International Journal of Communication 12(2018), 3788–3794 1932–8036/20180005

Authoritarian Practices in the Digital Age

Introduction

MARCUS MICHAELSEN[1]
MARLIES GLASIUS
University of Amsterdam, Netherlands

Academic debates on the role of digital technologies in authoritarian and democratic contexts rarely intersect. Research investigating the resilience of authoritarian regimes in the digital age generally runs parallel to inquiries about the "authoritarian qualities" of digital technologies in liberal democracies. Our Special Section breaks new ground by systematically examining authoritarian practices in relation to digital technologies in multilateral, transnational, and public–private settings. This introduction briefly explains the research agenda and aim of the collection, and then outlines its contributions.

Keywords: digital technologies, authoritarianism, democracy, censorship, surveillance, disinformation

The policies developed by authoritarian states in response to the challenges and affordances of the Internet seek to reinforce physical borders, yet they also clearly transcend domestic politics. Authoritarian regimes have adapted to digital communication technologies, erecting barriers of filtering and censorship to control information flows on and into their territories. They use surveillance, cyberattacks, and disinformation to consolidate their power and expand it beyond borders (see, e.g., Deibert, 2015; Hussain & Howard, 2014; King, Pan, & Roberts, 2017; Morozov, 2011). But they also exchange tools and expertise for Internet control and promote ideas on how to govern digital technologies at the international level. Finally, for all these measures, authoritarian states increasingly deal with and rely on private corporations that run the platforms and infrastructure and provide software and technical expertise. In short, digital authoritarian practices take shape in public–private and interstate collaborations and are diffused and legitimized in multilateral settings.

Marcus Michaelsen: m.michaelsen@uva.nl
Marlies Glasius: m.glasius@uva.nl
Date submitted: 2018–07–12

[1] This research was supported by the Authoritarianism in a Global Age project at the University of Amsterdam and received funding from the European Research Council (FP7/2007-2013)/ERC grant agreement number 323899.

Parallel to research on the evolving aptitude of authoritarian states in handling the Internet, there is increasing apprehension about the challenges that digital technologies pose to democratic politics (Bennett & Livingston, 2018; Howard, Woolley, & Calo, 2018; Tufekci, 2014). The revelations of Edward Snowden in 2013 on programs of mass surveillance run by intelligence agencies in leading Western democracies highlighted the fact that opaque and secretive practices are not exclusive to authoritarian regimes (Bauman et al., 2014; Greenwald, 2014; Lyon, 2014). The recent scandal about the abuse of information on more than 80 million Facebook users for political campaigns by a shady consultancy company, Cambridge Analytica, reinforced growing discomfort about the power accumulated by private digital platforms exploiting massive amounts of user data and steering public opinion (Cadwalladr, 2018; Cobbe, 2018; Foer, 2018).

The Russian disinformation campaigns targeting the 2016 U.S. Presidential elections saw these two trends intersecting: one of the most powerful and prominent authoritarian regimes used and abused the affordances of social media and their algorithm-curated news feeds to interfere with the election process of the oldest liberal democracy (Rutenberg, 2017; Shane, 2017). Yet in the academic world, debates on the role of digital technologies in authoritarian and democratic contexts rarely intersect. Research in comparative politics and international relations investigating the resilience of authoritarian regimes in the digital age generally runs parallel to inquiries about the "authoritarian qualities" of digital technologies in disciplines such as media, Internet, and surveillance studies.

This Special Section breaks new ground by transcending (sub)disciplinary boundaries to systematically examine authoritarian practices in multilateral, transnational, and public–private settings. Acknowledging the border-blurring qualities of digital politics, the contributions address the following central questions: *What configurations of political actors give rise to digital authoritarian practices? How are these practices produced and diffused, negotiated, and legitimized?*

The majority of the contributions emerged out of an expert seminar held in September 2016 in the framework of the five-year (2014–2018) multimethod project Authoritarianism in a Global Age, which was funded by the European Research Council and based at the University of Amsterdam (http://www.authoritarianism-global.uva.nl/). The project's point of departure was that openness to global ICT and media, international nongovernmental organizations, and inflow and outflow of people have presented new challenges, but perhaps also new opportunities for authoritarian rulers in terms of how to control citizens. It investigated whether, how, and to what extent the globalization of information and communication, association, and people movement affect authoritarian persistence—that is, how and with what policy mechanisms authoritarian states respond to the globalization of information and communication, association, and people movement, and what authoritarianism means in a global age.

Our conceptual prologue to the collection (Glasius & Michaelsen) introduces the twin concepts of digital illiberal and authoritarian practices. Illiberal practices infringe on the autonomy and dignity of the person, and they are a human rights problem. Authoritarian practices sabotage accountability and thereby threaten democratic processes. We argue that the threats citizens may be exposed to in a digitally networked world can be grouped into three categories: (1) arbitrary surveillance, (2) secrecy and disinformation, and (3) violation of freedom of expression. We use the example of the U.S. National Security Agency's massive data-gathering program to illustrate both what constitutes a practice and the distinctions as well as the

connections between illiberal and authoritarian practices in the digital sphere. The idea of "practices" allows us to go beyond structural regime type classifications to examine what political actors actually do in the digital realm that may be a threat to citizens. As an analytical tool, the concept illuminates how such practices are produced in configurations of authoritarian and democratic as well as state, interstate, and nonstate actors.

