Article

How Dictators Control the Internet: A Review Essay

Comparative Political Studies
2020, Vol. 53(10-11) 1690–1703

DOI: 10.1177/0010414020912278
journals.sagepub.com/home/cps

Eda Keremoğlu[1] and Nils B. Weidmann[1]

Abstract

A growing body of research has studied how autocratic regimes interfere with internet communication to contain challenges to their rule. In this review article, we survey the literature and identify the most important directions and challenges for future research. We structure our review along different network layers, each of which provides particular ways of governmental influence and control. While current research has made much progress in understanding individual digital tactics, we argue that there is still a need for theoretical development and empirical progress. First, we need a more comprehensive understanding of how particular tactics fit into an overall digital strategy, but also how they interact with traditional, "offline" means of autocratic politics, such as cooptation or repression. Second, we discuss a number of challenges that empirical research needs to address, such as the effectiveness of digital tactics, the problem of attribution, and the tool dependence of existing research.

Keywords

autocracy, ICT, repression

Introduction

In most autocratic regimes, governmental interference in digital infrastructure and communication is commonplace. Governments control where and when modern communication technology (ICT) is introduced in the first

[1]University of Konstanz, Germany

Corresponding Author:
Nils B. Weidmann, University of Konstanz, Universitätsstraße 10, 78457 Konstanz, Germany.
Email: nils.weidmann@uni-konstanz.de

place, who gets access to it, and what information is communicated. This influence occurs for political motives—to ban opposition activists from mobilizing their followers online, to contain the spread of information that is critical of the regime, or to spy on the population to identify potential dissenters. Examples include Hosni Mubarak's complete internet shutdown in January 2011 (Dainotti et al., 2014), or the censoring of online content deemed unacceptable by the Chinese government (King et al., 2013). In this review article, we take stock of the literature on autocratic interference in internet communication, but also identify gaps and propose pathways for future research.

The fact that dictatorships interfere in communication is not surprising, nor is it a new subject of study in political science. In fact, some of the classic work on authoritarian rule has emphasized the importance for autocrats to control the flow of public and private information (Friedrich & Brzezinski, 1965). In the digital age, this has become a greater challenge, but at the same time a tremendous opportunity for autocrats. Technological progress has vastly expanded the complexity, reach, and bandwidth of communications, requiring higher levels of technical sophistication for governmental interference. At the same time, however, digital communication technology opens up new possibilities for (fully or partly) automated interference: censorship software can automatically detect and block unwanted content, and network traffic can be scanned to single out users transmitting suspicious information.

Our review focuses on the different network layers that can be used for interference. In using a (simplified) technology-centered structure for our discussion, we do not mean to suggest that these are the only means of authoritarian influence over the internet. Most regimes rely also on political and legal measures to regulate the provision of telecommunication services and the actors involved. However, once internet services are available to large segments of the population—which is now the case in the vast majority of countries worldwide—internet control usually means tampering with the network infrastructure, the data traffic, and the content being transmitted. After our review of the literature, we conclude our essay with a discussion of the theoretical and empirical challenges that future research in this field should address.

Interference at Different Layers

The internet is constructed as a system of stacked network "layers," each of which uses and expands the functions provided by the lower ones.[1] For the purpose of our review, we distinguish between three layers: the *infrastructure*

layer, which includes hardware and cables to establish and maintain a connection; the *network* layer, which ensures that data packets are properly routed from source to destination; and the *application layer* that consists of the software tools that enable users to send and receive information over the network. In the following sections, we review the different ways in which governments can influence internet communication at these layers.

Infrastructure Layer

While earlier research found that autocracies were lagging behind in digital innovation and internet penetration rates were lower as in their democratic counterparts (Milner, 2006), more recent work found that they have now caught up (Stier, 2017). To some observers, this delay was a deliberate strategic choice, and internet service was not granted before accompanying control mechanisms were installed (Boas, 2006). Nonetheless, even today some governments are involved in meddling with the general infrastructure for digital communication. Research has found that governments still play a crucial role in access allocation, and service provision is systematically lower for politically excluded ethnic groups (Weidmann et al., 2016).

