Authoritarianism Online: What Can We Learn from Internet Data in Nondemocracies?

Sheena Chestnut Greitens, *Harvard University*

What kind of Internet data is generated in authoritarian political environments? And how can political scientists use that data to better understand the dynamics of nondemocratic regimes?

This article begins from a simple observation: different authoritarian regimes treat the Internet—and all information and communication technologies, or ICTs—differently. Governments vary in the degree to which they limit citizen access to ICTs, the degree to which they use those technologies for surveillance and monitoring, and the degree to which they actively attempt to intervene in and shape online content.

This variation provides two central leverage points for political scientists. First, for political scientists interested in using the data generated by ICTs to make inferences about the political system from which that data comes—as many of the articles in this symposium seek to do—it is important to understand how ICT policy affects the data generation process. Admittedly, the difficulty of collecting data on ICT policies poses significant challenges for research: for example, how does one observe censorship? These policies, however, affect what part of reality is reflected online, and to what degree, and therefore, shape the inferences that we can make using ICT data.

Second, variation in ICT policy itself can be an understudied and useful source of information about authoritarian governments' priorities, intentions, and actions. Censorship not only structures data, it *is* data. And it is data that may be particularly valuable in politically closed regimes, where policy priorities and behavior can be difficult to ascertain using traditional approaches. For both of these reasons, political scientists must take ICT policies seriously, and must explicitly identify and communicate how those policies have shaped their data.

MOVING BEYOND THE CURRENT DIGITAL DEBATE

The role of technology and social media in global politics has gained attention in recent years. Following US Secretary of State Hillary Clinton's January 2010 speech at the Newseum in Washington, DC, "Internet Freedom" has become a pillar of the Obama administration's foreign policy (Clinton 2010). A chorus of voices, ranging from technology companies to think tanks to media pundits, have picked up the theme, calling for America to adopt policies that promote online freedom of expression (Dale and Zuckerman 2011; Fontaine and Rogers 2011; Kalathil 2010; Kelly and Cook 2011; Schmidt and Cohen 2010).

Academic interest has flourished alongside this public discussion. Some scholars are optimistic: they see the Internet as an online public sphere where political communities can be created, debates advanced, and social capital built—in essence, a factor that promotes liberalization, if not democratization (Faris 2008; Rahimi 2011; Yang 2003; Zhang and Zheng 2009). Others have gone further in their enthusiasm, arguing that the Internet and social media have played (or *should* play) a critical causal role in fomenting mobilization and prodemocratic revolution (Bellin 2012; Howard 2010; Howard et al. 2011; Howard and Hussain 2011; Rogin 2012; Sullivan 2009).[1]

These optimistic assertions, however, have been challenged by a growing body of research that calls for skepticism. Kedzie (1997) cautioned that the correlation between connectivity and political freedom does not signify causality, and Norris (2001) suggests that political change determines levels of Internet diffusion rather than the other way around. In the Middle East and North Africa, multiple studies have questioned the supposed connection between ICT penetration and political mobilization (Hassanpour 2011; Meier 2011; Wilson and Dunn 2011; see also Edmond 2012; Kern and Hainmueller 2009). Aday et al. (2012) specifically finds that ICTs did more to inform international audiences than to catalyze collective action within any particular country or society. Mozorov (2011) marshals evidence that ICTs can be used to advantage authoritarian regimes as much as their opponents (for corroboration, see Esfandiari 2010; Freelon 2011; Gladwell 2010; Hounshell 2011). Diamond (2010) suggests that the battle between autocratic regimes and prodemocratic protestors will depend "not just on technology," but on more traditional factors like "political organization and strategy." And Drezner (2010), while arguing that "the 'information revolution' generally favors the empowerment of non-state actors," also notes that "the effect of this empowerment is not consistent across all types of political environments" (see also Mozorov and Howard 2011). Still other scholarship has shifted toward characterizing the online space as one of contestation—a "cat and mouse" game, to quote one analysis (Chung 2011; see also Lynch 2011)—and has sought to move beyond the cyberutopian-versus-cyberskeptic debate by identifying precise mechanisms through which new media and ICTs affect a range of political outcomes (Aday et al. 2010, 2012).

