybrid regime*) ortaya çıktı. Hem uluslararası toplumun, hem piyasaların, hem de iç kamuoyunun nezdinde meşru bir rejim olma ya da en azından meşru görünme ihtiyacı ile şekillenen bu rejimler, siber alanla girdikleri ilişkide de geleneksel otoriter rejimlerden farklı davrandılar. Geleneksel otoriter rejimler vatandaşların kendi denetimlerinin dışında bir iletişim ve örgütlenme imkanına kavuşmalarına izin vermezken, bu yeni rejimler sansürün ve baskının yerine yöntemler geliştirmektedirler. Literatürde "şebekeleşmiş otoriteryanizm" (*networked authoritarianism*) olarak adlandırılan bu olguda ülkeler muhalif sesleri bastırmamakta, onlarla rekabet etmekte ve yine internet üzerinden kontrollü bir kamusallık yaratarak, muhalefetin genişlemesini engellemektedir. Biz bu çalışmamızda bu kavramı ve kavramın vaaz ettiği kurum ve yöntemleri Çin ve Rusya örnekleri üzerinden ele alacağız. Hipotezimiz, bu iki ülkenin de siber alanı salt bastırma/susturma yöntemleri ile değil, onun içinde örgütlenerek, onun sunduğu imkanlarla kontrol ettiği ve bu şekilde Türkmenistan, Kırgızistan, İran ve Kuzey Kore gibi internet karşısında geleneksel otoriter rejim refleksleri gösteren ülke örneklerinden farklılaştıklarıdır. Çalışma, bu hedef doğrultusunda önce otoriter rejimlerin interneti kontrol etmek için benimsedikleri yöntemleri analiz edecek, bu yöntemlerden şebekeleşmiş otoriter rejim kavramına ulaştıktan sonra bu kavram etrafında Çin ve Rusya deneyimlerini tartışacaktır.

Bilişim Teknolojileri ve Demokrasi: Beklentiler Gerçeklere Karşı

Teknolojik gelişimin demokratik hayat ve kurumları da olumlu etkileyeceği uzun süredir destek bulan bir varsayımdır. Özellikle teknolojinin bilişim alanında getireceği yeniliklerin karar alma süreçlerine daha aktif bir katılımı sağlayacağı genel bir beklenti haline gelmiştir (Hague ve Loader, 1999). Gerçekten de, bilişim (*information and communication technologies-ICT*) alanındaki gelişmelerin tüm siyasal ve toplumsal kurumları dönüştürdüğü ve birçok alanda da insan/birey merkezli, özgürlükçü ve katılımcı yeni bir hayatı öne çıkardığı görülmektedir. ICT'nin hem bilgi sağlama hem de süreçlere katılımı artırma yönünde sunduğu imkanlar gün be gün artmaktadır. Öyle ki, 1980'lerden itibaren bu teknolojinin gelişimi ile birlikte zamanla klasik demokratik seçim yöntemlerinin dönüşeceği ve hatta temsili demokrasi yerine doğrudan demokrasinin öne çıkacağı beklentisi yaygınlaşmıştır (Becker, 1981; Morris, 2000). Temsil edilen ile temsil kurumu arasındaki mesafeyi ortadan kaldırması beklenen bu yeni fenomene de ilgili literatürde elektronik demokrasi (*e-demokrasi*), dijital demokrasi, siber demokrasi, teledemokrasi gibi isimler uygun görülmüştür (Becker, 1981). Ted Becker (1981) teledemokrasi kavramını şu şekilde tanımlar: "Teledemokrasi –elektronik tabanlı, hızlı, iki yönlü iletişim– oy verenlerin siyasi konularda bilgi almasını sağlar, önemli kararların tartışılmasını kolaylaştırır, oy verme işlemlerini hızlandırır ve hatta insanların kamusal meselelerde doğrudan oy kullanmasını sağlar" (s. 6).

Şüphesiz ki, ICT içinde en çok ön plana çıkan araç internettir. 2018 verilerine göre dünya nüfusunun %54'ü, Kuzey Amerika'nın %95'i ve Avrupa'nın %85'i internet kullanmaktadır ("World Internet Usage", 2017). Kullanan kişi sayısı ve kullanım alanının yaygınlığı dikkate alındığında internetin sahip olduğu gücün ne kadar etkili olduğu aşikardır. Bu haliyle internet toplumsal yaşamın tüm veçhelerini, düşünce sistemlerini, alışkanlıklarını ve geleneklerini değiştirecek bir kapasiteye sahiptir. Öyle ki, artık bir "ağ toplumu"nda yaşadığımız kabul edilmektedir (Van Djik, 2012). Bu ağ toplumunda siyasal hayatın da internetin etkisi altında dönüşeceği beklentisi oluşmuştur. Bu dönüşümün niteliğine dair de son yirmi yıldır birçok olumlu beklenti dile getirilmiştir. İnternetin hükümetleri ve demokrasiyi kökten değiştireceği, yeni bir demokratik dalga oluşturacağı ve otoriter rejimlerin bunun karşısında direnemezken, var olan demokrasilerin de olgunlaşacağı düşüncesi güçlüdür. Hatta internetin, klasik Yunan demokrasisi ve temsili demokrasiden sonra üçüncü dönem olarak elektronik demokrasiyi getirdiğini iddia edenler de olmuştu (Grossman, 1995, s. 33-40).

Gerçekten de geçtiğimiz yirmi yılda internetin siyasi hayatta birçok yapısal değişiklik yaratacağı beklentisi oldukça yüksekti. Öncelikle internetin siyasete "idarecilik" anlamında büyük bir yenilik getireceği düşüncesi mevcuttu. O vakte kadar köhnemiş bürokratik kurumlar tarafından idare edilen siyasal sistem, internetin devreye girmesi ile etkinleşecek, şeffaflaşacak ve böylece demokratik baskıya daha da açık hale gelecekti. Özellikle yerel yönetimler, internet aracılığıyla hem hizmetlerin niteliğini artıracak hem de vatandaşların karar alma süreçlerine katılımını kolaylaştıracaktı. Benjamin Barber (1998) da bu süreçte teknolojinin, plebisit imkanını artırması nedeniyle katılımı öne çıkaran "güçlü demokrasiyi" (*strong democracy*) geliştireceğini iddia etmiştir (s. 582).

Büyüsü bozulan demokrasi ve siyasal partilere olan ilgi kaybı gibi günümüz sorunları karşısında da internetin ilgiyi yeniden canlandırabileceği beklentisi oluşmuştu. Hem kamusal bilginin

yaygınlaşması hem de katılım imkanlarının süreklileşmesi insanları canlı bir siyasal atmosferin içine yerleştirecekti. Kurumsal yapıların ve özellikle siyasal partilerin bu dönüşümden etkilenmesi kaçınılmazdır. Bireyler düşünce ve çıkarlarını bir siyasal parti aracılığıyla değil bizzat kendi imkanları ile kamuoyuna ulaştırabilecek olanaklara sahip olacak ve bu da hem partilere hem de maddi kaynaklara bağımlılığı azaltacaktı. Bu dönüşümden parlamento da etkilenecek, vatandaş, parti ve parlamento arasındaki ilişkiyi dönüştürecekti (Ferdinand, 2000, s. 9-10).

Küresel politika veçhesinde ise internetin, otoriter rejimlerin baskısını ve kontrolünü ortadan kaldıracağı düşüncesi hakimdi. 1995 tarihinde bir Pentagon yetkilisi internetin otoriter rejimler üzerindeki beklenen etkisini şu cümlelerle ifade etmekteydi:

> …internet otoriter rejimler için stratejik bir tehlikedir ve ona karşı üretebilecekleri etkin bir önlem bulunmamaktadır. Dünyanın dört bir yanından vatandaşlara ulaşan bilgiler, rejimin kendisi ve dünya hakkında sunduğu imajla çarpışacak ve meşruiyetini ortadan kaldırıp, protestoları getirecektir. Yine ülke vatandaşlarının dünyanın diğer kısmındaki insanlarla kuracağı iletişim de, rejimin imajını zedeleyecek ve onun kontrol aygıtlarını zayıflatacaktır. Ülke içindeki hak ihlalleri ve baskılar da internet kanalıyla dünya kamuoyuna taşınacak ve bu da rejimi uluslararası toplumun müdahalesi ile karşı karşıya getirecektir. (akt. Ferdinand, 2000, s. 12)

İnternetin yarattığı uluslararası kamuoyunun, baskıcı rejim üzerinde güçlü bir etki uyandırdığı ilk deneyim Chipas'daki Zapatista hareketinin eylemliliğidir. Yine Endonezya'daki Suharto rejiminin yıkılmasında da internetin sağladığı kamusallığın etkili olduğu belirtilmektedir. Dönemin gözlemcileri de internetin bir ulus-üstü sivil toplum yaratacağı ve bunun da otoriter rejimlere demokratikleşme konusunda baskı yapacağı beklentisindeydiler (Ferdinand, 2000, s. 16).

