Networked Authoritarianism Is on the Rise*

Tobias Burgers / David R. S. Robinson

Abstract: This paper argues that authoritarian states have flouted the utopian hope of networked platforms favoring democracy and free speech. Over the last decade, platforms have instead helped authoritarian states to surveil, track and control their populations. China pioneered, and other nations followed, a model of *networked authoritarianism*. As a result, questions are raised about the utility of such platforms.

Keywords: Networked platforms, networked authoritarianism, China, digital politics
Schlagwörter: Vernetzte Plattformen, digitaler Autoritarismus, China, digitale Politik

1. Introduction

Networked platforms are institutionally controlled, technological systems which enable one-to-one (personal), one-to-many (mass), and many-to-many (social) modes of communication, have been lauded as a tool for liberal political change. Research by the Internet and Democracy Project at Harvard's Berkman Center for Internet and Society gave examples of how networked platforms supported the development of democracy and free speech. Goldstein's (2007) report on Ukraine's Orange Revolution showed how citizens used networked platforms to create and access an alternative mass media. At the same time, citizens used the same platforms to rapidly coordinate large protest groups (ibid 2007). Indeed, as McFaul (2005) noted, the revolution in Ukraine may have been the first whose success was largely dependent on networked platforms. Likewise, in Iran's politically unsuccessful Green Movement (2009), as well as in Egypt's Revolution (2011), networked platforms – foremost social media – played a major role (Bailly 2012; Moghanizadeh 2013). Networked platforms have also been used to resolve politically contested issues. Larry Diamond's description of the case of Sun Zhigang, a Chinese worker in the southern megacity of Guangzhou beaten to death in custody because he failed to provide valid temporary residence papers, shows how networked platforms were used by Chinese citizens to place a focus on police violence and close, notoriously rough detention centers (Diamond 2010). Networked platforms have proven useful in less violent circumstances, too. In Taiwan's student-led Sunflower movement, networked platforms were used to quickly mobilize students, to counterpoint government media narratives, and to liaise with both the press and the government (Chen et al. 2014).

The examples illustrate to what degree networked platforms empower the *demos* and contribute to democratic revolutions. It should thus come as no surprise that networked platforms are lauded as a liberating technology, a technology favoring those striving for equal justice, democracy and human rights (Eltahawy 2010). Larry Diamond coined the term "liberating technology", which he defined as: "any form of information and communication technology (ICT) that can expand political, social, and economic freedom. In the contemporary era, it means essentially the modern, interrelated forms of digital ICT—the computer, the Internet, the mobile phone, and countless innovative applications for them, including 'new social media' such as Facebook and Twitter" (Diamond 2010: 70). Indeed, from the late 1990s through the first decade of this century, networked platforms were hailed as technology that would liberate societies, enable free speech and eventually create a framework in which democracy could arise. This belief has influenced many authoritarian states to limit their population's access to networked platforms – particularly via the Internet.

However, networked platforms are also empowering for authoritarian states, empowering, as they offer states the ability to surveil societies to an unprecedented extent (Villasenor 2011). Fifteen years ago, Kalathil and Boas (2001) pointed out that authoritarian regimes were already reactively limiting their population's use of networked platforms for pro-democracy and free speech purposes. Since then, however, the situation has changed. States proactively rather than reactively use networked platforms. That is, they use the same platforms to improve the efficiency of intelligence and security services (Morozov 2011). Therefore, as much as it seems that networked platforms enable democracy, they likewise are a tool for authoritarian stability.

The success of some authoritarian nations, notably China, in openly promoting and proactively sponsoring the spread of this digital authoritarianism has meant globally decreased negative attitudes and perceptions toward digital authoritarianism. The Chinese digital governance model shows how networked platforms can stabilize, strengthen, and legitimize authoritarian governments (MacKinnon 2011: 36). Other nations, such as Russia, Turkey and Thailand, seeing the success of China, have sought to learn and implement the same digital authoritarian governance model (Freedom House 2016). A resulting shift is taking place, away from the hope of intrinsically "liberating technologies" toward the idea that networked platforms can contribute to population control and surveillance.