However, even when the infrastructure is in place, there are other means to temporarily disable the entire infrastructure (Deibert & Rohozinski, 2010). This means that in the case of political events that are potentially threatening to a regime, "just-in-time" shutdowns allow governments to temporarily disconnect parts of or the whole population (Dainotti et al., 2014; Deibert et al., 2010; Freyburg & Garbe, 2018; Gohdes, 2015). However, there are also other means to calibrate country-wide access. Those include tampering with digital communication by throttling bandwidth to the extent that browsing of either the internet or specific applications becomes nearly impossible (Ogola, 2019).[2]

Network Layer

The network layer is highly susceptible to intervention and provides governments with the means to fine-tune control while the infrastructure remains intact and usable otherwise. Several studies have found that authoritarian governments systematically censor information and communication they deem to be critical. To do so, the network layer provides various tools such as filtering mechanisms based on critical keywords or senders/receivers of data packets (Hellmeier, 2016; Murdoch & Anderson, 2008; Zittrain & Palfrey, 2008). China's "Great Firewall" is the most popular example of internet censorship where the government aims to regulate what content

citizens can see and which applications they can use. This is achieved by blocking connections to specific websites and services, thereby creating a highly regulated "national intranet" (Kalathil & Boas, 2003). In addition to these refined techniques, so-called denial-of-service attacks provide a relatively cheap way of censoring information where automated control cannot be implemented easily. These attacks take down a website by swamping the hosting server with requests up until the point that it cannot be reached anymore (Lutscher et al., 2020; Nazario, 2009; H. Roberts et al., 2012). This is a particularly effective tool if servers hosting opposition websites are located outside a government's jurisdiction. In cases where domestic companies own those servers, governments often have legal and illegal means to compel providers to comply with governmental control practices (Deibert & Rohozinski, 2010).

We also know that governments interfere with the network layer to monitor opposition and citizens. By manipulating routing, authorities can force digital traffic to go through a government provider before it reaches its destination. A recent example is the re-routing of telegram messages through state providers in Iran, which gave the government the opportunity to access the content of these messages (O'Neill, 2018). Other techniques, such as deep packet inspection, constantly scan traffic and provide automated surveillance for authorities (Fuchs, 2013). As a result, potential dissidents can be identified by tracking down users attempting to transmit or access allegedly threatening content (Deibert et al., 2008).

Application Layer

Interference with the application layer is where most of the research on autocratic internet control has been done. There are at least four ways in which autocrats make use of the internet. First, autocrats control and censor content where filtering at lower levels fail or is not available. Authorities are keen to review social media posts and have contentious messages removed (King et al., 2013) to ensure that potential threats remain invisible. These tactics are complemented with more sophisticated ones that do not block, but rather impede, access to information. The Chinese government, for instance, taxes information and makes users "pay money or spend more time if they want to access the censored material" (Roberts, 2018, p. 2).

Second, we know that an increasing number of governments complements censorship with pro-active framing and manipulation of information (Deibert, 2015). Authorities co-opt social media (Gunitsky, 2015), flood the web with distracting messages (Munger et al., 2018; Roberts, 2018), and thereby influence what is communicated. Here, authorities propagate a

pro-government image and attempt to spread information about its strength and popularity (Guriev & Treisman, 2019; MacKinnon, 2011; Spaiser et al., 2017). Oftentimes, this is done with the help of paid users (Han, 2015; King et al., 2017). However, more aggressive tactics, such as spreading discrediting information on opposition actors, or even harassment of users online, are also commonly employed (Tucker et al., 2017).