2000'lerde de bilişim teknolojilerinin siyasal alanı demokratikleşme yönünde etkilediği birçok gelişme yaşanmıştır. Özellikle Web 2.0'ın yani ikinci nesil web sitelerinin/programlarının ortaya çıkışı ile bu demokratikleşme eğilimi giderek güç kazanmıştır. Sosyal medya uygulamaları Web 2.0'ın en çok öne çıkan yüzleridir. Bu uygulamalar ile bilginin üretilmesi ve yayılması yatay bir eksenden gelişmeye başlamış ve geleneksel medyanın dikey iletişim biçiminin aksine daha eşitlikçi ve özgür bir platform ortaya çıkmıştır (Calingaert, 2010, s. 65). Web 2.0 sadece ifade özgürlüğünü geliştirmekle kalmamış, buna ek olarak örgütlenme özgürlüğünü ve imkanını da artırmıştır. Fiziksel mesafelere bakmaksızın bireylerin fikir alışverişinde bulunup tartışmalarını sağlayan bu teknoloji, onların ortak hedefler etrafında bir araya gelmelerini de mümkün kılmıştır. Öyle ki, Web 2.0'ın yurttaş aktivizmini (*civic acitivism*) geliştirdiği iddia edilmiştir (Calingaert, 2010, s. 66).

Gerçekten de bu yıllarda bilişim teknolojilerinin imkan verdiği birçok yurttaş aktivizmi örneği yaşanmıştır: 2004'te Ukrayna'da muhalif Yuschenko'nun taraftarları "turuncu devrimi" mesaj teknolojisinin sağladığı örgütlenme ile başarmışlardır. 2005'te Suriye Ordusu'nun, Lübnan'dan çekilmesinde de aktivistlerin e-posta ve mesajlarla örgütlenmesi etkili olmuştur. İran'da şaibeli 2009 başkanlık seçimleri sonrasında gelişen protesto hareketlerinin de Twitter üzerinden geliştiği tespit edilmiştir (Bremmer, 2010, s. 86-87). Ancak bu olumlu gelişmelerin yanında otoriter rejimlerin bilişim teknolojilerinin yaygınlık kazanmasına rağmen varlıklarını devam ettirdikleri görülmektedir.

Başlangıçta umulan her kültürün ve siyasal rejimin bu teknolojilerin getirdikleri imkanlar ile liberalleşeceği ve küresel hümanist değerleri benimseyeceği beklentisi gerçekleşmemiş ve kullanıcılar kendi yerel değerlerini savunmak ve meşrulaştırmak için bu platformları kullanır olmuşlardır. Böylelikle internet çoğulculuk ve evrenselcilik getirmemiş aksine ulusal gururun bu değerler hilafına öne çıktığı bir alan haline gelmiştir. Bu hayal kırıklığında "tekno-iyimserlerin" (*techno-optimists*) bu araçlara demokratik bir öz atfetmeleri ve onu nötr bir araç olarak görmemeleri etkili olmuştur. Ian Bremmer'in (2010) de belirttiği gibi bu araçları kullanma imkanına sahip olmak bir özgürlük edimidir, fakat bu zorunlu olarak ötekilerin özgürlüğünü de artıran bir özgürlük biçimi değildir. İletişim teknolojisinin gelişimi demokrasiye olan talebi artırmaz, böyle bir talep varsa onun büyümesine katkıda bulunur. Örneğin Çin'de internet, batı karşıtlığı üzerinden ulusal gururu yüceltmek ve de Tibetli, Uygurlu azınlıklara karşı nefret söylemini artırmakta kullanılmıştır (s. 87-88). Tabi bunun yanında siyasal iktidarların, bilişim teknolojileri ile kurdukları ilişki de bu teknolojilerin demokrasi ile bağlantısını şekillendirmektedir. Bu noktada Larry Diamond'un (2010) "geleceğimizi teknoloji değil, fakat onu kullanan halkların, örgütlerin ve devletlerin iradesi belirleyecektir" iddiasının haklı olduğu görülmektedir (s. 82). Zira bilişim teknolojileri vatandaşların bilgiye ulaşımlarını artırdığı gibi iktidarların da bu bilgileri manipüle edebilmelerini ve vatandaşların görüş alışverişlerini takip edebilmelerini sağlamaktadır (Calingaert, 2010, s. 67). Neticede otoriter rejimler bu teknolojilere uyum sağlayıp, rejimlerinin istikrarı içinde bunlardan faydalanmaktadırlar.

Şebekeleşmiş Otoriteryanizmin Gelişimi

Üçüncü Demokratikleşme dalgasına rağmen otoriter rejimlerin sayısının azalmadığı ve hatta giderek küresel bir boyut kazanmaya başladığı sıklıkla dile getirilmektedir. Larry Diamond, Marc F. Platter ve Christopher Walker (2016) özellikle 2005'ten itibaren demokratikleşme dalgasının sona erdiğini ve otoriter bir karşı dalganın büyümeye başladığını belirtmektedirler. "Renkli Devrimler" sonrası başlayan bu büyüme ile "beş büyük otoriter rejim" (Çin, Rusya, İran, Suudi Arabistan ve Venezuela) demokrasiye karşı çok daha koordine ve kararlı bir şekilde harekete geçmişlerdir. Öyle ki, küresel çaptaki demokratik kurumların karşısına kendi aralarında kurdukları işbirliği teşkilatlarıyla çıkıp demokratik normların içini boşaltmaya çalışmaktadırlar. Ayrıca, ülke içinde demokratik muhalefeti, ifade ve toplanma hürriyetini sınırlandırarak bastırdıkları gibi sivil toplumu ve medyayı da ya devşirerek (*co-opt*) ya da manipüle ederek kendi ideolojilerinin yayılmasını sağlamaktadırlar. Bu noktada küresel çapta yayın yapan televizyon kanallarından da (Rusya'nın RT'si, Çin'in CCTV'si, İran'ın Press TV'si) oldukça faydalanmaktadırlar (s. 3-4). Otoriter rejimlerin bu şekilde küresel bir hedefle ortaya çıkması oldukça yenidir ve bir strateji değişikliğinin göstergesidir. Zira eski tip otoriter rejimler ne içeride ne de dışarıda bir meşruiyet arayışında bulunmazlarken, günümüzde bu rejimlerin de "meşru" görünme çabası içinde oldukları görülmektedir. Bu da salt baskı yerine "yumuşak güç" (*soft power*) taktiklerine yöneldiklerinin işaretidir.

Bu rejimlerin "yumuşak güç" taktikleri çerçevesinde bilişim teknolojilerini ve özellikle de interneti başarılı bir şekilde kullandıkları birçok araştırmacı tarafından tespit edilmektedir (Calingaert, 2010; Deibert ve Rohozinski, 2010a; Karlekar ve Cook, 2009). Bu araştırmacılardan Karin Deutsch Karlekar

ve Sarah G. Cook (2009) otoriter rejimlerin enformasyonu erişimi engelleyerek, içeriği sınırlandırarak ve kullanıcı haklarını (mahremiyetini) ihlal ederek kontrol ettiklerini belirtmektedirler (s. 1).

Ronald Deibert ve Rafal Rohozinski (2010a) ise bu sınıflandırmayı daha da detaylandırmışlardır. Buna göre, otoriter rejimler siber alanı birden fazla yöntemle kontrol etmeye çalışmaktadırlar. Bunların başında yasal düzenlemeler gelmektedir. Hükümetler, hakaret, telif hakkı ve ulusal güvenlik gibi yasal gerekçelerle siber alan kullanımını denetlemekte ve sınırlandırmaktadırlar. Gayri resmi taleplerle de hükümetler, özel internet sağlayıcılarından ve de şirketlerden "ulusal güvenlik" ve "kültürel hassasiyet" gibi gerekçelerle belirli içeriklerin kaldırılmasını isteyebilmektedirler. Hatta zaman zaman aktivistlerin ve muhaliflerin protestolarını durdurabilmek için internet sağlayıcılardan hizmetlerini yavaşlatmalarını ve durdurmalarını talep etmektedirler. İnternet sağlayıcı kurumlar ve siber şirketler de ama gönülsüz ama gönüllü politikalarını hükümetlerin hassasiyetlerini göre şekillendirebilmektedirler. Dış kaynak kullanımı (*outsourcing*) olarak adlandırılan bu uygulamada küresel şirketler ülkelerin hukuksal çerçevesi ve de hassasiyetleri üzerinden her birine farklı hizmetler sunmaktadırlar. Örneğin, Microsoft'un arama motoru Bing her ülkede farklı içerikleri sansürlemektedir. Bir diğer dış kaynak kullanımı da hükümetlerin internet sağlayıcılara ve de internet kafelere kullanıcılarının kimlik bilgilerini güvenlik birimlerine bildirme zorunluluğu getirmesidir. Böylece firmalar, devlete gözetim ve kontrol sağlamakta katkıda bulunmaktadırlar (s. 51-52). Muhalif sitelerin ya da muhalifler tarafından kullanılan platformların anlık saldırılarla (*just-in-time blocking*) engellenmesi de bir diğer yöntem olarak öne çıkmaktadır. Botnet saldırılar olarak da bilinen bu saldırılarda hükümet karşıtı herhangi bir site, bir merkezden engellenebilmektedir. Yine serverların bulunduğu binaların elektriğini kesme de bu anlık saldırı örnekleri arasında yer almaktadır. Hükümetlerin muhalif platformlar/siteler karşısında benimsediği bir diğer taktik de vatansever bilgisayar korsanlığıdır (*patriotic hacking*). Burada hükümetler yüksek bilgisayar kullanma becerilerine sahip taraftarlarını gayri resmi bir şekilde muhalif sitelere karşı yönlendirmekte ve bu siteleri ya ele geçirmekte ya da kullanılmaz hale getirmektedirler. İran'da kendilerini "İran Siber Ordusu" olarak tanımlayan bu korsanlar 2009 yılında muhalif birçok Twitter hesabını ele geçirmişlerdir. Hükümetler son olarak muhaliflerini takip edebilmek için kötü amaçlı yazılımlar (*social malvare attack*) ile onların networklerine girmeye ve bu şekilde faaliyetlerinden haber almaya çalışabilmektedirler (Deibert ve Rohozinski, 2010a, s. 54-55).