This article argues that networked platforms are not intrinsically democratic and that they can be tools of oppression. It will first show how networked platforms have actually been more suitable for surveillance and control. It will build on MacKinnon's (2011) model of digital authoritarianism, an argument that the Internet is both a tool and space used by states to strengthen authoritarian powers. However, her model excludes non-Internet networked technologies – e.g. Closed-circuit television (CCTV) and facial recognition software – which the authors include. As such, rather speaking of digital authoritarianism,

* This article has been double blind peer reviewed.
The authors very kindly wish to thank the reviewers for their insights, comments and suggestions.

https://doi.org/10.5771/0175-274X-2016-4-248
DOI: 10.5771/0175-274X-2016-4-248

we seek to use the term networked authoritarianism. After outlining this model, the paper will discuss how, in China, networked platforms are used to produce a form of networked authoritarianism on steroids. It will subsequently illustrate the success of the "Chinese model" and show how Chinese networked authoritarianism has been globally both cloned and accepted. It will conclude by speculating on the near future, to understand to what extent we should reconsider networked platforms as an enabler of global control rather than democracy.

2. Network Platforms, Network Control

Networked platforms enable control by favoring surveillance and remote access by institutional actors. These capabilities are ideal for digital authoritarianism. Consider the best known example, the basis of the networked authoritarianism model: the Internet. It has long been regarded as a global free space under limited state control (AIV 2014; Kenney 2001; Tkacheva 2013). Issues such as "the rights to privacy, data protection, confidential communication and freedom of expression [are] notable examples of Internet freedom" (AIV 2014: 6). However, this notion of Internet freedom is fading. New users in China and Singapore, among others, must register their websites and blogs with government identification, and they must agree with conditions that limit their speech – violation of these conditions would lead to a juridical response (China IPR SME Helpdesk 2015; Freedom House 2015).[1] These rules are both for individuals as well as for groups, such as NGOs or the press, and noncompliance results in arrest and jail time. China has gone so far as to require the registration of real names in order to use popular instant-messaging services, and the comment sections of websites and forums (Caragliano 2013; Freedom House Ibid). South Korea too pursued a similar real-name registration policy, until its constitutional court revoked it in 2012, deeming the policy a violation of free speech (Suh-Young 2012). The acceptance of real-name registration marks a departure of the relative anonymity that long existed on the Internet. As Lee and Liu (2016) note, this has also created incentives for other major – Western – companies such as Google and Facebook to pursue similar policies. Accordingly, access to the Internet is becoming dependent on providing one's personal details. This destroys the entire concept of anonymity in digital space. It also facilitates authoritarian-oriented nations to use the Internet, and in particular social media, as a tool for tracking dissidence.

The Internet is not the only tool and space in which control, regulation and surveillance have increased (MacKinnon 2011). Mobile phones, now the primary mode of Internet access, have proved ideal tools to track citizens and to monitor their movements and communications. This starts with the policy of providing identification when buying a Subscriber Identity Module (SIM) card or registering a phone contract – a policy that is nearly universal (GMSA 2013). This registration data is used by authorities to associate phone use with identities, through the use of, for example, international mobile subscriber identity (IMSI) catchers. Over the last decade, this remained a novel approach with the use of mobile phones favoring protest movements. Governments facing large protests would often, instead, shut down cellular networks (Kavanaugh et al. 2011). Indeed, the protest squares of Egypt, Iran and Ukraine frequently had no signal, with cellular service disabled over entire blocks. However, as Steinert-Threlkeld et al. (2015: 8) and Owsley (2015) note, governments now use cellular data to track citizens, with the help of "dirt boxes."[2]. The ability to record the movements and associations of individuals turns cellular networks to the government's benefit. Rather than shutting them down, Scheid (2013) notes, governments now proactively use cellular networks. They use gathered data to prevent protests and potentially subversive gatherings, to spread propaganda, and to warn possible protesters that the government is aware of and tracking them, such as happened in Egypt and Iran. Helped by the companies like Hacking Team, governments can monitor, access, and alter citizens' mobile phones (Kushner 2016). In an era when much is done via phones – from banking, to dating, to communication – these abilities are valuable tools for authoritarian states to surveil and control. A security service is not only capable of following a possible dissident, but can access his or her data, profile family and friends, and even alter data to discredit the targeted person or group (ibid 2016). Even if one can get an unidentified SIM card, or turns off their phone, tracking is still possible. The main processor, running a user facing operating system such as Apple's iOS, or Google's Android, may be turned off but the operator facing baseband processor will remain active – allowing for phones to remain tracked (Burel et al. 2002). Likewise, security agencies are capable of installing software that ensures a phone remains connected to the cellular network. Only if the battery is entirely removed is tracking no longer possible (Gallagher 2013). It is impossible to evade digital control via cellular data. Furthermore, it is easy to track the metadata of various data transmissions. Edward Snowden revealed exactly how wide the use of metadata is with regard to the tracking, collection and monitoring digital data (Mornin 2014).