Recent evidence also suggests that ICT freedom also cannot be reduced to an issue of regime type. Just as it is overly simplistic to associate ICTs with social movements and

doi:10.1017/S1049096513000346

censorship with the state, Internet freedom also cannot be reduced to something that exists in free democracies and is lacking in unfree autocracies. Democracies sometimes have decidedly illiberal policies toward information and communication technologies. South Korea, for example, has one of the highest levels of Internet and cell phone use in the world, and online political activities and organization are relatively unfettered. The South Korean government, however, filters or blocks access to "anti-state" (generally pro-North Korean) content, and criminalizes those who support such platforms (Chung 2008). In 2010, the government interrogated 151 people, prosecuted 182, and shut down 178 websites for pro-North content; they also deleted 67,300 individual webposts for that reason from January through October 2011 (Choe 2012; Glionna 2012; "South Korea" 2012). In Asia alone in the last several years, incidents in India, Malaysia, Thailand, and Vietnam (not a comprehensive list) have highlighted the restrictions that a variety of regimes are putting in place (Fuller and Drew 2012; "Internet Freedom in Vietnam" 2012; Palatino 2012; Timmons 2011). Consistent with these observations, the cross-national study by Egorov, Guriev, and Sonin (2009) finds a generally positive correlation between democracy and media freedom, but also observes "substantial variation in the degree of media freedom even controlling for the level of democracy."

increasing surveillance and activism. Although China is famous for its control and censorship, monitoring and state-sponsored online activism are also important components of its strategy. Venezuela's Hugo Chavez—whose Twitter account has nearly 3.6 million followers—has relied on activism more than control (although control is certainly not absent), as have the Bahraini authorities who attempted to flood Facebook, Twitter, and other online forums with proregime content during protests in 2011 (Aday et al. 2012).

Contemporary discussions of authoritarian Internet regulation has tended to focus more on the dimension of control, perhaps because it is easier for scholars and pundits to observe. The dimensions of surveillance and activism, however, are equally important, and including them in the discussion is helpful in a number of ways. Focusing on surveillance, for example, highlights two different kinds of Internet "freedom": freedom to access the Internet and use a cell phone versus the freedom to do so unobserved by the government. Whether one kind of freedom exists versus another may have very different political consequences for citizens, for their ability to mobilize, and eventually for political stability.

Focusing on activism, on the other hand, highlights that regimes can be "competitively authoritarian" when it comes to their ICT policies as well as their electoral politics (Le-

Thus, even within the category of "authoritarian," regimes vary widely in their approach to ICT censorship and regulation, with broadly ranging degrees of control and contestation.

Thus, even within the category of "authoritarian," regimes vary widely in their approach to ICT censorship and regulation, with broadly ranging degrees of control and contestation. So far, however, most studies of the Internet's role in political life have focused on exploring microempirical data from a single country. As a result, systematic cross-national comparison of ICT policy has been limited (for exceptions, see Deibert et al. 2008; 2010).

This article is a first cut at conceptualizing the variation that we see. State approaches to ICT vary across three primary dimensions. The first, and most discussed, is *control*: the degree to which a government seeks to limit or curtail citizen access to information and communication technologies, usually through means such as censorship and filtering. The second is *surveillance*: the degree to which a particular regime uses ICT activity and data in its effort to monitor the population. The third is *activism*: the degree to which a regime seeks to actively shape online or social media content in ways that are favorable to the regime. In all three realms, governments can emphasize either technological or regulatory tools: they can either create policies that shape citizen behavior or acquire hardware or software that simply make certain activities impossible.

In practice, authoritarian regimes use a mix of strategies. Until recently, North Korea relied almost exclusively on control, but more recently seems to be decreasing control and

vitsky and Way 2010). Some variation in the ICT landscape is market driven rather than political in its origins—a matter of which companies deliver the best products to market. But some variation *is* overtly political. It exists because, just as authoritarian regimes have a say in whether opposition parties are allowed to compete at the polls, they have a strong interest, voice, and capability when it comes to shaping the "online opportunity structures" within which dissidents can criticize, organize, and mobilize others. If technology has had a more limited effect on empowerment in some places, it may be because the authorities in those regimes want it that way. By focusing more on social movements' use of technology than on government regulation of this space (or on government-protestor interaction in the digital sphere), the extant literature has largely overlooked this crucial point. Even when the Internet is relatively free, regimes do not have to create a level playing field for those using it in politics.