Deibert ve Rohozinski'nin (2010b) bir başka çalışmalarında ise bu yöntemler üç nesil üzerinden ele alınmaktadır. Buna göre ilk nesil kontrol yöntemi, teknik filtreleme-sansür ve internet kafeleri takip etmektir. Defansif olarak tanımlanan bu yöntemde ülkenin güvenlik birimleri internet sitelerini gözlemleyip, zararlı bulduklarını doğrudan internet sağlayıcılara bildirmekte ve onlar da bu sitelere erişimi engellemektedir (s. 23-24). İnternet kafelerde de tüm kullanıcıların bilgileri toplanmaktadır. Birinci nesil kontrol yöntemi olarak adlandırılan bu model daha çok az gelişmiş, otoriter rejimlerde karşımıza çıkmaktadır. Ayrıca bu uluslararası toplum tarafından da en rahat şekilde gözlemlenebilen, tespit edilebilen baskı formudur. Çin'in benimsediği ulusal çapta filtreleme ağı olan Great Firewall bu formun en tipik örneğidir (Deibart, 2015, s. 65).

İkinci nesil kontrol yöntemlerinde ise devlet yasal-normatif bir çerçeve ve yahut teknik imkanlar kullanarak ya sözde meşru yollarla ya da tespit edilmeden interneti denetlemektedir. Yasal çerçeveden

kasıt hükümetin hakaret ve pornografi gibi hukuki gerekçelerle içeriklere ve hesaplara erişimi engellemesidir. Teknik imkan ise hukuki bir yol gözetmeden ve sorumluluk yüklenmeden içerikleri anında kapatabilme ve erişimi engelleme kudretidir. Yasal yöntemlerin başında sitelerin sunucularını ülkede bulundurma zorunluluğu gelmektedir ve buna bağlı olarak hükümetin uygunsuz bulduğu siteleri ulusal domainden silmesi de bir diğer yasal yöntemdir. İçeriklerin hakaret, kişisel bilgilerin ifşası ve de ulusal güvenliği tehdit gibi nedenlerle kaldırılması da bu yöntemin sık başvurulan formlarındandır. Teknik kontrolün başında ise hükümetin internet sağlayıcılara –informel şekilde – belirli sitelere erişimi engelletmesi gelmektedir. Bunun daha çarpıcı formu ise bölgesel ya da ulusal düzeyde internetin kapatılmasıdır. Bu iki formda da genellikle teknik arıza açıklamasının arkasına sığınılmaktadır. Teknik kontrolün son formu ise hükümetin yönlendirdiği siber saldırıların muhalif siteleri ya ele geçirmesi ya da işlemez hale getirmesidir. Bu saldırılarda da hükümetin doğrudan etkisini tespit etmek çok zordur (Deibert ve Rohozinski, 2010b, s. 25-26). Kontrolün bu formunda "ulusal güvenlik" ve "siber suçlar" gibi ifadeler de müdahale için en sık başvurulan bahaneler olmaktadır. Yakın dönemde Etiyopya'da altı blog yazarı ve üç gazeteci terör ve ihanet suçlaması ile tutuklanırken, Tayland da yeni bir "siber suç" yasası geçirerek, otoritelerin elektronik postalara, telefon kayıtlarına ve bilgisayarlara mahkeme onayı olmadan erişebilmelerine izin verilmiştir. Hükümetin, özel sektörden informel işbirliği talebi de bu ikinci nesilde görülen bir diğer uygulamadır. Bu noktada hükümetler hem hizmet sağlayıcılardan, hem de yazılım üreticilerinden kendisinin gözetim imkanı için "arka kapılar-boşluklar" istemektedir. Örneğin Rus hükümeti, internet sağlayıcıların SORM'a – elektronik iletişimi sürekli takip eden ve yerel güvenlik birimlerine arşivlemesi ve incelemesi için gönderen hükümete ait bir gözetim sistemi – uyumlu olmalarını zorunlu kılmıştır (Deibert, 2015, s. 67).

Üçüncü nesil kontrol yöntemi ise ilk ikisine göre çok daha sofistikedir, tespiti en zor ama en yetkili yöntemdir. İlk nesil kontrol, savunma odaklıyken (*defansif*), ikincisi siber alanı sürekli tarayıp, kontrol altına alır, üçüncü nesil ise saldırgandır (*ofansif*). Bu formda bastırmaktan ziyade enformasyon alanında siyasi rakiplerle rekabet etme arzusu daha belirgindir. Burada rekabetten kasıt ise muhalifler karşısında karşıt bilgi üretme ve böylelikle onları itibarsızlaştırıp, demoralize etmektir. Bunlardan ilki ulusal internet hizmetini yetkisiz bir şekilde sürekli gözetlemektir (*warrantless monitoring*). Bu noktada internet sağlayıcıların yardımı hiç şüphesiz hayatidir. İkincisi ise ulusal bir internet alanı (*national cyberzone*) kurmak ve böylece küresel ağın dışına çıkmaktır. Bu yöntem hem internet sağlayıcıların hem de bireysel kullanıcıların işine gelmektedir zira internetin hem erişim hem alan maliyetini düşürmektedir. Bir diğer yöntem ise özellikle Çin'de sıklıkla rastlanan "hedefli casusluk" (*targeted cyberspionage*) uygulamasıdır. Pekin yönetimi, insan hakları, demokrasi ve bağımsızlık taraftarı hareketleri sürekli takip etmekte ve internet üzerindeki her türlü faaliyetlerini incelemektedir. Bunu da kötü amaçlı yazılımlar gönderip hesapları ele geçirerek yapmaktadır. Bu kontrol yönteminin doğal sonucu ise sivil toplumda ve muhaliflerde otosansürün gelişmesi ve eylemsizliğin başlamasıdır (Deibert, 2015, s. 69; Calingaert, 2010, s. 65). Son yöntem ise devlet destekli gruplarla, muhalif hedeflere saldırmak ve onların muhalefetini boşa çıkarmaktır. Öyle ki, bu yöntemde amaç muhalifin internete erişimini engellemek değil, toplumda azınlık olduğunu ve de yaydığı bilgilerin yanlış olduğunu iç ve dış kamuoyuna duyurmaktır. Popüler dilde "troller" olarak da anılan bu "elektronik ordular" muhalifler hakkında aşağılayıcı bilgiler servis etmekte,

hükümetin propagandasını yapmakta ve de anketleri manipüle ederek hükümet lehine kamuoyu oluşturmaktadırlar (Deibert ve Rohozinski, 2010b, s. 27-28). Kendilerini otantik bir kamuoyu gibi sunmayı başaran bu orduların eylemleri ortaya çıktığında da hükümetler rahatlıkla aralarındaki ilişkiyi inkar edebilmektedirler. Bu elektronik orduların örnekleri, Venezuela'da Chavistaların yönettiği "Communication Guerillas", Mısır'da "Mısır Siber Ordusu", Suriye'de Esad taraftarı "Suriye Elektronik Ordusu", Rusya'nın Putin taraftarı blogcuları ve Çin'in "Fifty-Cents" topluluğudur. Bu son nesil yöntem nispeten gelişmiş ve dış ile iç kamuoyunun hassasiyetlerine kağıt üzerinde saygı gösteren rejimlerde görülmektedir ve bu kontrol giderek yaygınlık kazanmaktadır (Deibart, 2015, s. 69). Calingeart (2010) da birinci nesil kontrol yöntemlerinin Çin ve İran gibi otoriter rejimlerde benimsenirken, bu sonuncu yöntemin Mısır, Rusya ve Malezya gibi "kısmi özgür" ülkelerde tercih edildiğini belirtmektedir. Ancak son dönemlerde Çin'in de vatandaşlarının tepkisinden çekinerek sansürü giderek azalttığını ve daha çok üçüncü nesil kontrol yöntemlerine yaklaştığını söyleyebiliriz (s. 70).