Beyond the use of cellular data and the Internet, the core of MacKinnon's digital authoritarian model, governments have additional technological options. It is these non-Internet networked platforms that lead to a more capable and intrusive version of MacKinnon's model. We define this evolved model as networked authoritarianism. First to mention are CCTVs. They have increased in quantity. It is now impossible to visit any major city without being recorded. They have increased in quality. The days of grimy, black and white pixels are over. Combined with facial recognition software (FRS) and license plate tracking software, persons and their vehicles, in public and private spaces, can be tracked. Further enhanced by cutting-edge algorithms, Smart closed circuit televisions (CCTVs) are able to autonomously track persons (Brey 2004). And as Introna and Wood (2004) point out, once biometric facial or gait data is recorded, there is no way to avoid the software (Best and Begg 2006). In addition, it is impossible to distinguish between a regular

1 In China, for example, that could mean that the respective person registering the website would need to agree not to post their website or blog for purposes deemed anti-government, such as pro-democracy or human rights.

2 A dirtbox (DRT box) is a device that creates a powerful signal that overrides the official phone company towers. Nearby mobile phones automatically switch to this signal, allowing the operator to control nearby phones and intercept their communications.

CCTV and a smart one, thereby making it what Introna and Wood (ibid) call a "silent technology", silent in that there is no visible sign of use. Furthermore, once identified, further searches can be conducted on the historical movements of subjects. Cars are tracked similarly. Recognition software tracks license plates, allowing actors to register and follow the car (ACLU 2013).

Even vocal speech is subject to surveillance through evolved networked platforms. Vocal speech used to be difficult to track. Recording conversation required sophisticated microphones of limited range. However, a new generation of microphones is now capable of recording at high quality and at long distances. These systems, with names such as Shotspotter, initially enabled military and police to quickly know where a gunshot was fired (Benjamin 2002). However, these systems record other sounds, ranging from barking dogs to birds, and human voices (ibid). In Oakland, a shooter was identified not because a gunshot was located and officers arrived on time; but, because the victim mentioned the name of the shooter.[3] In addition, CCTV systems increasingly have microphones. This means vocal communication via non-digital means – that is a simple conversation – are now overheard, recorded and stored (Klitou 2014: 141). Through the use of recognition software, voices can be selected and the conversations of subjects "followed" as they pass through monitored areas (ibid).

The examples illustrate how it has become technologically possible to develop an evolved networked authoritarianism model capable of surveilling both the digital and physical world. The success of this model is as much economic as technical. The economics of the digital revolution has provided nearly half of the world's population with access to both cellular and Internet service (Kalahil and Boas 2003; ITU 2015). As the number of users increases, so have opportunities to track, surveil and control. The cost of surveillance technology has lowered as well (Bankston & Soltani 2014). Indeed, as Drew Cohen (2014) points out, it costs the NSA 0.065 USD an hour, per citizen to spy on the US population. Actors acquire significant electronic surveillance capabilities with limited budgets. Furthermore, the price of data storage has also decreased. A decade ago, storing gigabytes was expensive and cumbersome. Now, as Dutta and Hasan (2013: 1) argue, "storage appears to be free or very cheap, and there is an illusion of infinite storage". This has enabled security agencies to simply collect and store incredible amounts of data, to use when the opportunity arises. In the words of Villasenor (2011: 1), "it is now possible to record nearly everything". This ability fundamentally changes the notion of surveillance, tracking and control. Before, targets were first located, then surveilled in detail, tracked and monitored. But now it is possible to retroactively surveil, thereby creating what Villasenor (2011: 1) describes as surveillance time machine. In this regard, the past as much as the present becomes part of the networked authoritarianism model. Such would only increase fear among citizens to contradict the goals of an authoritarian ruler. After all, one mistake or one word misspoken could put one's loved ones or oneself in danger.

3 CBS SF Bay Area, Oakland's Shotspotter Equipment Records Voice Conversations, online news report, available at http://sanfrancisco.cbslocal.com/2014/05/21/shooting-crime-privacy-tech-oaklands-shotspotter-equipment-records-voice-conversations/ (accessed 5/7/2016).