Moving on to the empirical studies of the collection, the first three contributions focus on international *diffusion* of technical and political tools for authoritarian Internet control. The literature on authoritarian Internet control, both academic and advocacy-oriented, often overlooks these dynamics because it generally focuses on the policies of single states. Comparative quantitative research—for instance, in the form of global rankings on Internet restrictions—also takes the country as the unit of analysis. By isolating specific types of practices, it is possible to observe how they travel across borders and even across regime types.

Jaclyn Kerr's article investigates mechanisms of collaboration and diffusion in the former Soviet region. She points to the central role played by Russia in the transfer of technical expertise and legislation. Since the early 2000s, Russia's System for Operative Investigative Activities (SORM) has provided both the legal and technical infrastructure for interception of communications and mass surveillance by the Russian security service. Kerr dissects how both the legal and technical aspects of the system have gradually been adopted, in whole or in part, by at least nine other states in the post-Soviet space. What is notable in terms of the commonalities across the region are the legal frameworks, which clearly and explicitly mandate that private service providers and manufacturers install the necessary equipment to make interoperable interception possible. Kerr also points out how Russia's doctrine of "information security," tying online control to questions of national security, has been emulated in the region and has challenged Western ideas about the relationship between state sovereignty and the Internet.

Sarah McKune and Shazeda Ahmed take up the topic of norm contestation and focus on China's promotion of "Internet sovereignty." This is the ideological label, the article explains, that China uses for its preferred mode of Internet governance. As such, it is both an already existing guiding principle of national Internet policy and a model China proselytizes for at the international level. Discursively, at the global level, Internet sovereignty is nowadays posed as an alternative to U.S. dominance as well as to multistakeholder approaches to Internet governance. The model is also presented as a means of combatting the "three evils" of terrorism, separatism, and extremism, constructing these so broadly that any form of dissent can be targeted. The authors discuss how China has used the Shanghai Cooperation Organization and the World Internet Conference, held since 2014 in Wuzhen, to diffuse the concept in principle and in practice. By linking Internet sovereignty to the established (legal) norm of state sovereignty, they argue, the Chinese government seeks to advance its own interpretation of international law and defend its policies of Internet control against rights-based criticism.

In his article on Iran, Marcus Michaelsen investigates a very different manifestation of the diffusion of digital authoritarian practices: "learning from adversaries." He shows how external threats in the form of cyberattacks, Western democracy promotion, and sanctions have created conditions that enabled the Iranian state to practically advance as well as to justify capabilities for censorship and surveillance. The

geopolitical and ideological opposition to the West, particularly the United States, has pushed the regime to perceive the Internet as a strategic battleground for regime stability and to strengthen its hold over critical Internet infrastructure. In the desire to defend national autonomy and security, the Iranian state started establishing a "national information network"—a communication structure more resistant to external interference *and* susceptible to state control. The article demonstrates how the political interests and ideas of competing international political actors get built into Internet architecture.

The next two contributions focus on *public–private relations* and authoritarian practices. Aofei Lv and Ting Luo challenge the received wisdom that sees the Chinese state as an all-powerful Big Brother controlling the Chinese digital sphere. They find that, while it is well-known that the Chinese government engages in targeted surveillance and censorship, the mass surveillance carried out by corporate Chinese Internet giants has received little attention. These companies have almost untrammeled power to influence and cultivate user behavior through surveillance and information manipulation. Focusing on China's three biggest Internet companies—Baidu, Alibaba, and Tencent—the authors describe how the technical resources and economic clout of these companies relates to those of government agencies, which do not have the same access to vast amounts of data on the population, nor the capacity to process and utilize them. Lv and Luo also explain how China's much-debated central social credit system is, in fact, shaped much more by the interests and capacities of the technology giants than by the government's aspirations alone. While the hazards from corporate mass surveillance are universal in principle, they are exacerbated in China's political context: neither the government nor the companies are keen to set up regulations protecting the privacy of users because they both have ambitions to exploit the potential of big data, albeit with different motivations.

Turning to sub-Saharan Africa, Tina Freyburg and Lisa Garbe investigate the relationship between the ownership structure of Internet service providers (ISPs) and Internet shutdowns during contentious events, focusing on 33 presidential and parliamentary elections between 2014 and 2016. They argue that ownership structure helps explain the occurrence of intentional network disruptions, because authoritarian governments do not implement shutdowns themselves; rather, they order Internet providers and telecom operators to cut services. While state ownership of these key intermediaries provides a direct way to control infrastructure and traffic, the involvement of privately owned ISPs complicates the equation. Zooming in on the cases of Uganda and the Republic of the Congo, the authors show that private companies with domestic ownership and possible stakes in the regime as well as companies with roots in emerging economies and other authoritarian countries are more likely to succumb to government pressure and shut down the Internet. Operators from established democracies, by contrast, may risk public condemnation or even legal challenges if they comply with shutdown requests from local power holders, and they are thus more likely to resist.