Otoriter rejimlerin dijital iletişim teknolojileri ile pekala barışık yaşadığını savunan Rebecca MacKinnon (2011), otoriter rejimlerin bu teknolojiye uyum sağlamasını "otoriterliğin şebekeleşmesi" adını vermektedir (*networked authoritarianism*). Otoriterliğin şebekeleştiği bu devlette ülkeyi tek bir parti yönetmesine rağmen, ülkenin problemleri sosyal medyada ve diğer sitelerde konuşulabilmektedir. Hükümet online sohbetleri takip etmekte, bazen de insanlar sosyal problemlere ve adaletsizliklere dikkat çekmek ve hükümeti bu konuda harekete geçirmek için interneti kullanmaktadırlar. Bunun neticesinde insanlar klasik bir otoriter rejimde deneyimleyemeyecekleri şekilde konuşma ve dinlenme üzerinden bir özgürlük duygusuna sahip olabilmektedirler. Fakat bu hisse rağmen, bu ülkelerde de bireysel hak ve özgürlüklerin hiçbir garantisi bulunmamaktadır; rejimin tehdit olarak gördüğü insanlar tutuklanmakta, rekabetçi, özgür, adil seçimler yapılmamakta ve mahkemeler rejimin aygıtı olarak çalışmaktadırlar. Hükümet interneti sürekli gözetim altında tutmakta ve siber gündemi manipüle etmektedir, böylece anlamlı bir muhalefetin oluşumunu engellemektedir. Ayrıca tartışılmasına izin verdiği siyasi, toplumsal gündemle de vatandaşlarının ülkeleri ve dünya hakkındaki görüşlerini bulanıklaştırmaktadır. Bu noktada özellikle Batılı gözlemcilerin internetin otoriter rejimler için bir truva atı hizmeti göreceği ve onları zayıflatacağı beklentisinin de gerçekleşmediğini söylemek durumundayız. Demir Perde'nin uydu yayınlarının etkisi ile çözüldüğü gibi, otoriter rejimlerin de internet ile çözüleceği varsayımı ile hareket eden bu gözlemcileri, şebekeleşmiş otoriter rejimler hayal kırıklığına uğratmaktadırlar (s. 33-34).

Şebekeleşmiş otoriter rejimler yukarıda saydığımız üç nesil kontrol yöntemine de zaman zaman başvuruyor olsalar da daha çok üçüncü nesil kontrol yöntemlerini tercih etmektedirler. Zira, bu rejimlerde sansür ve yasaklama asgari seviyede tutulurken, internet kullanımı sürekli gözetlenmekte veya manipüle edilmektedir. Bunun bir neticesi, kullanıcıların internette özgürce dolaşırken, kendilerini otosansür uygulamaları ve rejimin muhakkak onu gözetlediği ve kimliğini tespit edebileceği şüphesiyle politik konulardan uzak durmasıdır. Şebekeleşmiş otoriter rejimin bir diğer veçhesi de sanal ortamda kendi taraftarı bir suni kitle yaratarak muhalefeti diğer kullanıcılara karşı hem görece zayıf göstermek hem de onların direncini kırmaktır. Şimdi, iki büyük otoriter rejimin, Rusya ve Çin'in, interneti nasıl kendi istikrarları için araçsallaştırdıklarına yakından bakıp bu yeni

olguyu sahada inceleyeceğiz. Ancak öncesinde şunu belirtmeliyiz ki, bu iki ülke her ne kadar üçüncü nesil kontrol yöntemlerini benimsiyor olsa da, bir set olarak bu yöntemlerin hepsine değinilmeyecek, ülke örneklerinde öne çıkan kontrol yöntemlerine yoğunlaşılacaktır.

Çin Halk Cumhuriyeti

Çin, bu üç nesil kontrol yöntemini de başarıyla uygulayan ülkelerin başında gelmektedir ve bu durum vatandaşlarının internetle kurdukları ilişkide kendisini açıklıkça göstermektedir. Rebecca MacKinnon'a (2012) göre Çinliler, ülkeleri ve dünya hakkında ya bilgisizdirler ya da çarpıtılmış bir bilgiye erişmelerine izin verilmektedir. Devlet Başkanı Deng döneminde (1978-1989) ekonomi alanında başlayan hareketlilik, 1990'larda internetin gelişimi ile daha da artmış ve bu alanda kısmi serbestliklere izin verilmiştir. İnsanlar sosyal-siyasal meseleleri ve hukuksuzlukları bu siber alandan konuşmaya başlamışlardır ancak bu etkileşimin siyasal sistemde herhangi bir değişikliğe neden olmadığı gözlemlenmiştir. Hatta internet kullanımında hükümetin kırmızı çizgilerini geçenler yirmi yıl önceki muhaliflerin kaderini paylaşmak durumunda kalmışlardır. 2008 tarihli bir insan hakları raporu ülkedeki siyasi tutukluların sayısının internet kullanımının yaygınlaşmasıyla kat be kat artığını iddia etmektedir. Ancak bu artışın bilgisi bile Çinli internet kullanıcılarından öğrenilememiştir.

Çin hükümetinin internet ile ilişkisi üzerinde yoğunlaşan MacKinnon (2011), internetin Çin'de ve diğer baskıcı rejimlerde hızlı bir demokratikleşme doğurma beklentisinin aceleci olduğunu iddia eder. O da internetin ve mobil teknolojilerin özgürlük ve özerkleşme sunan potansiyellerinin ortaya çıkmasının ancak hükümet politikaları ve şirket sorumluluklarının düzenlenmesi ile mümkün olabileceğini savunmaktadır. MacKinnon, Çin hükümetinin internet dünyasına hızlı adaptasyonu ve diğer otoriter rejimlerden farklı olarak internetin hızını düşürmeyip, vatandaşlarına yüksek hızlı internet sunması nedeniyle klasik bir otoriter rejim olmadığını fakat "şebekeleşmiş bir otoriter rejim" olduğunu iddia etmektedir.

Çinli gazeteci Michael Anti'nin 2012 yılındaki TED konuşması da bize bu şebekeleşmiş otoriter rejim hakkında bilgiler sunmaktadır. "Great Firewall" olarak anılan Çin'in güvenlik duvarının ardında çok canlı bir sosyal medya deneyiminin olduğunu belirten Anti, 500 milyon internet kullanıcısı (*netizens*) olan ülkede tüm küresel uygulamaların muadili olduğunu belirtmektedir: Google-Baidu, Twitter-Wiebo, Facebook-Renren, Youtube-Youku. Çin hükümeti sunucularını ülkede kurmaya yanaşmayan, dolayısıyla kontrol edemediği bu platformları ülkesine sokmamakta ve fakat vatandaşlarını da bundan mahrum etmemektedir. Yani hükümet "blokla ve klonla" yöntemini benimsemektedir. Anti bu noktada Ortadoğu rejimleri ile Çin'in uygulamaları arasındaki farka dikkat çeker ve bu rejimlerin, vatandaşlarının kendilerini eleştirmelerini engellemek için interneti kapattıklarını fakat bunu yaparak onları sokağa inmeye teşvik ettiklerini belirtir. Tunus lideri Ben Ali'nin ise interneti ve sosyal medyayı serbest bıraktığı ve neticede buralarda örgütlenen muhalefetle devrildiğini aktarır. Bu örnekler karşısında Çin'in kendine has bir internet ağı (ChinaNet) yaratarak, bunların dışına çıktığını gösterir. Anti'ye göre Çin'de her ne kadar güçlü bir sansür ve kontrol olsa da, 300 milyonluk blog ve 500 milyonluk internet kullanıcısıyla geçmişte görülmemiş gerçek bir kamusal alan ortaya çıkmıştır; sosyal medyada eleştiriler başarısız bakanları makamlarından edebilmektedir.

Ancak yine de sosyal medya şirketleri hükümet ile yakın bir işbirliği içindedir ve platformlarının hükümet karşıtı şekilde kullanılmasına izin vermezler. Herhangi bir sosyal hareket örgütlenmesi/planlanması anahtar kelimeler üzerinden anında kayıt altına alınıp güvenlik birimlerine bildirilmektedir. Merkezi hükümet sansürü ve denetimi elinde tutuyor olsa da yerel otoriteler karşısında halkın hoşnutsuzluğunun dile getirilmesi ve tartışılmasını tolere edebilmektedir, rejimin tartışılmaması kaydıyla. Öyle ki, Çin hükümetinin sansür kullanmamayı tercih etmesi bir siyasal araç haline gelmiştir ve rejim içi siyasal kavgalarda, halkın hoşnutsuzluğu sansür edilmiyorsa, merkezi hükümet o bürokratı ya da yerel lideri gözden çıkarmış demektir. Böylece rejime olan muhalefet ve memnuniyetsizlik yerel liderler ve bürokratların halkın protestoları ile indirilmesi gösterisi ile giderilmektedir.