Third, the public character of online communication also facilitates surveillance. Public social media posts can reveal crucial information about dissidents and opposition activity. Oftentimes, private internet providers are forced to share information on critical users, which can be used to track down their real identity (Deibert et al., 2008). In some cases, governments are quite open about their surveillance practices. In China, for instance, two virtual police officers remind citizens that their browsing behavior is monitored (King et al., 2013). Whether autocrats monitor openly or not, news websites, opposition actors, and citizens usually know that they are being watched, which can ultimately lead to self-censorship (Deibert & Rohozinski, 2010).

Finally, the internet can also mitigate the information dilemma autocrats are faced with (Wintrobe, 1998): while they want to learn about public preferences and potential grievances in order to avert threats of unrest (Chen & Xu, 2017; Gunitsky, 2015), they simultaneously restrict civil liberties and media freedom that would help them obtain this information. Rather than letting citizens voice their current demands publicly on social media, many autocrats install controlled venues of preference articulation. An increasing number of autocrats enhances e-governance structures that offer digital public services and feedback channels on particular public issues. In this way, authorities can retrieve information on mass preferences, calibrate policies, and increase perceived responsiveness (Gunitsky, 2015; Kalathil & Boas, 2003). Research suggests that these tools are not mere window-dressing, but that autocrats are actually responsive to citizens, especially when they fear collective action and unrest (Chen et al., 2016). These innovations further mitigate principal-agent problems between rulers and local officials when citizens help to detect corruption, which in turn is expected to alleviate grievances (Chen et al., 2016; Lorentzen, 2014).

Overall, the literature on authoritarian interference with the internet finds that governments oftentimes limit the provision and functionality of internet access and target the content of digital communication. Our review highlights that to do so, governments exploit various layers of the network structure and the opportunities they provide. Rather than understanding interference as an exclusive application-layer tactic, for instance, our review shows that different means of information control can and do take place at different levels, often invisible to the ordinary user.

Theoretical Shortcomings

Recent scholarship has made much progress to help us understand how autocrats interfere with online communication. Nonetheless, there are a number of shortcomings and gaps in the literature that should be addressed in future research. In this section, we discuss the need for more theoretical work on governmental interference, from the perspective of comparative autocracy research. We focus in particular on the interplay of different tactics of authoritarian control. Autocrats rarely ever use a single tactic to ensure political influence; similar to social movements and opposition groups (Horowitz et al., 2018), they rely on a portfolio of different tactics that together constitute a *strategy* for political survival (Tilly, 2010). Hence, to fully understand why an autocratic government employs particular tactics but not others, we need to adopt a broader perspective and examine autocratic repertoires or "toolkits"—different autocratic tactics in combination with each other. This stands in sharp contrast with existing work on governmental interference in digital communication, which has usually examined particular tactics such as shutdowns, censorship, or propaganda independently of others. We believe that this research agenda should be advanced in two ways, which we describe in more detail below.

The Autocrat's Digital Toolkit

As our literature review above has shown, most of the research in political science on digital interference remains confined to a single tactic, rather than examining it in combination with others. We have yet to understand better what "digital strategy" autocratic governments adopt to fend off challenges to their rule. As regards this strategy, there are two sets of questions that research should address.

First, we need to understand the overall purpose of the digital strategy. Autocrats may keep all interference secret, or they may censor blatantly in an open fashion to signal their strength. To what extent does this depend on whether they interfere preemptively to deter contention, or rather as a reaction to visible contention? Large-scale shutdowns may be signs of crises when used as a last-straw response to mobilized masses, whereas covert censorship may be motivated by precaution to avoid mobilization in the first place. Governments may also follow a more differentiated strategy and combine overt and covert tools. This seems to be practiced by the Chinese government, where a message from a fictitious "internet police" is displayed when a user accesses content that has been removed for political reasons (King et al., 2013). Other operations remain much less visible to the public

such as the censorship and surveillance functions built into many chat applications in China (Deibert, 2015, p. 67).