The last two articles focus on authoritarian and illiberal practices in *formally democratic* settings. Ben Wagner's article, like the previous one, focuses on Internet shutdowns, but it zooms in on a single country, Pakistan, documenting an astounding 41 shutdowns in Pakistan over a five-year period. Wagner argues that, by blocking all content and interrupting all communications, Internet shutdowns have a very different intent and effect than censorship, which only shapes the access to and quality of available information. He conceptualizes Internet shutdowns as "communicative ruptures" to underline how the state,

by controlling communication infrastructure, interferes in the "lifeworld" of citizens, curtailing their capacity to interact and to constitute themselves as full members of society. The article makes a distinction between short-term shutdowns in urban areas and long-term shutdowns in outlying territories. Short-term shutdowns are primarily strategic, aiming to prevent or hinder political mobilization. Long-term shutdowns, such as witnessed in Pakistan's province of Balochistan, can last for weeks or even months and should be considered as having punitive intent, a form of symbolic violence. The purpose is to deny the people of a province seen as "unruly" their dignity as social human beings as well as their political subjecthood as participants in the Pakistani community. Wagner's article also suggests that the persistent use of shutdowns in Pakistan, a formally democratic country, is only possible in a global normative environment that apparently does not consider the practice as exceptionally reprehensible.

The concluding article, by Stefania Milan and Arne Hintz, takes the concept of illiberal and authoritarian practices into the context of liberal Western democracies, discussing the consequences of mass, data-based surveillance. The authors discuss the policy changes that have followed the Snowden revelations: whereas mass surveillance in the early 2000s was typically shrouded in secrecy and its legislative basis questionable, new comprehensive legislation in a raft of states explicitly enables wider data collection and analysis by state agencies. The British Investigatory Powers Act (2016) is a case in point: on the one hand, it made strides in opening up secret surveillance to public oversight; on the other hand, "rather than limiting state surveillance powers in light of the Snowden leaks, it confirmed, legalized, and expanded existing practices" (Milan & Hintz, this Special Section). Complementing their top-down discussion of policy and legal developments, Hintz and Milan discuss public responses to data collection and surveillance, which, they claim, have facilitated the normalization of surveillance and the consolidation of a "surveillance culture."

Taken together, the contributions to this Special Section extend our understanding of the relationship between contemporary forms of authoritarianism and digital communication technologies. Conceptually, the Special Section aims to advance knowledge on what constitutes an authoritarian practice in the field of digital communication technologies and how these practices, in turn, may change the way the technologies are used and developed in an increasingly interconnected world. Combining insights from China, Russia and Central Asia, Iran, Pakistan, sub-Saharan Africa, and Western Europe with expertise in Internet control and surveillance, governance, and legislation, the contributions also give empirical flesh to the idea of authoritarian and illiberal practices as they are diffused between states, coproduced by states and corporate actors, and experienced by citizens.

References

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology*, *8*(2), 121–144. doi:10.1111/ips.12048

Bennett, W. L., & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication*, *33*(2), 122–139. doi:10.1177/0267323118760317

Cadwalladr, C. (2018, March 18). "I made Steve Bannon's psychological warfare tool": Meet the data war whistleblower. *The Guardian*. Retrieved from https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

Cobbe, J. (2018, March 20). The problem isn't just Cambridge Analytica or Facebook—it's "surveillance capitalism." *Open Democracy UK*. Retrieved from https://www.opendemocracy.net/uk/jennifer-cobbe/problem-isn-t-just-cambridge-analytica-or-even-facebook-it-s-surveillance-capitali

Deibert, R. (2015). Cyberspace under siege. *Journal of Democracy*, *26*(3), 64–78. doi:10.1353/jod.2015.0051

Foer, F. (2018, March 21). It's time to regulate the Internet. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2018/03/its-time-to-regulate-the-internet/556097

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. New York, NY: Picador.

Howard, P. N., Woolley, S., & Calo, R. (2018). Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration. *Journal of Information Technology and Politics, 15(2), 81–93*. doi:10.1080/19331681.2018.1448735

Hussain, M. M., & Howard, P. N. (2014). *State power 2.0: Authoritarian entrenchment and political engagement worldwide*. Surrey, UK: Ashgate.

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.

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data and Society*, *1*(2). doi:10.1177/2053951714541861

Morozov, E. (2011). *The net delusion: How not to liberate the world*. London, UK: Allen Lane.

Rutenberg, J. (2017, September 13). RT, Sputnik and Russia's new theory of war. *The New York Times Magazine*. Retrieved from https://www.nytimes.com/2017/09/13/magazine/rt-sputnik-and-russias-new-theory-of-war.html

Shane, S. (2017, September 7). The fake Americans Russia created to influence the election. *The New York Times*. Retrieved from https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html

Tufekci, Z. (2014). Engineering the public: Big data, surveillance and computational politics. *First Monday*, *19*(7). Retrieved from http://firstmonday.org/article/view/4901/4097