This point is important for two communities of scholars: those who are interested *theoretically* in what role information and communication technologies play in authoritarian political systems and those who are interested *methodologically* in how to use Internet data to understand these countries' political dynamics.

For scholars who are interested in ICTs as a source of data and *methodological* innovation, the challenge is to learn enough

about the policies and political context to explicitly identify how they have affected the generation of online data. Overlooking this question risks conceptual confusion, biased statistical estimates, and flawed conclusions. If citizens in a certain country use text messages rather than Facebook, for example, but researchers use Facebook because that is what they can see and collect, they risk mischaracterizing the relationship between ICT presence and political organization (see, for example, Howard et al. 2011). Focusing on jihadis who can be found online might lead researchers to exaggerate their importance relative to groups that do not have a significant online presence (Aday et al. 2012), or to mis-estimate the on-the-ground degree of organization by assuming it mirrors online activity. Understanding how ICT data is produced, therefore, is necessary for researchers to be clear about what part of political reality their data represents, and which inferences they can safely draw from the data. And on the positive side, in addition to guarding against methodological pitfalls, recognizing this fact opens up creative ways for scholars to use new data to gain analytical leverage and insight into these countries' politics.

Table 1

Basic Questions about Information and Communication Technology

CHARACTERISTIC	RELATED QUESTIONS
User Community	Who uses the Internet (and other ICTs)? How big is each user population compared to the overall population? How representative is the user population? (demographically, socially, economically, geographically, etc.)
Service Provision	What do people use ICTs for? Where do they go to use these services? Who generates ICT content, and who consumes it?
Market	What are the dominant platforms? How fragmented is market share? Are the major providers domestic or foreign? What is the level of state involvement with these providers?
Control, Surveillance, & Activism	What kind of registration is required for ICT use? How is use monitored? Who monitors and censors ICT content? At what level are censorship decisions made? Under what circumstances is information censored? (when, where, what, why) Does the state sponsor any other intervention or proregime activism online?

For scholars who are interested in generating and testing *theoretical* claims about the role of ICTs in authoritarian political systems, it is equally critical to understand a country's ICT policies and digital landscape. Understanding the structure and potential biases of the data is the only way for scholars to make precise and accurate causal claims. Contextual information also enables scholars who engage in micro-empirical work on the role of ICTs in one or a handful of cases—currently the majority of the work being done on this topic—to specify the scope conditions and generalizability of their argument. Finally, starting with an analysis of ICT policy allows scholars to think about outcomes of interest beyond mobilization and democratization.

One possible way to start is with a series of simple questions, grouped into the categories shown in table 1.

In sum, data generated by information and communication technologies in authoritarian countries are shaped by the policies that the regimes adopt toward those technologies. For that reason, research that uses ICT data, or examines the role of ICTs in politics, must consider political context. Doing so is both a useful exercise to shed light on the objectives and operations of the political systems from which the data comes, and a necessary component of methodologically sound research.

The following sections demonstrate this argument by analyzing ICT policy and context in two authoritarian regimes in East Asia: China and North Korea. Both countries are widely known for their Internet censorship, but in fact, their approaches to ICT have differed significantly. The case of China illustrates how authoritarian ICT policies structure data and inform research methodology, whereas the North Korea case demonstrates the value of treating authoritarian ICT policies as an independent object of inquiry.

CHINA: WHY ICT CONTEXT MATTERS FOR SCHOLARSHIP

Discussions in the field of Chinese politics on the importance of ICT growth have mirrored the larger debate in political science. During the past decade, literature on the development of the Internet in China and whether it is enabling a digital civil society has blossomed (Herold and Marolt 2011; MacKinnon 2011; Yang 2003; Yang 2009; Zhang and Zheng 2009; Zheng 2008; Zhou 2006). These studies have noted that the Chinese government has an interest in relatively unfettered Internet use to promote economic development, as well as in allowing online dissent as a "safety valve" to vent grievances. A relatively open Internet also assists the party and state officials in understanding public opinion, monitoring local officials, and improving governance (Qiang 2011; Zheng and Fewsmith 2008).