Second, we need to understand the relation between governments' digital strategy and the targets of interference. To what extent is interference directed at specific users or groups rather than targeting the population as a whole? An obvious example for the latter is internet shutdowns (Dainotti et al., 2014), while Chinese online censorship targets specific users and content (King et al., 2013). Also, how does the combination of tools change when different groups are targeted? In general, there are reasons to assume that more developed countries resort to more differentiated types of interference (Guriev & Treisman, 2019) and that some tactics work for ordinary citizens, but not the elites (Roberts, 2018). We have to keep potential targets in mind when we assess autocrats' tools of choice and differences among governments in their overall strategies.

Digital Tools and Conventional Tactics

Research has long argued that autocratic regimes select from a large repertoire of approaches to ensure political survival (Davenport, 2007; Gerschewski, 2013), for example by co-opting elites, increasing legitimacy, or by violently repressing dissent. With the advent of digital tactics, a regime's repertoire has expanded tremendously. How do these modern digital tools relate to established, conventional strategies of autocratic survival? In general, we can distinguish between three scenarios. First, digital tools can serve as replacement for conventional tools. For example, if a regime can effectively contain mass mobilization by censoring and blocking online channels, this reduces the need for violent repression of protest. This is what we call *substitution*. Second, digital interference can be used in addition to traditional means of control, as for example when a government restricts freedom of the press, but at the same time censors online channels. This is an instance of *reinforcement* of conventional tactics of control. Third, conventional and digital tactics may *complement* each other. This is the case if digital interference interacts with conventional strategies, for instance, when governments shut down the internet "just-in-time" to disrupt opposition forces' coordination and increase violent repression on the ground (Gohdes, 2015). Xu (2020) shows how digital interference helps the government to refine its conventional tools of repression and cooptation. Weidmann and Rød (2019) study the effect of internet technology on mobilization for protest and analyze how conventional tactics (violent repression of protest) interact with online mobilization. While these are first steps, future research needs to tackle these questions head-on.

Challenges for Empirical Analysis

In addition to the need to theoretically situate autocrats' digital tactics in their entire portfolio, there are several challenges we face in the empirical research on digital interference in autocracies.

Effectiveness of Digital Tactics

A key assumption in almost any analysis of autocratic interference is that it serves a political purpose, for example by deterring political challenges and helping autocrats to stay in power. Yet, there are few systematic tests of whether particular tactics are actually effective in achieving these ends. So far, research on the short-term impacts of "just-in-time" interference has produced results that are rather inconclusive. We know that large-scale shutdowns can facilitate offline repression of opposition groups during violent conflict (Gohdes, 2015). At the same time, however, interference can also backfire (Huang, 2018). Hobbs and Roberts (2018) find that China's blocking of Instagram motivated users to bypass also other blocks and spurred political interest and critical online discourse. Finally, Pan and Siegel (2020) suggest that repression of dissenters can also simply be ineffective even if it does not backfire.

An even larger gap exists when it comes to understanding the long-term impact of authoritarian interference. While some theoretical work suggests that the internet may impede non-democratic rule (Edmond, 2013), empirical research provides tentative support for cyber-pessimists who claim that the internet plays into the hands of autocrats (Rød & Weidmann, 2015). However, our understanding of the reasons for this is limited. Do efforts of information framing and manipulation, for instance, actually lead to increased perceptions of regime legitimacy among the public—and if so, does this in turn bolster authoritarian rule? Autocrats actively disseminate information in their favor, and while we know that propaganda may inhibit collective action (Huang, 2018), we do not know whether the recipients of these digital messages actually believe this information. Similarly, evidence also suggests that increased internet coverage reduces mobilization (Weidmann & Rød, 2019), but we again do not know whether this is because of the intentional use of digital tactics by governments.

Moreover, particular digital tactics employed by the government may even backfire and undermine autocrats' rule in the long run. When autocrats exclude certain groups from the internet, they establish new "digital divides" in the population, which in turn could increase grievances and motivations to mobilize. Even if digital tools do not backfire, they might simply be

ineffective. Roberts (2018) notes that friction, a form of "porous" censorship that requires users to spend more time or money to access information, does not hold back everyone from seeking censored content. In other instances, interference can be countered and blocks can be circumvented by knowledgeable users, despite governmental efforts to prevent this (Deibert et al., 2012).