MacKinnon (2011) da, Hirschman'ın ses ve çıkış (*voice and exit*) kavramları üzerinden Çin hükümetinin sansür ile ilişkisine eğilmektedir. Buna göre hükümet, rejimi sorgulamayan, sistem içi eleştiriler olarak gördüğü ses aktivizmine izin vermekteyken, Pekin'i sorgulayan ve radikal taleplerde bulunan çıkış aktivizmine ise izin vermemektedir. Ses aktivizmi ile reformist politikacılar, yerel ya da muhafazakar idarecileri/siyasileri, reform yapılmazsa daha sert protesto dalgaları gerçekleşeceği argümanı ile reformlara ikna edebilmektedirler (s. 35). Çin hükümetinin internet ile ilişkisini daha genel bir perspektiften "otoriter müzakerecilik" (*authoritarian deliberation*) olarak yorumlayan yaklaşımlar da mevcuttur. Buna göre rejim halkla arasında sınırlı ve kontrollü iletişim kanalları açmakta ve bu kanallar üzerinden meşruiyetini güçlendirmeye çalışmaktadır.[1] Medyanın ticarileşmesi ve internetin yaygınlık kazanmasının hükümetin daha zımni bir propaganda yürütmesini sağladığı gibi kamuoyunu yakından takip edebilmesine imkan tanıdığı da söylenmektedir (Stockmann, 2013). Bu noktada internetin temel işlevi de sisteme dönük olmayan akut şikayetleri öğrenip giderme ve bu diyalog kanalı ile halkı kontrol etmektir. Hükümetin bu alanda kullandığı üç temel platform vardır: merkezi propaganda siteleri, hükümetin regüle ettiği ticari siteler ve de sivil toplum örgütleri tarafından yönetilen ticari olmayan kamusal siteler. Hükümet, her üç platformda da tartışmaları takip etmekte, vatandaşlarla iletişim kurmakta ve muhalif/hassas içerikleri engellemektedir (Jiang, 2010). Sert ve keyfi sansürün geri tepeceğini düşünen Çin hükümeti böylece interneti yasaklamaktan ziyade o platformda kendi varlığını/görünürlüğünü artırmakta ve kendi pozisyonunu savunacak "yorumcuları" istihdam etmeye yönelmektedir. Bu sayede propagandadan ziyade halkın dikkatini yönetmeyi tercih etmektedir.

2000'lerin ortalarından itibaren ise hükümet vatandaşlarının siyasi süreçlere daha fazla katılması ya da en azından öyle görünmesi ya da vatandaşları nezdinde öyle hissedilmesi için internet üzerinden bir dizi interaktif uygulama başlatmıştır. Devlet başkanı ile sohbet edebilme ve ona soru sorabilme imkanı sunan yıllık sohbet programı (web-chats) ve parlamentoya yasa önerisinde bulunma imkanı sunan *elektronik parlamento* (e-parliament) uygulaması bunların başında gelmektedir (MacKinnon, 2011, s. 42). Ancak ülke aynı dönemde insan haklarına, gazetecilere ve etnik azınlıklara karşı büyük

1 Andrew Nathan (2003) Çin'i ele aldığı çalışmasında, bu otoriteryan rejimin atlattığı onca badireye rağmen nasıl ayakta kaldığını tartışmış ve nedenlerden biri olarak da bu iletişim boyutunu öne çıkarmıştır. Buna göre, Çin rejiminin Tiananmen olayları ve Üçüncü Dalga demokratikleşme hareketleri karşısında yıkılması beklenirken vatandaşlarına sunduğu iletişim (*input*) kanalları/kurumları sayesinde onların yerel yönetimlere dönük şikayetlerini öğrenmiş ve böylece hem sisteme dönük eleştirilerin önünü kesmiş, hem de vatandaşların rejime olan güvenlerini artırmıştır (s. 7-10).

bir baskı politikası da uygulamaktadır. Hükümet bu interaktif uygulamalarıyla içeride ve dışarıda ülkenin demokratikleşmeye doğru ilerlediğine dair bir fotoğraf oluşturmaya çalışmaktadır.

Çin hükümeti internet üzerinde yürüttüğü bu sıkı denetimi özel sektörün yardımı ile sürdürmektedir. İfşa olan birçok belgede hükümetin sosyal medya platformu yöneticilerine sansürlenmesi gereken içerikleri ve temaları bildirdikleri görülmektedir. MacKinnon (2011), hükümetin halkının hangi bilgiye ulaşacağı, tartışacağı ve hangi konular etrafında örgütleneceğini yönlendirebilmek için bir dizi taktik geliştirdiğini belirtir. Bunlar, insan hakları savunucularının ve muhalif ulusal ya da yabancı gazetecilerin hesaplarına yönelik siber saldırılar, ülkede iç pazar için üretilen bilgisayarlara gözetim için bir program yükletmek (Green Dam Youth Escort)[2], firmalara ve kişilere "cn" alan adı uzantısını zorunlu kılarak çok daha sıkı bir kontrol sağlamak, bölgesel internet kesintileri yapmak, kullanıcıları resmi kimlikleri ile kaydederek gözetlemek – özellikle internet cafe kullanımlarında – ve son olarak proaktif bir şekilde internet gündemini belirlemeye, yönlendirmeye çalışıp bu görev için de suni bir kitle oluşturmak ve personel istihdam etmektir (*astroturfing and public outreach*). Bağımsız bir raporun belirttiklerine göre Çin hükümeti, kendi propagandasını yapması için 280 bin kişi istihdam etmektedir, bunun yanında parti üyesi olmak isteyen Komünist Gençlik Derneği üyeleri de "gönüllü" olarak hükümetin mesajlarını sosyal medyada yaymaktadırlar. Ayrıca birçok bağımsız blog sahibi de, hükümet tarafından devşirilmek (*co-opt*) için basın açıklamalarına ve özel konferanslara davet edilmektedirler (s. 39-41).

Çin hükümetinin internet kamuoyunu bastırmaktan ziyade yönlendirmek için tercih ettiği yöntemlerin başında suni kitle oluşturmak (*astroturfing*) gelmektedir. Suni kitle oluşturmak, reklamcılıkta ve politikada kullanılan bir halka ilişkiler (PR) yöntemidir. Bu yöntemde ücret karşılığında tutulmuş olan insanlar belirli bir ürün, politika ya da olaya destek vermektedirler. Çin hükümeti de 2004 yılından başlayarak kendi lehine yorum yazılması için bu yönteme başvurmaya başlamıştır. İlk defa bu tarihte Hunan bölgesindeki bir yerel birimin "internet yorumcuları" istihdam ettiği basına yansımıştır. Bu yorumcuların sabit bir ücret haricinde paylaştıkları her yorum için "50 sent" alıyor olmaları, muhalefetin onları "Fifty Cent Army" olarak adlandırmalarına neden olur (Han, 2015, s. 112). Aynı yılın sonunda bu sefer partinin merkez disiplin-gözetim departmanının 127 yorumcuya yolsuzluk karşıtı propaganda konusunda eğitim verdiği haberlere yansır. Bu kişiler arasında kamu görevlisi olup, rutin işinin dışında yorum da yazanlar olduğu gibi hususi bu iş için istihdam edilmiş insanlar da mevcuttur. 2010 yılında açığa sızan bir belgede "yorumcu" olarak istihdam edilmenin şartları şu şekilde sıralanmıştır: 1) Parti politikasına ve liderine bağlılık, 2) İnternet diline hakimiyet ve iyi bir kalem yeteneği, 3) Nitelikli bilgisayar kullanma becerisi ve uygulama ile yazılımlara hakimiyet, 4) Parti yayın organlarının vesayetini ve rehberliği kabul etmek (Han, 2015, s. 114). Talimatları ortak mesaj programları ile alan bu anonim yorumcular, 1) partinin ve hükümetin politik hedefleri doğrultusunda mesajlar yazma ve bunları yaymakla görevlidirler, 2) önemli olaylar hakkında çıkabilecek dedikoduları engellemek için otoritenin sunduğu bilgileri yayarlar, 3) sıcak gelişmeler/konular hakkında soruları yanıtlar ve internet kullanıcılarının kafa karışıklığını gidererek

2 Gençleri zararlı içeriklerden koruma niyetiyle başlatılan bu projenin kullanıcıları takip etme ve de internet erişimine sansür koyma gibi bir gizli gündemi olduğu çok çabuk anlaşıldı. Neticede hem içeriden hem de dışarıdan gelen eleştiriler ile yürürlüğe girmesi ertelenmiştir (Calingaert, 2010, s. 71).

dikkatlerini başka yöne çekerler ve 4) zararlı bilgileri dağıtarak kamu oyuna rehberlik eder ve böylece hükümetin bilgi yönetimini güçlendirirler. Kısacası bu yorumcular kamuoyunun nabzını tutup hükümetin propagandasını yapar ve krizleri dağıtırlar (Han, 2015, s. 116-117).