At the same time, however, China's Internet censorship policies are widely known and much criticized. Several studies highlight how these attempts at information control have helped to strengthen the regime, but resulted in poor governance (see Wu 2009 and Zheng 2009; Harwit and Clark 2001; Kalathil and Boas 2003). According to one recent study, the scale of Chinese censorship efforts is "unprecedented in world history" (King, Pan, and Roberts 2012). The most common metaphor in popular writing is that of "The Great Firewall."[2] Used to describe China's blocking of objectionable websites and search results, the metaphor suggests a monolithic, massive, and heavy-handed effort at stamping out all online

dissent and criticism of the regime. It emphasizes control as the single defining factor of Chinese ICT policy.

In fact, examining China's approach to information and communication technology using the framework proposed above shows that China has relied not just on control, but also on surveillance and activism to shape the ICT landscape. (Thus far, accounts of activism in China's ICT policy have primarily focused on whether the Chinese government sponsors cyberspace activities detrimental to foreign actors and interests (see, for example, Barnes, Gorman, and Page 2013; Sanger, Barboza, and Perlroth 2013).) In fact, China's domestic ICT efforts are more decentralized, agile, and proactive than commonly portrayed, and they actively seek to involve the population in favorably shaping online content—context that should be taken into account as scholars generate questions for research and develop data collection strategies.

China's ICT landscape is more complex and decentralized than popular depictions often credit. Its service providers and social media platforms are largely non-Western, and market share is relatively fragmented. Facebook and Twitter are prohibited, but even in realms where Western competitors are present, Chinese platforms dominate; search competition, for example, is mostly between the Chinese search engine Baidu and its newer, also-Chinese rival Qihoo, rather than Google, whose market share (~15% at time of writing) has declined since the company moved to Hong Kong in early 2010 (Mozur 2012). Services such as microblogging are distributed across hundreds of locally provided sites and are also much more fragmented than the common analogy of Weibo as "China's Twitter" suggests.

Censorship in China is similarly decentralized, operationalized at multiple levels of government, and conducted in "public-private partnership" with actors in the technology industry. At the highest level, the National Leadership Group on Informatization oversees information policy, which includes industry development, regulation, and political control; regulation is implemented by the Ministry of Information Industry. Primary responsibility for censorship at the central level appears to rest with the Web Bureaus of the Chinese Communist Party's Central Propaganda Department and State Council Information Office, which have subordinate offices at the provincial, municipal, and county levels. A range of other institutions, from the Ministries of Public and State Security to the General Bureau for Postal and Telecommunications and the Ministries of Education and Culture, also collaborate in policing media and online content (Chen and Ang 2011; Qiang 2011; Wu 2009; Zheng 2008). Although the accuracy of these estimates is difficult to gauge, each province reportedly has 40–60 Internet police, each prefecture 30–40, and each county 3–4: a national total of between 20,000 and 50,000. Individual companies and websites are also required to engage in self-monitoring and censorship; everyone from a company whose website is available in China to the owner of a local Internet café (*wangba*) can be penalized for inappropriate content (MacKinnon 2012; Zheng 2008). An additional 250,000–300,000 paid "50-cent party members" (*wumao dang*) mix control and activism online: they assist in monitoring content, making favorable comments, and generally pushing discussion toward pro-Party lines (Chen and Ang 2011; King, Pan, and Roberts 2012).

These actors can deal with objectionable content in several ways. Sites can be blocked altogether. Searches for certain terms can also be blocked, or search results filtered so that certain websites do not appear. These techniques of control, however, are bolstered by others, many of which are human rather than automated, that rely on surveillance and activism to monitor and proactively shape online content. For example, posts that contain particular keywords can be filtered to prevent them from appearing on websites or social media platforms, but censors also review content as it is posted to remove problematic posts (Bamman, O'Connor, and Smith 2012; MacKinnon 2009). Although website blocking and search filtering are generally what people have in mind when they refer to "The Great Firewall," the post-by-post surveillance and activism dimensions of China's policy also play a significant role in how censorship is conducted and how its efforts are perceived by citizens.

The most common metaphor in popular writing is that of "The Great Firewall."[2] Used to describe China's blocking of objectionable websites and search results, the metaphor suggests a monolithic, massive, and heavy-handed effort at stamping out all online dissent and criticism of the regime.