3. Evolved Network Authoritarianism Manifest: The Case of China

Nowhere has evolved networked authoritarianism manifested itself more than in China. Over the course of the last two decades, the Chinese government both limited the political democratic value of networked platforms, and at the same time use them to enhance surveillance and control (Jiang 2016: 30, 31). The most well-known element has been the Great Firewall, a system of connected firewalls intended to block content deemed inappropriate by Chinese censors (MacKinnon 2011). With the firewall, the Chinese state has built a national version of the Internet, in which it holds full power and exercises control at will. China's Internet governance model is unique, in having nationalized its part of the global Internet; contrary to other nations, where national Internet boundaries remain fluid. Furthermore, and more importantly, it succeeds in controlling its national cyberspace through both automated blocking as well as with an army of censors, estimated up to tens of thousands in size, who patrol the web searching for anything deemed politically unacceptable (King et al. 2013). Much of this desire to build a "harmonious and healthy Internet development" as the Chinese government euphemistically called their Chinese version of the internet, one free of any government criticism, – and its effectiveness have been the result of coopting commercial entities, whom must abide by Chinese laws by signing declarations to support censorship (MacKinnon 2012: 68). All major Chinese internet companies, such as Tencent, SINA and Baidu, have staff dedicated to the censorship process (ibid).

Censorship on the web is part of a larger surveillance effort, which seeks to process, track and control most networked platforms. Within this surveillance network, Internet communication is a major component, but so is the tracking and recording of cellular data. This network extends over all mobile data and cellular service providers. The government has the capability to track locations, read messages and even to transform phones into listening devices. Both cell phones and cellular networks have the capability for so-called "lawful access" built into them by the private industry in partnership with governments (Meyer 2015). The acquired data is used to intimidate, warn, pressure and even blackmail anyone the government deems a risk (Langfitt 2013). At the same time, the government has installed over 20 million surveillance cameras in the last years, with CCTV coverage in over 97% of China's cities (ibid).

The result of these efforts have not been total control; but, rather a broad understanding that the state can find, and can track and monitor, at any time. As such, the achievement is the idea of total control, rather than actual total control. Of course, the evolved authoritarian model depends on the political situation and willingness of those participating within it to accept it. As Denyer (2016) notes, in areas in western China, such as Tibet and the Muslim dominated province Xinjiang, where government opposition is high, the model is more prevalent than in the eastern provinces, where the public is more supportive of the government. In this, the Chinese model rewards loyalty. The ultimate expression of this is an entire new control system, which citizens ostensibly can voluntarily join. This society spanning network platform, called the social credit system, incorporates

all data it can possibly acquire with the aim of ranking a citizen's trustworthiness. This spectrum of data ranges from that of social status, credit history, social connections, digital interaction, use of social media, online consumption and behavioral patterns (Creemers 2014; Hsu 2015). The catch of this system, which builds on an existing commercial system – Sesame, used by Internet giant Alibaba – is it awards users providing more data with more benefits. These benefits range from a wider range of potential partners on dating apps, to visa waivers for foreign travel. Those with a low rating will be unable to book hotels, rent cars or purchase goods via credit card. This system is a novel approach in any authoritarian model, as generally such structures are enforced by power.

The Chinese Government has mastered the use of networked platforms. It has expanded their scope to surveil an entire society, in both the digital and physical world. As Zheng (2007) and MacKinnon (2011) note, China has illustrated how networked platforms can be used to prolong authoritarian rule; and, quite absurdly, how said rule can be made attractive to its citizens. China seems to have mastered and elevated the Panopticon concept to the 21st century – a digital Panopticon – one in which there is strong incentive to remain inside of it, even if one has already served his or her time.[4]

4. Networked Authoritarianism Going Global?

The Chinese success has demonstrated to other nations how networked authoritarianism is possible. If the Chinese government is able to surveil, control, track and curtail more than 1.3 billion people, it is apparent to other nations, with smaller populations, that they can do this too. As such, authoritarian nations now seek to copy the "Chinese evolved model" – often with the help of China (MacKinnon 2011). As Denyer (2016) notes, China openly advocates its model to the rest of the world. As Howard et al. (2011) and Fielder (2012) both note, the standard operating procedure for authoritarian states had been to shut down networked platforms when used as a tool by dissident or anti-government activity. However, in the recent years, nations such as Kazakhstan, Egypt, Azerbaijan, as well Singapore, among others, have sought to more proactively use networked platforms, aligned more with the Chinese model (Anceschi 2015; Pearce and Kendzior 2012; Pearce and Guliyev 2015). Thus, the spreading authoritarian use of networked platforms is normalizing and competing with the influence of the western notion of digital democracy and networks as a force for "good".