The Attribution Problem

The problem of attribution is something that affects much research on digital interference: in most cases, it is difficult to identify the actors who actually intervene in online communication. While most instances of interference likely happen in secret, for the ones we are able to observe, we oftentimes cannot say with certainty that the government is actually responsible. Some forms of interference might not be carried out by or in the name of the government but by private actors. Even though the nature of interference might suggest a governmental act—for instance, when an opposition website is defaced or taken down by a DoS attack—we cannot be sure that it is not some loyal individual responsible for it (Villeneuve & Crete-Nishihata, 2012). The attribution problem is exacerbated when governments hire private companies and actors to interfere with the internet. These practices help autocrats to shift responsibility for censorship and surveillance (Deibert et al., 2012), which makes it even more difficult to analyze the nature and extent of government control. Similarly challenging are technical issues that make it difficult to judge whether an outage is the intentional result of an attack. If we mis-attribute a particular action, we risk over- or underestimating the extent to which autocrats are willing and able to control online communication. Addressing the attribution problem is difficult; in rare instances, we may be able to work with network forensics experts that are able to trace certain activities back to their origins.

Tool-Dependent Research

An increasing fraction of research is "tool-dependent," which means that it relies on very specific digital platforms (such as Twitter or Facebook) and, in addition, specific functions these platforms offer. This begs the danger of producing research and results that apply exclusively to this tool or functionality, but cannot easily be generalized. The challenge is to identify functionality that exists across platforms (e.g., posting "messages," or "sharing" information), such that we can at least theorize (but possibly also study) their impact independently of a particular platform. A second limitation imposed by tool-dependency is that research—by abiding to their terms of

service—has to adapt to possibly changing policies of those platforms, which can severely hinder ongoing research. A current example includes Facebook's recent closure of its Pages API, which impedes the legal and technical means of content extraction for research (Freelon, 2018).

Conclusion

Recent research has significantly increased our knowledge of the political role of digital communication in autocracies. Not surprisingly, autocrats make systematic use of digital tools and interfere with online communication to contain challenges to their rule. In this review, we have given an overview of the literature by referring to the key layers of the internet—the infrastructure, the network, and the application layer. We have also discussed theoretical gaps and empirical challenges in research on the internet's political role in non-democratic countries. Related to the former, we encourage research that looks at governments' overall strategy, both when it comes to the different digital tactics that governments have at their disposal, but also how they interact with conventional ones such as violent repression. For example, in the digital age, governments may resort to overt violent repression less frequently, because they can better anticipate and prevent potential dissent. Our article also discussed a number of empirical challenges that arise in the study of internet communication and autocratic rule: the need to analyze, rather than assume, the effectiveness of digital tactics, the difficulty of observing the perpetrators of digital interference, and the tool dependence of existing research. Overall, theoretical and empirical progress depend on each other; for example, being able to better observe a particular digital tool can help us theorize its relationship to other, conceptually distinct forms of interference. Similarly, we need to advance (and possibly revise) theories of conventional repression by considering the numerous ways in which dictators and their agents influence internet communication.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The authors gratefully acknowledge funding from the German National Science Foundation (DFG) under Research Grant 402127652.

ORCID iD

Nils B. Weidmann https://orcid.org/0000-0002-4791-4913

Notes

1. This idea is at the core of the Open System Interconnection (OSI) model, the most important conceptual model for computer networks.
2. While technically the latter examples refer to network interference, we include them with the work on access provision and control.

References

Boas, T. C. (2006). Weaving the authoritarian web: The control of Internet use in nondemocratic regimes. In J. Zysman & A. Newman (Eds.), *How revolutionary was the digital revolution? National responses, market transitions, and global technology* (pp. 361–378). Stanford University Press.