Edward Snowden[3] sonrası dönem Çin hükümetinin interneti kontrol edebilmek için ihtiyaç duyduğu uygun ortamın oluşmasına da katkıda bulunmuştur. Çin 2015 yılında yabancı internet şirketlerine birer mektup yollayarak Çin yurttaşlarının verilerini Çin sınırları içinde tutmalarını ve Çin'in ulusal güvenliğine zarar vermemelerini istedi. Yine aynı yıl bir anti-terör yasası çıkararak, yabancı şirketlerin serverlarını ülkede kurmalarını (*data localization*) ve gerektiğinde hükümetin bu verilere ulaşmasına yardımcı olmalarını zorunlu hale getirdi (Sargsyan, 2016, s. 2226).

Rusya Federasyonu

Şebekeleşmiş otoriteryanizmin görüldüğü bir diğer ülke de Rusya'dır. Rus internet politikası "batı dünyasının, interneti zayıf muhalefetlerin olduğu ülkelerdeki hükümetleri devirmek için kullandığı" yargısı ile temellenmiştir (Nocetti, 2015, s. 114). Rus dış politikası Westfalyacı ulus devlet egemenliği düşüncesine sıkı sıkı bağlıdır ve bu düşüncenin vaat ettiği "müdahalesizlik" argümanının devamlılığını istemektedir. Açık ve serbest internet fikri ise bu prensibi tehdit etmekte ve de yabancı ve yıkıcı düşüncelerin Rusya'da dolaşımının önünü açmaktadır. Yine 2000'li yıllarda vuku bulan "renkli devrimler" ve "Arap Baharı" gibi sosyal hareketler de internetin statükoyu tehdit ettiği yargısını güçlendirmiştir (Nocetti, 2015, s. 113). Putin, 2011 seçimleri sonrası yaşanan protestoları da Amerika'nın sosyal medya üzerinden icra ettiği bir komplo olarak yorumlamış ve Amerikan menşeili sosyal medyayı hedef tahtasına oturtmuştur (Herszenhorn, D. M ve Barry, E, 2011). Bu nedenle Rusya'da bilginin serbest dolaşımını sağlayan internet sadece muhalefete zemin sağladığı için değil, Amerikan hükümetinin Rusya'nın egemenliğini çiğnemesine fırsat verdiği için de arzu edilmeyen ve sıkı bir şekilde kontrol edilmesi gereken bir platformdur.

Rusya Çin'e nazaran internet erişimine nadiren engel koymakta, daha çok sansürü ve yıldırmayı tercih etmektedir. Ancak Rusya da, yakın dönemde erişimi engelleyecek ve kriz anlarında Runet'i küresel internet ağının dışında bırakacak bir arayış içine girmiştir (Deibert ve Rohozinski, 2010b, s. 17-18). Ülkede internet "İletişim, Bilgi Teknolojileri ve Medya Denetleme Federal Servisi"nin kontrolü altındadır ve bu kontrol kurumuna kısaca Roskomnadzor adı verilmektedir. Roskomnadzor'un belirli içerikleri mahkeme kararı olmadan anında engelleme hakkı bulunmaktadır. Bunun yanında aynı kuruluşlar internet sağlayıcılara bir "kara liste" vererek bu listeye erişimin engellenmesini mahkeme kararı olmadan isteyebilmektedir. Bu direktiflere uymayan sağlayıcıların lisansları yenilenmemektedir (Maréchal, 2017, s. 32). Ülkede ayrıca özel sektör, oligarşi ve istihbarat servisi FSB arasındaki ilişkinin doğası da internet üzerindeki kontrolü kolaylaştırmaktadır. Nepotik kapitalizm olarak da adlandırılan bu iktisadi düzende devleti elinde tutan oligarşi aynı zamanda özel sektörü de

3 2013 yılında Amerikan Ulusal Güvenlik Dairesi (NSA) çalışanı Edward Snowden, FBI ve NSA'nın PRISM adlı program ile ABD menşeili birçok internet şirketinin verilerine ulaştığı ve böylece dünya üzerindeki birçok insanın mahremiyetini ihlal ettiğini ortaya koydu. ABD'nin bu programla dünya üzerindeki internet kullanımının büyük kısmını gözetlediğinin açığa çıkması, internet üzerinde sıkı bir kontrol uygulamak isteyen otoriter rejimler tarafından memnuniyetle karşılandı. Öyle ki, benzer programlar bu ülkeler tarafından da "terör" gerekçesiyle kullanılır hale geldi. Bu konuda bkz. Hill (2014).

kontrol altında tutmaktadır. Bu nedenle özel sektörün bilişim firmaları hükümetin sansür taleplerini yerine getirmede istekli görünmektedirler (Vendil Pallin, 2017; Kelly, Earp, Reed, Shahbaz ve Truong, 2014). Bu işbirliğinin sonucu olarak da 2014'te kamusal internet ağlarına girilirken telefon numarası, kimlik veyahut pasaport bilgisinin belirtilmesi zorunluluğu getirilmiştir (Maréchal, 2017, s. 32). 2014 yılında çıkarılan başka bir yasayla da blog kullanıcılarının Roskomnadzor'a kayıt yaptırmaları zorunlu hale getirilirken takma ad kullanmaları da yasaklanmıştır.

Bu yasal ve teknik sansürün yanında Rusya'nın siyasal-toplumsal kültürü ve interneti tehlikeli bir alan olarak sunan ideolojik aygıtları da özgür internetin önündeki diğer engellerdir. Rus yönetici sınıfı ve ana akım medyası interneti tehlikeli bir alan olarak sunmakta ve içeriğini de güvenilmez, önyargılı ve tehlikeli olarak tanımlamaktadırlar. Bu propagandanın işe yaradığı söylenmektedir, zira Rus halkı internetin kontrol edilmesini istemekte ve internetin yabancılar tarafından Rusya'ya karşı bir silah gibi kullanıldığına inanmaktadırlar (Maréchal, 2017, s. 32). Rusya'nın internet kullanımı üzerindeki gözetimi 1995 yılına kadar geri gitmektedir. Bu tarihte SORM olarak kısaltılan "System of Operational Investigatory Measures" adlı uygulama yürürlüğe girmiştir. Rus İstihbarat Servisi FSB tarafından yürütülen bu uygulama ile tüm telekomünikasyon operatörleri FSB'nin sunduğu bir donanımı sistemlerine yüklemek zorunda bırakılmıştır. Bu donanım sayesinde FSB tüm telefon görüşmelerini, email trafiklerini ve internet kullanımını inceleyebilir hale gelir. 1999'da SORM-2 ile, bu sefer aynı donanımı internet sağlayıcıların takması zorunlu hale getirilir. Böylelikle, FSB tüm kredi kartı işlemlerini, elektronik postaları ve internet kullanımlarını takip eder duruma gelir. 2014'te ise SORM-2 sosyal medya, forum ve sohbet uygulamalarına doğru genişletilmiştir (Maréchal, 2017, s. 33). Şu anda Rus hükümetinin bu programla tüm internet kullanıcılarını takip edebildiğine inanılmaktadır. Bu noktada Edward Snowden'ın CIA'in tüm Amerikalı bilişim şirketlerinin datalarına PRISM adlı programla ulaştığını ifşa etmesi de, Rusya'nın SORM uygulamasını meşrulaştıran bir işlev görmüştür.

Snowden olayının Rusya hükümetine baskıcı internet ortamını sürdürmede bir diğer katkısı da veri yerelleştirme (*data localization*) arzusunu perçinlemesidir. Snowden'ın ifşaları tüm dünya hükümetleri tarafından büyük bir tehdit olarak algılanmıştır (Hill, 2014). Vatandaşlarının verilerinin CIA tarafından sürekli takip edildiği bilgisi onları internet konusunda yeni arayışlara yöneltmiştir. Hükümetler önceleri ulusal sınırlar içine veri akışından imtina ederlerken bu tarihten sonra bilgiyi içerde tutma telaşına düştüler. Bu telaş da Küresel Ağ olarak (World Wide Web) anılan internetin bu tanımlayıcı niteliğinden uzaklaşmasına ve bilgi paylaşımı üzerinden genişleyecek bu ağın, parçalara ayrılmasına neden olmaktadır. Küresel ağ geniş bilgi paylaşımı üzerinden ticaretin yaygınlaşmasına, maliyetlerin düşmesine ve inovasyonun ilerlemesine katkıda bulunmaktayken, veri yerelleştirmesi bu ilerlemeyi durdurmakta ve maliyetleri hem kullanıcılar hem de internet sağlayıcılar için artırmaktadır (Chander ve Le, 2014, s. 4). Bu noktada veri yerelleştirme yasalarını 19. yüzyılda serbest ticareti boğan tahıl yasalarına benzetmek de mümkündür. Veri yerelleştirme yasaları ülkeden ülkeye değişmekle birlikte bunların belli başlı özellikleri saptanabilmektedir. Bazı hükümetler, verinin ulusal sınırlar dışına taşınmasını engellemektedir, bazıları veri sahiplerinden data transferi öncesi izin alınmasını zorunlu kılmaktadır, diğerleri aktarılan dataların kopyalarının içeride de depolanmasını