5. Conclusion

MacKinnon's model of networked authoritarianism has evolved. Originally focusing solely on the Internet, it now includes all networked platforms. It enables the surveillance of the digital and physical realms. The evolved model has seen political success too, because China's embrace of networked authoritarianism has resulted in its acceptance as a valid view in the global debate on the utility of networked platforms. Others nations – ranging from very authoritarian to moderately so – are building on China's vision.

Further research is needed on the future of networked platforms and their political utility. This research should be multipart. First, it should both predict and track how the networked authoritarianism model develops in the future. The effectiveness and pervasiveness of social control through the inclusion of additional technologies is as yet unknown. Second, research is needed to find counters to the rise of the networked authoritarianism model. Such research should focus on current and future technologies and countermeasures to their use in surveillance and oversight. The success of the networked authoritarianism model has been as much technological as political. Therefore, any research in developing alternatives must also address the political success of this model. A new narrative is needed to counter blind faith in digital technology. For it favors surveillance, oversight and enables control, online and offline. If we seek to counter the networked authoritarianism model, we must first change the narrative on technology itself. This article is a modest contribution and hopefully will serve as the basis for such further research.

4 The original concept of Panopticon dates back to the works of the 18th century English philosopher and social theorist Jeremy Bentham, who developed the Panopticon as a concept for a prison. The idea behind this concept is that in theory the inmates could be watched over, at all times, unaware if they were actually watched over or not. This way, the concept allows for an idea of perpetual possible surveillance, leaving the surveilled unaware if surveillance is actually taking place.

Tobias Burgers is currently a Doctoral Candidate at the Otto Suhr Institute, Free University Berlin, from which he holds a diploma in political science. His research interests include the impact of cyber and robotic technology on security dynamics, East-Asian security relations and the future of conflict.

David R.S. Robinson is a freelance technologist, formerly of Microsoft and ThoughtWorks. Over his 15-year career, he has consulted for both private business and government, as well as spoken at numerous conferences on topics in information technology.

References

Advisory Council on International Affairs, 1st Initial. (2014). The Internet. A global free space with limited state control, Advisory Council on International Affairs to the Royal Dutch Foreign Ministery, report 92, available at http://www.ivir.nl/syscontent/pdfs/83. [Accessed: May 5th 2016]

American Civil Liberties Union. (2013). You are being track. How License Plate Readers Are Being Used To Record Americans' Movements, available at https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf, [Accessed: May 7th 2016]

Anceschi, L. (2015).The Persistence of Media Control Under Consolidated Authoritarianism: Containing Kazakhstan's Digital Media., Demokratizatsiya: The Journal of Post-Soviet Democratization, vol. 23 no 3, pp. 277-295

Bailly, J. (2012). The impact of Social Media on Social Movements: A Case Study of the 2009 Iranian Green Movement and the 2011 Egyptian Revolution , MA thesis, Washington State University.

Bankston, K.S. and Soltani, A. (2014). Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones, in The Yale Law Journal, Volume 123, available at http://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones, [Accessed: May 9th 2016]

Benjamin, C. (2002). Shot Spotter and FaceIt: The Tools of Mass Monitoring. , UCLA Journal of Law and Technology, vol. 6. , pp.1-24.

Best, R. & Begg, R. (2006). Overview of Movement Analysis and Gait Features. In Begg, Rezaul, Palaniswami & Marimuthu, Computational Intelligence for Movement Sciences: Neural Networks and Other Emerging Techniques. Idea Group

Brey, P. (2004). Ethical Aspects of Face Recognition Systems in Public Places, Journal of Information, Communication & Ethics in Society, 2:2, 97-109.

Burel, G.; Quinquis, A.; Azou, S. (2002). Interception and furtivity of digital transmissions, Paper presented at the IEEE Communications conference, December 5-7, Bucharest, Romania

Caragliano , D. (2013). Why China's 'Real Name' Internet Policy Doesn't Work, The Atlantic. Available at http://www.theatlantic.com/china/archive/2013/03/why-chinas-real-name-internet-policy-doesnt-work/274373/ [Accessed: Jun 1st, 2016].