This complexity presents serious methodological issues for researchers seeking to use Chinese ICT data. Most obviously, market fragmentation creates practical hurdles for data collection. A researcher using Google search results, for example, could capture 98% of market share with that source in Egypt, but would be observing a much more limited segment of the population in China. The fact that that portion of the population might well be unrepresentative in some way, also, could bias inferences drawn from that data. Decentralization creates additional analytical challenges because researchers cannot assume that either access to technology or the process of censorship is nationally standardized. These issues make the direction or magnitude of any bias introduced by the choice of sources and the data collection procedures much more difficult to assess.

Two recent studies make an effort to move beyond blocking and filtering by collecting microblog and social media postings to examine understudied aspects of China's censorship

process. First, Bamman, O'Connor, and Smith (2012) examines both search blocking and message deletion rates on Sina Weibo. They show a clear pattern of temporal spikes in censorship related to politically sensitive news events or rumors, and discover that politically sensitive terms can be identified by comparing Weibo to uncensored Chinese-language Twitter content. Their study also finds evidence of sub-national variation in censorship; message deletion rates are higher for posts originating in Tibet, Qinghai, and Ningxia, indicating that posts from these politically sensitive areas may be more strictly monitored. Second, King, Pan, and Roberts (2012) uses blog post deletion rates for 1,400 (non-Weibo) content providers to test two possible motivations for Chinese censorship, each of which predicts a different pattern in message deletion. Their results suggest that China's censorship is focused on forestalling collective action rather than suppressing criticism of the government or party. The study also finds that temporal spikes in censorship are predictive of government activity, typically preceding official action by several days.

By adopting data collection procedures that consider the political context of Chinese ICTs, these studies generate new findings that are both methodologically innovative and theoretically relevant. The methods they develop, such as comparing social media platforms to identify politically sensitive issues, or using message deletion patterns to predict government action, are likely to be useful for other researchers. And they depict characteristics of Chinese behavior—active concern with shaping public opinion, openness to mass participation in pro-regime or nationalist political campaigns, and internal variation across provinces and localities—that have been noted elsewhere with respect to China (Heilmann and Perry 2011; Perry and Goldman 2007; Shen and Breslin 2010), but that have not yet been incorporated into broader discussions about authoritarian government approaches to information and communication technology.

In an ideal research environment, scholars would complement these data with fieldwork—including obtaining archival documents and conducting interviews or field observations—that would help to fill in some of the processes at work and that would mirror the growing body of work on citizens' use of online space. In an authoritarian regime, however, where on-the-ground research on this behavior may not be possible, the use of Internet data provides a window into questions that would otherwise be difficult to address. Political context, properly recognized, is therefore both a constraint and an enabler of effective research on sensitive topics. Understanding context helps scholars generate creative methodologies and innovative theoretical claims that not only illuminate a particular country's political dynamics, but also speak to broader debates within the discipline.

Political context, properly recognized, is therefore both a constraint and an enabler of effective research on sensitive topics. Understanding context helps scholars generate creative methodologies and innovative theoretical claims that not only illuminate a particular country's political dynamics, but also speak to broader debates within the discipline.

NORTH KOREA: THE VALUE OF STUDYING ICT POLICIES

It may seem paradoxical to focus on the role of information and communication technology in a country infamous for banning the Internet. North Korea, however, represents a hard case for the idea that ICT-generated data can be useful to political scientists. If we can learn from looking at the Internet in a country where the Internet barely exists, we have a good chance of learning even more elsewhere. In fact, examining North Korea's ICT policies—and the recent evolution in those policies—provides valuable clues about the regime's priorities and policies.

Until recently, North Korea's ICT landscape has been distinguished by technical rather than regulatory solutions. Rather than blocking and censoring online *content*, as China does, North Korea simply banned the physical *infrastructure* like cell phones and computers that could provide access to information outside regime control. Possession of foreign media is a crime, and radios are hardwired to receive only official channels. Computers are rare; concentrated in official hands, they run a special North Korea-designed custom operating system called Red Star and display "Respected Leader" Kim Jong Un's name in slightly larger font size (Lee 2012). An estimated 50,000 privileged citizens have access to a domestic Intranet controlled by the Korean Computer Center ("How Widespread" 2012). Called Kwangmyong, it came online in 2000 and offers a search engine, technical texts, a message/chat function, and official news to the select group who can access approved content (Chen, Ko, and Lee 2010; "Weird But Wired" 2007). Internet access is reserved for a handful of trusted elites, estimated by one expert to be no more than a few dozen families (Bruce 2012a, 2012b).