şart koymaktadır, son yasa yöntemi ise ihraç edilen dataları vergilendirmektir (Chander ve Le, 2014, s. 3).[4]

Rusya, bu yönde adımlarını 2012 yılında ITU'nun (International Telecommunication Union) düzenlediği konferanslarda atmış ve tüm ulusların kritik internet kaynaklarını kullanmada eşit haklara sahip olması önerisini dile getirmiştir. Fakat bu öneri başta Amerikan hükümeti olmak üzere, ABD sivil toplum kuruluşları, bilişim firmaları ve diğer Batılı hükümetler tarafından internet özgürlüğüne bir tehdit olarak sunuldu ve böylece reddedilir. 2013 yılında Snowden olayının patlak vermesiyle Rusya'nın eli güçlenmiş ve 2015 yılında Veri Yerelleştirme Yasasını (Data Localization Law) yürürlüğe sokmuştur. Bu yasa ile internet sağlayıcılarına ve firmalarına Rus kullanıcıların verilerini Rusya topraklarında saklama yükümlülüğü getirilmiştir. Ayrıca, aynı yasayla yabancı şirketlerin de iletişim sistemlerine devletin verdiği şifreleme cihazlarını yerleştirmeleri zorunlu hale getirilir (Sargsyan, 2016, s. 2226-2227).

Rus hükümetinin internet üzerindeki kontrolünün bir diğer ayağı da, Rus menşeili sosyal medya platformlarının hükümet tarafından teşvik edilmesidir. Mail.ru, Yandex, Vkontakte, Odnaklassniki gibi şirketler bu platformların başında gelmektedir. Sunucuları haliyle ülke içinde olan ve sahipleri de hükümete yakın kişiler olan bu şirketlerin toplumsal muhalefetin takip edilmesi ve bastırılmasında etkili olacağı düşünülmektedir (Gunitsky, 2015).[5]

Şebekeleşmiş otoriteryanizm olgusuna Rus siyasal kültürünü sürdüren post-Sovyet ülkeleri üzerinden baktığımızda ise yerli bir internet yaratma motivasyonunun yanında bu ülkelerde bir de kullanıcıları caydırma gibi bir olgunun varlığından bahsetmek zorundayız. Bu rejimlerde de tıpkı Çin örneğinde olduğu gibi internetin yarattığı büyük imkanlardan faydalanma ve fakat onun getireceği toplumsal muhalefet riskinden sakınma arzusu mevcuttur. Bu nedenle, açık erişim ve sansür arasında bir orta yolu tercih etmektedirler (Pearce ve Kendzor, 2012, s. 2). İnternet üzerinden örgütlenen muhalefet karşısında bastırma ya da sansür uygulamaktan ziyade bu söylem ile rekabet etmeyi veya muhalefete bu eylemlerinin beyhudeliğini göstermeyi seçmektedirler. Pearce ve Kendzor'un (2012) Azerbaycan'ı inceledikleri çalışmalarında Azerbaycan hükümetinin sansür ve sistemik bir baskıdan ziyade bizatihi internetin iletişim imkanlarını kullanarak sosyal medyadaki muhalefeti yıllar içinde azalttığı, yani kullanıcıların politik davranışlarını değiştirdiği tespit edilmektedir. 2009 yılında vuku bulan "eşek bloggerları" (*donkey blogger*) olayı bu tutumun en net göstergesi olmuştur. Azerbaycan'ın Almanya'dan ithal ettiği eşekler ile kurgusal bir röportaj yapıp, bu hayvanların Azerbaycan vatandaşlarından daha fazla hakka ve özgürlüğe sahip olduğunu iddia eden iki blogger bir yıl süre ile hapiste tutuldu. Bu vaka ile ilgili haberler Azerbaycan otoriteleri tarafından sansür edilmediği gibi tüm kullanıcılar tarafından duyulmasına da özen gösterildi. Hükümetin bu misillemesinin duyulması internet kullanıcıları arasında kaygıya ve muhalefet etme konusunda tereddütlere neden oldu (s. 5). Pearce ve Kendzor, hükümetin bloggerların paylaşımını sansürlemiş olsaydı, kullanıcılarda böyle bir kaygıya neden olmayacağını söylemekte ve bu tercihi ile de her bir kullanıcıyı korku sarmalına

4 Son dönemde veri yerelleştirme yasaları çıkaran ülkelerin arasında Çin ve Rusya gibi otoriter rejimler olduğu gibi Avrupa Birliği gibi liberal rejimler de bulunmaktadır. Bu ülkelerdeki farklı uygulamalar için bkz. Chander ve Le (2014).

5 2011 parlamento seçimlerinde Twitter ve Facebook kullanıcıları seçimde hile yapıldığına inanmaktayken, Vkontante ve Odnaklassniki kullanıcıları böyle bir tartışmadan dahi haberdar değildi. Bu konuda bkz. Reuter ve Szakonyi (2015).

ittiğini belirtmektedirler. Tutuklanan bloggerlardan birinin ifadesi de bu noktaya işaret etmektedir: "bu onların çalışma tarzı (...) birilerini cezalandırıp, bunu herkesin görmesini sağlıyorlar. Demek istedikleri şu 'sizin de başınıza bu gelebilir'". (akt. Pearce ve Kendzor, 2012, s. 5).

Arap Baharı'ndan sonra sosyal medyaya ve internete olan yaklaşımın daha da farklılaştığını söyleyebiliriz. Bu dönemde sosyal medya kullanımının şeytanlaştırıldığı ve akıl hastalığı ile tanımlandığını görmekteyiz. Azerbaycan ulusal basınında sosyal medya kullanıcılarının suç işlemeye eğilimli oldukları ve aile trajedileri yaşadıklarına dair haberler çıkmaktadır. Hatta ülkenin önde gelen psikiyatristleri bu platformları kullananların gerçek hayattan kaçtıkları ve sosyal iletişim kurmalarını engelleyen psikolojik sorunlara sahip olduklarını açıklamışlardır. 2011 Mayıs'ında ise parlamento sosyal medyanın zararlı sonuçları üzerine toplanmış ve bunu engelleyecek yasa teklifleri önermiştir (Pearce ve Kendzor, 2012, s. 12-13).

Sonuç

Otoriter rejimlerin geleneksel baskıcı yöntemlerden uzaklaşarak *soft power* diye adlandırılan taktikler benimsemesi giderek yaygınlık kazanmaktadır. Bu taktiklerin uygulandığı bir diğer yer de siber alandır. Günümüzün asli iletişim kanalı ve medya organı haline gelen siber alan, politikanın üretildiği ve farklı politik düşüncelerin karşı karşıya geldiği temel zemindir. Bu nedenle, tüm siyasal iktidarların birinci derecede kontrol etmek istedikleri yerlerin başında gelmektedir. Geleneksel bir otoriter rejim, kontrol etmekte zorlanacağı böyle bir alanı yasaklayacakken, günümüz rejimleri onun yarattığı ekonomik sistemi ve inovasyonu reddedemeyecekleri için farklı bir şekilde mücadele etmeyi tercih etmektedirler. İnterneti yasaklamanın ve katı bir şekilde sansürlemenin hem maliyetli olacağını hem de halkın tepkisini çekeceğini bilen bu rejimler interneti yasaklamadıkları gibi geniş banttan veri akışını sağlayacak şekilde altyapılarını revize etmektedirler. İnternetin rejimin askeri, iktisadi ve teknik gücünü artırma potansiyellerini kabul eden fakat demokratik muhalefet tarafından kullanılmasını istemeyen bu rejimlerin başında Çin ve Rusya gelmektedir. Siber alandaki gelişmelerin demokratikleştirmediği, şeffaflaştırmadığı ve hatta baskıcı rejimlerine istikrar kazandırdığı bu ülke deneyimlerine literatürde şebekeleşmiş otoriteryanizm adı verilmektedir.

Bu iki şebekeleşmiş otoriter rejimin birbirlerinden çok farklı nitelikleri bulunmakla birlikte, ortak özellikler de sergilemektedirler. Buna göre her iki rejim de interneti vatandaşlarından esirgememekle birlikte farklı yollardan demokratik muhalefeti kontrol etmektedirler. Bunlardan en önemlisi veri yerelleştirme (*data localization*) uygulamasıdır. Özellikle Snowden olayı sonrasında her iki ülke de yabancı menşeli internet firmalarına yurttaşlarının verilerini ülke içinde tutmayı zorunlu hale getiren yasalar çıkartmışlardır. Bunun doğal sonucu da, rejimin vatandaşları hakkındaki verilere rahatlıkla ulaşabilmesi olmuştur. Yine her iki ülkede de bu gelişmeye paralel olarak internet sağlayıcılarına ve de bilişim firmalarına hükümetin gözetimini kolaylaştıracak donanımları kullanmaları dayatıldı. Rusya SORM programı ile bunu yaparken Çin de Green Dam Youth Escort ile bunu yapmaya çalıştı. Hem veri yerelleştirme, hem de bahsi geçen bu donanımlar ile iki rejim de muhalifleri doğrudan gözetleme imkanına kovuştular. Bu durumun doğal çıktısı da, kullanıcıların sürekli gözetlenme kaygısı ile otosansüre yönelmeleridir.