Chen, B.; Liao, D.; Wu, H. (2014). The Logic of Communitive1 Action: A Case Study of Taiwan's Sunflower Movement, Available at http://ipp.oii.ox.ac.uk/sites/ipp/files/documents/IPP2014_Chen.pdf

China ipr sme helpdesk. (2015). Registering and Protecting Chinese Domain Names, Available at http://www.china-iprhelpdesk.eu/sites/all/docs/publications/China_IPR_SME_Helpdesk-domain_name_Guide.pdf [Accessed: May 12th, 2016]

Cohen, D.F. (2014). It Costs the Government Just 6.5 Cents an Hour to Spy on You, Politico (online), available at http://www.politico.com/magazine/story/2014/02/nsa-surveillance-cheap-103335 [Accessed: Sept 12th, 2016]

Creemers, R. (2014). Planning Outline for the Construction of a Social Credit System (2014-2020), Available at https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020 [Accessed: Jun 6th, 2016].

Diamond, L. (2010). Liberation Technology, Journal of Democracy, vol. 21, issue3, pp.69-83.

Denyer, S. (2016). China's scary lesson to the world: Censoring the Internet works, Washington Post, May 23th, available at https://www.washingtonpost.com/world/asia_pacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html [Accessed: Jul 11th, 2016]

Dutta, A.; Hasan, R., 1st Initial. (2013). How Much Does Storage Really Cost? – Towards a Full Cost Accounting Model for Data Storage , pp. 29-43., in Proceedings of the 10th International Conference, GECON 2013, Zaragoza, Spain, September 18-20.

Eltahawy, M. (2010). Facebook, YouTube, and Twitter Are the New Tools of Protest in the Arab World, The Washington Post, available at http://www.washingtonpost.com/wpdyn/content/article/2010/08/06/AR2010080605094.html [Accessed: Nov 15th, 2015]

Freedom House, Silencing the Messenger: Communication Apps Under Pressure, online report, available at https://www.freedomhouse.org/report/freedom-net/freedom-net-2016, (accessed 7th December 2016)

Fielder, J. (2012). Dissent in digital: the Internet and dissent in authoritarian states, PhD (Doctor of Philosophy) thesis, University of Iowa, Iowa Research Online.

Freedom house. (2015). Freedom of the Net 2015: Privatizing Censorship, Eroding Privacy, Available at https://freedomhouse.org/sites/default/files/FOTN%202015%20Full%20Report.pdf [Accessed: Jun 1st, 2016]

Gallagher, R. (2013), NSA Can Reportedly Track Phones Even When They're Turned Off, report for Slate magazine, online, available at http://www.slate.com/blogs/future_tense/2013/07/22/nsa_can_reportedly_track_cellphones_even_when_they_re_turned_off.html [Accessed: 7th December 2016]

GSMA. (2013). The Mandatory Registration of Prepaid SIM Card Users, White Paper, available at http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf, [Accessed: May 10th 2016]

Goldstein, J. (2007). The Role of Digital Networked Technologies in the Ukrainian Orange Revolution, Berkman Center Research Publication 14.

Howard, P.; Agarwal, S.; Hussain, M. (2011). The Dictators' Digital Dilemma: When Do States Disconnect Their Digital Networks?, Issues in Technology Innovation, Issue 13 The Center for Technology Innovation at Brookings.

Hsu, S. (2015). China's New Social Credit System, The Diplomat. Available at http://thediplomat.com/2015/05/chinas-new-social-credit-system/ [Accessed: Jun 2, 2016] Introna, L.; Wood, D. (2004). Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems , Surveillance & Society, vol. 2. 3, pp. 177-198.

International Telecommunications Union. (2015). ICT facts and figures 2015, available at https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf, [Accessed: May 8th 2016]

Jiang, M. (2016). The co-evolution of the Internet, (un)civil society and authoritarianism in China, In deLisle, J. ,Goldstein A. & Yang, G. (eds.), The Internet, Social Media, and a Changing China (pp. 28-48). Philadelphia, PA: University of Pennsylvania Press.