Chen, J., Pan, J., & Xu, Y. (2016). Sources of authoritarian responsiveness: A field experiment in China. *American Journal of Political Science*, *60*(2), 383–400.

Chen, J., & Xu, Y. (2017). Why do authoritarian regimes allow citizens to voice opinions publicly? *The Journal of Politics*, *79*(3), 792–803.

Dainotti, A., Squarcella, C., Aben, E., Claffy, K. C., Chiesa, M., Russo, M., & Pescapé, A. (2014). Analysis of country-wide Internet outages caused by censorship. *IEEE/ACM Transactions on Networking*, *22*(6), 1964–1977.

Davenport, C. (2007). State repression and political order. *Annual Review of Political Science*, *10*, 1–23.

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

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (Eds.). (2008). *Access denied: The practice and policy of global internet filtering*. MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (Eds.). (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace*. MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (Eds.). (2012). *Access contested: Security, identity, and resistance in Asian cyberspace*. MIT Press.

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

Edmond, C. (2013). Information manipulation, coordination, and regime change. *Review of Economic Studies*, *80*(4), 1422–1458.

Freelon, D. (2018). Computational research in the post-API age. *Political Communication*, *35*(4), 665–668.

Freyburg, T., & Garbe, L. (2018). Blocking the bottleneck: Internet shutdowns and ownership at election times in sub-Saharan Africa. *International Journal of Communication*, *12*, 3896–3916.

Friedrich, C. J., & Brzezinski, Z. K. (1965). *Totalitarian dictatorship*. Harvard University Press.

Fuchs, C. (2013). Societal and ideological impacts of deep packet inspection Internet surveillance. *Information, Communication & Society*, *16*(8), 1328–1359.

Gerschewski, J. (2013). The three pillars of stability: Legitimation, repression, and co-optation in autocratic regimes. *Democratization*, *20*(1), 13–38.

Gohdes, A. R. (2015). Pulling the plug: Network disruptions and violence in civil conflict. *Journal of Peace Research*, *52*(3), 352–367.

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

Guriev, S., & Treisman, D. (2019). Informational autocrats. *The Journal of Economic Perspectives*, *33*(4), 100–127.

Han, R. (2015). Defending the authoritarian regime online: China's "voluntary fifty-cent army." *The China Quarterly*, *224*, 1006–1025.

Hellmeier, S. (2016). The dictator's digital toolkit: Explaining variation in Internet filtering in authoritarian regimes. *Politics & Policy*, *42*(5), 635–657.

Hobbs, W. R., & Roberts, M. E. (2018). How sudden censorship can increase access to information. *American Political Science Review*, *112*(3), 621–636.

Horowitz, M. C., Perkoski, E., & Potter, P. B. (2018). Tactical diversity in militant violence. *International Organization*, *72*(1), 139–171.

Huang, H. (2018). The pathology of hard propaganda. *The Journal of Politics*, *80*(3), 1034–1038.

Kalathil, S., & Boas, T. C. (2003). *Open networks, closed regimes: The impact of the internet on authoritarian rule*. Carnegie Endowment for International Peace.

King, G., Pan, J., & Roberts, M. E. (2013). How censorship in China allows government criticism but silences collective expression. *American Political Science Review*, *107*(2), 326–343.

King, G., Pan, J., & Roberts, M. E. (2017). How the Chinese government fabricates social media posts for strategic distraction, not engaged argument. *American Political Science Review*, *111*(3), 484–501.

Lorentzen, P. (2014). China's strategic censorship. *American Journal of Political Science*, *58*(2), 402–414.

Lutscher, P. M., Weidmann, N. B., Roberts, M. E., Jonker, M., King, A., & Dainotti, A. (2020). At home and abroad: The use of denial-of-service attacks during elections in nondemocratic regimes. *Journal of Conflict Resolution*, *64*, 373–401.

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

Milner, H. V. (2006). The digital divide: The role of political institutions in technology diffusion. *Comparative Political Studies*, *39*(2), 176–199.