Veri yerelleştirmeyi kolaylaştıran ve böylece de rejimin kontrol gücünü artıran bir diğer uygulama da interneti yerelleştirmektir. Özellikle popüler sosyal medya sitelerinin taklitleri ile kotarılmaya çalışılan bu taktiğin gayet başarılı olduğunu söylemek zorundayız. Her iki ülkede de rejimin milli sosyal medya siteleri büyük bir popülerliğe sahiptir. Yasaklamaktan ziyade klonlamanın tercih edilmesi hem halkın bu programlara dönük ihtiyaçlarını gidermekte hem de rejimin toplum üzerindeki kontrolünü sağlamaktadır.

Bu iki rejimde tanık olduğumuz bir diğer ortaklık da suni internet yorumcuları (*astroturfing*) kullanmalarıdır. Otantik bir kamuoyu gibi hareket edip, hem ulus içinde hem de dışında rejimin halk desteğinin yüksek olduğunu göstermeye çalışan bu uygulamada örgütlü bir azınlık kamuoyunu dilediği gibi yönlendirebilmektedir. Rusya'da Putin'in Trolleri, Çin'de ise Fifty-Cent Ordusu bunun en tipik örnekleridir. Kamuoyunu taklit eden ve muhalif söylemlerle rekabet edip, onları marjinalleştiren bu kitleler giderek yaygınlaşmaktadır ve bunların karşısında demokratik güçlerin geliştirilebileceği pek fazla çözüm bulunmamaktadır. Yapılabilecek tek şey bu orduları tespit edip, ifşa edebilmek ve böylece otantik kamuoyunun sesini ortaya çıkarabilmektir. Son dönemde *astroturfingi* tespit etmek için modeller geliştiren çalışmalar artmaktadır (Ratkiewicz, Conover, Meiss, Gonçalves, Flammini ve Menczer, 2011).

Bunların yanında internet üzerinde kontrollü bir kamuoyunun oluşmasına izin vermek de şebekeleşmiş otoriter rejimlerin bir diğer ortak özelliğidir. Böyle yapmakla rejimin tamamına dönük olarak yoğunlaşacak eleştirinin gazını almakta ve halkta hükümetin hesap sorulabilir olduğuna dair bir kanaat oluşturmaktadırlar. Otoriter müzakerecilik (*authoritarian aeliberation*) olarak da adlandırılan bu yeni olgunun ilerleyen dönemlerde göz yumulan bu kısmi kamusallık ile demokratikleşme için zemin oluşturacağına dair beklentiler de mevcuttur.

Son olarak diyebiliriz ki, internetin demokrasi ve insan haklarıyla arzulanan olumlu ilişkisinin kendiliğinden kurulacağına inanmamak için çok fazla gerekçemiz bulunmaktadır. İnternetin beklenen bu sonucu doğurabilmesi için öncelikle ülkede demokratik kurumların yerleşmiş olması gerekmektedir. Sansür ve gözetimden korunmanın yolu da şeffaf, hesap-verebilirliği yüksek kurumlar ve bağımsız mahkemeler ile mümkündür. Bunlar olmadığı taktirde şebekeleşmiş otoriterlik sansürün ve gözetimin daha yeni formları ile karşımıza çıkacak ve interneti, demokrasiyi değil otoriteryanizmi güçlendirmek için kullanacaktır.

Kaynakça

Anti, M. (2012). Michael Anti: Behind the Great Firewall of China [Video dosyası]. https://www.ted.com/talks/michael_anti_behind_the_great_firewall_of_china adresinden erişilmiştir.

Barber, B. R. (1998). Three scenarios for the future of technology and strong democracy. *Political Science Quarterly*, *113*(4), 573-589.

Becker, T. (1981). Teledemocracy-Bringing power back to people. *Futurist*, *15*(6), 6-9.

Bremmer, I. (2010). Democracy in cyberspace: What information technology can and cannot do. *Foreign Affairs*, 86-92.

Calingaert, D. (2010). Authoritarianism vs. the Internet. *Policy Review*, (160), 63.

Carothers, T. (2002). The end of the transition paradigm. *Journal of democracy*, *13*(1), 5-21.

Chander, A. ve Le, U. P. (2014). Breaking the Web: Data localization vs. the global internet. Emory Law Journal, Forthcoming, UC Davis Legal Studies Research Paper No. 378.

Deibert, R. (2015). Cyberspace under siege. *Journal of Democracy*, *26*(3), 64-78.

Deibert, R. ve Rohozinski, R. (2010a). Liberation vs. control: The future of cyberspace. *Journal of Democracy*, *21*(4), 43-57.

Deibert, R. ve Rohozinski, R. (2010b). Control and subversion in Russian cyberspace. *Access controlled: The shaping of power, rights, and rule in cyberspace*, 15-34.

Diamon, L. (2010). Liberation Technology. *Journal of Democracy*. 21 (3), 69-83.

Diamond, L., Plattner, M. F. ve Walker, C. (Ed.). (2016). *Authoritarianism goes global: The challenge to democracy*. JHU Press.

Ferdinand, P. (2000). The Internet, democracy and democratization. *Democratization*, *7*(1), 1-17.

Grossman, L. K. (1995). *The electronic republic: Reshaping democracy in the information age*. Viking Penguin.

Gunitsky, S. (2015). Corrupting the cyber-commons: Social media as a tool of autocratic stability. *Perspectives on Politics*, *13*(1), 42-54.

Hague, B. N. ve Loader, B. (Ed.). (1999). *Digital democracy: Discourse and decision making in the information age*. Psychology Press.

Han, R. (2015). Manufacturing consent in cyberspace: China's' fifty-cent army'. *Journal of Current Chinese Affairs*, 44(2), 105–134.

Herszenhorn, D. M., & Barry, E. (2011). Putin contends Clinton incited unrest over vote. *New York Times*, *8*.

Hill, J. (2014). The growth of data localization post-snowden: Analysis and recommendations for us policymakers and business leaders. *The Hague Institute for Global Justice, Conference on the Future of Cyber Governance.*

Jiang, M. (2010). Authoritarian deliberation on Chinese internet. *Electronic Journal of Communication*, 20 (3&4).

Karlekar, K. ve Cook, S. (2009). Access and control: A growing diversity of threats to internet freedom. *Freedom on the Net*, 1-11.

Kelly, S., Earp, M., Reed, L., Shahbaz, A. ve Truong, M. (2014). *Freedom on the net: 2014*. Freedom House. https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf adresinden erişilmiştir.

MacKinnon, R. (2011). China's "networked authoritarianism". *Journal of Democracy*, *22*(2), 32-46.

MacKinnon, R. (2012, 28 Ocak). China's "networked authoritarianism". *National Post*, (Mart 2018) https://nationalpost.com/opinion/rebecca-mackinnnon-chinas-networked-authoritarianism adresinden erişilmiştir.

Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: Understanding Russian Internet policy. *Media and Communication*, *5*(1).

Morris, D. (2000). Direct democracy and the internet. *Loy. LAL Rev.*, *34*, 1033.

Nathan, A. J. (2003). Authoritarian resilience. *Journal of Democracy*, *14*(1), 6-17.

Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs*, *91*(1), 111-130.

Pearce, K. E. ve Kendzior, S. (2012). Networked authoritarianism and social media in Azerbaijan. *Journal of Communication*, *62*(2), 283-298.

Reuter, O. J. ve Szakonyi, D. (2015). Online social media and political awareness in authoritarian regimes. *British Journal of Political Science*, *45*(1), 29-51.

Ratkiewicz, J., Conover, M., Meiss, M. R., Gonçalves, B., Flammini, A. ve Menczer, F. (2011). Detecting and tracking political abuse in social media. *ICWSM*, *11*, 297-304.

Sargsyan, T. (2016). Data localization and the role of infrastructure for surveillance, privacy, and security. *International Journal of Communication*, *10*, 17.

Stockmann, D. (2013). *Media commercialization and authoritarian rule in China*. Cambridge University Press.

Van Dijk, J. A. G. M. (2012). *The network society*. Sage.

Vendil Pallin, C. (2017). Internet control through ownership: the case of Russia. *Post-Soviet Affairs*, *33*(1), 16-33.

World Internet Usage and Population Statistics. (2017, 31 Aralık). 18 Mart 2018 tarihinde https://www.internetworldstats.com/stats.htm adresinden erişilmiştir.