Kalathil,S & Boas. T.C. (2001). The Internet and state control in authoritarian regimes: China, Cuba, and the counterrevolution, First Monday, Volume 6, Number 8, available at http://firstmonday.org/ojs/index.php/fm/article/view/876/785, [Accessed: May 18th 2016]

Kalathil, S. & Boas, C. (2003). Open Networks Closed Regimes The Impact of the Internet on Authoritarian Rule, Carnegie Endowment for International Peace,Washington D.C. Kavanaugh, A.; Yang, S.; Sheetz, S.; Li, L.T.; Fox, E.A. (2011). Between a rock and a cell phone: Social Media Use during Mass Protests in Iran, Tunisia and Egypt. Kenney, M. (2001). The Growth and Development of the Internet in the United States. Brie Working Paper 145, available at https://escholarship.org/uc/item/05z7r9mt, [Accessed: May 25th 2016]

King, G.; Pan, J.; Roberts, M.E. (2013). How Censorship in China Allows Government Criticism but Silences Collective Expression, in American Political Science Review, Volume 107, Issue 2, pages 1-18.

Klitou, D. (2014). Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century, Springer. Kushner, D. (2016). Fear this man, Foreign Policy (online), available at https://foreignpolicy.com/2016/04/26/fear-this-man-cyber-warfare-hacking-team-david-vincenzetti/ [Accessed: Jun 3rd, 2016].

Langfitt, F. (2013). In China, Beware: A Camera May Be Watching You. Available at http://www.npr.org/2013/01/29/170469038/in-china-beware-a-camera-may-be-watching-you [Accessed: Jun 6th, 2016].

Lee, J.; Liu, C., 1st Initial. (2016). Real-Name Registration Rules and the Fading Digital Anonymity in China, Washington International Law Journal,, vol. 25. 1, pp. 1-35.

Mackinnon, R. (2011). China' s Networked Authoritarianism., Journal of Democarcy, vol. 2. 2, pp.32-46.

MacKinnon, R. (2012). Consent of the Networked: The Worldwide Struggle for Internet Freedom, Basic Books Press, New York City, USA.

Meyer, R. (2015). How the Government Surveils Cellphones: A Primer. The Atlantic (online). Available at http://www.theatlantic.com/technology/archive/2015/09/how-the-government-surveils-cell-phones-a-primer/404818/, [Accessed: Sep 28th, 2016]

Mornin, J.D. (2014). NSA Metadata Collection and the Fourth Amendment, in Berkeley Technology Law Journal, Volume 29, Issue 4, Pages 985-1006.

Owsley, B. (2015). Spies in the skies: Dirtboxes and airplane surveillance, Michigan Law Review First Impressions, vol. 113. 75, pp. 75-84.

Pearce, K. E. & Guliyev, F. (2016). Digital knives are still knives: The affordances of social media for a repressed opposition against an entrenched authoritarian regime in Azerbaijan on panel Opposition 2.0: Challenging authoritarianism in the 21st century. Paper presented to the Association for the Study of Nationalities Conference, New York, NY.

Pearce , K. & Kendzior, S. (2012). Networked Authoritarianism and Social Media in Azerbaijan, Journal of Communication , vol. 62. , pp.283–298.

Rushkoff, Douglas, (2002). Renaissance Now! Media Ecology and the New Global Narrative. Hampton Press. pp. 26–28.

Steiner-Threlkeld, Z.; Mocanu, D.; Vespignani, A. & Fowler, A. (2015). Online social networks and offline protest, EPJ Data Science, vol. 4. 19, pp. 1-9.

Suh-Young , Y. (2012). Online real-name system unconstitutional, Korea Times, Aug 23, available at http://www.koreatimes.co.kr/www/news/nation/2012/08/117_118115.html [Accessed: May 7th 2016]

Tkacheva, T.; Schwartz, L.; Libicki, M. (2013). Internet freedom and political space, RAND research report, available at https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR295/RAND_RR295.sum.pdf, [Accessed: May 19th 2016]

Van dijk, J. (2013). Digital Democracy: Vision and Reality, in I. Snellen & W. van de Donk Public Administration in the Information Age: Revisited.

Villasenor, J. (2011). Recording Everything: Digital Storage as an Enabler of Authoritarian Governments, Center for Technology Innovation at Brookings research paper, available at ttp://www.brookings.edu/~/media/research/files/papers/2011/12/14-digital-storage-illasenor/1214_digital_storage_villasenor.pdf, [Accessed: May 12th 2016]

Zheng, Y. (2007). Technological Empowerment The Internet, State, and Society in China, Edition of book, Stanford University Press, Stanford, CA.