Munger, K., Bonneau, R., Nagler, J., & Tucker, J. A. (2019). Elites tweet to get feet off the streets: Measuring regime social media strategies during protest. *Political Science Research and Methods*, *7*(4), 815–834.

Murdoch, S. J., & Anderson, R. (2008). Tools and technology of Internet filtering. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access denied: The practice and policy of global internet filtering* (pp. 57–72). MIT Press.

Nazario, J. (2009). Politically motivated denial of service attacks. In C. Czosseck & K. Geers (Eds.), *The virtual battlefield: Perspectives on cyber warfare* (*Vol. 3*, pp. 163–181). IOS Press.

Ogola, G. (2019, February 20). Shutting down the Internet doesn't work—but governments keep doing it. *The Conversation*. http://theconversation.com/shutting-down-the-internet-doesnt-work-but-governments-keep-doing-it-111642

O'Neill, P. H. (2018, July). Telegram traffic from around the world took a detour through Iran. *CyberScoop*. https://www.cyberscoop.com/telegram-iran-bgp-hijacking/

Pan, J., & Siegel, A. A. (2020). How Saudi crackdowns fail to silence online dissent. *American Political Science Review*, *114*, 109–125.

Roberts, H., Zuckerman, E., & Palfrey, J. (2012). Interconnected contests: Distributed denial of service attacks and other digital control measures in Asia. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access contested: Security, identity, and resistance in Asian cyberspace* (pp. 133–151). MIT Press.

Roberts, M. E. (2018). *Censored: Distraction and diversion inside China's great firewall*. Princeton University Press.

Rød, E. G., & Weidmann, N. B. (2015). Empowering activists or autocrats? The Internet in authoritarian regimes. *Journal of Peace Research*, *52*(3), 338–351.

Spaiser, V., Chadefaux, T., Donnay, K., Russmann, F., & Helbing, D. (2017). Communication power struggles on social media: A case study of the 2011-12 Russian protests. *Journal of Information Technology and Politics*, *14*(2), 132–153.

Stier, S. (2017). Internet diffusion and regime type: Temporal patterns in technology adoption. *Telecommunications Policy*, *41*(1), 25–34.

Tilly, C. (2010). *Regimes and repertoires*. University of Chicago Press.

Tucker, J. A., Theocharis, Y., Roberts, M. E., & Barberá, P. (2017). From liberation to turmoil: Social media and democracy. *Journal of Democracy*, *28*(4), 46–59.

Villeneuve, N., & Crete-Nishihata, M. (2012). Control and resistance: Attacks on Burmese opposition media. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access contested: Security, identity, and resistance in Asian cyberspace* (pp. 153–176). MIT Press.

Weidmann, N. B., Benitez-Baleato, S., Hunziker, P., Glatz, E., & Dimitropoulos, X. (2016). Digital discrimination: Political bias in Internet service provision across ethnic groups. *Science*, *353*(6304), 1151–1155.

Weidmann, N. B., & Rød, E. G. (2019). *The Internet and political protest in autocracies*. Oxford University Press.

Wintrobe, R. (1998). *The political economy of dictatorship*. Cambridge University Press.

Xu, X. (2020). To repress or to co-opt? Authoritarian control in the age of digital surveillance. *American Journal of Political Science*. Advance online publication. https://doi.org/10.1111/ajps.12514

Zittrain, J., & Palfrey, J. (2008). Internet filtering: The politics and mechanisms of control. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access denied: The practice and policy of global internet filtering* (pp. 103–122). MIT Press.

Author Biographies

Eda Keremoğlu is a postdoctoral researcher at the University of Konstanz. Her research interests include comparative authoritarianism, with a particular focus on the political role of new ICTs, citizen-state relations, and political protest.

Nils B. Weidmann is a professor of Political Science and head of the Communication, Networks and Contention Research Group at the University of Konstanz. His research interests include political protest and violent conflict, with a particular focus on the impact of new communication technology.