In the past decade, however, ICT presence inside North Korea has slowly increased. Mobile phones were illegal prior to 2002, and outlawed again from 2004 to 2008. Beginning in 2008, however, the level of cell phone penetration began to rise; North Korean company Koryolink, in which the regime holds an official 25% interest, signed a joint venture contract with Egyptian telecommunications company Orascom to provide mobile phone service. Coverage is good, even outside of Pyongyang, and by February 2012, Koryolink had signed up its millionth subscriber, with reports in early 2013 that the number had reached 1.8 million (Farrell 2012; "Foreigners Visiting" 2013; Martin 2012; Williams 2011). Until January 2013,

foreigners' mobile phones were confiscated at the airport or border, but at the time of writing were allowed in ("Exclusive" 2013).

Internet penetration has followed more slowly. Since spring 2011, students at Pyongyang University of Science and Technology, Pyongyang's only private university, have had Internet access—albeit a single IP address shared among 370 students (out of a total of 1,024 for the country; Kim Young-jin 2012; "One IP Address" 2012; Park 2012). In 2013, the Associated Press reported that foreigners would be allowed to use the Internet on devices they brought with them, and reports have also surfaced recently about a North Korean tablet (Allnut 2011; "News Summary" 2013; Ramstad 2012). Finally, in a speech discussing land management in April 2012, new leader Kim Jong Un called for party cadres to use the Internet (Kim 2012).

Despite this progress, control remains extraordinarily strict, even in comparison to other authoritarian regimes. Cell phone possession requires approval from one of the security agencies. Phones also have technical restrictions, reportedly including disabled camera and Bluetooth features, restrictions on making calls from outside the city where the phone is registered, and no ability to call "internationally"—even to foreign diplomats or nongovernmental organization workers resident in the country or to the Chinese phones in widespread, if illicit, use along the border (Kim Tae Hong 2012; Park and Lee 2011; Williams 2012). Both North Korean and Chinese-imported phones are also rumored to feature monitoring capabilities designed to provide informational advantages to a regime that has long sought to penetrate and surveil every aspect of society (Collins 2012; Gause 2012).

North Korea's recent embrace of ICTs seems somewhat puzzling. Given the regime's opposition to ICT presence in the past, it is surprising that the regime would allow the introduction of cell phones just as these were reportedly facilitating antiregime mobilization in the Arab Spring. Is this, as some have speculated, a sign of generally reformist inclinations on the part of the new "Respected Leader" Kim Jong Un (Fish and Cathcart 2012; Lee 2012)?

Closer examination of North Korea's ICT policies suggests a less optimistic interpretation. The introduction of cell phones and tablet computers certainly marks a change in the availability of technology in North Korea. But the evidence suggests that North Korea's leaders may have calculated that switching strategies—from an approach that emphasizes total control to one more reliant on surveillance and activism—will have greater political benefits for regime survival. It allows them to maximize foreign investment and confiscate hard currency from the population, to replace illicit sources of information with those managed and monitored by the regime, and to use technology to disseminate proregime propaganda.

The first benefit of this strategy switch is economic. North Korea is a country so dependent on hard currency that it is willing to resort to criminal activity to obtain it (Chestnut 2007; Haggard and Noland 2008; Kim 2011). Allowing foreigners to bring in phones and use the internet provides Koryolink with an additional customer base and income stream; one recent report suggests that a Koryolink SIM card costs 50 euros ("Foreigners Visiting North Korea" 2013). The lack of phone and Internet services has also been one of the principal complaints of Chinese investors (Haggard, Lee, and Noland 2012). North Korea may have decided that providing these services to foreign businesspeople is essential to attract foreign investment and hard currency.

In addition to attracting hard currency from outside the country, phones may also be a way for the regime to extract cash from society. When this article was written, the price of phones reportedly started at $250; registration required additional fees; and subscribers had to prepay monthly fees averaging $13.90 a month, in a country whose per capita GDP is less than $2000/year (Park and Lee 2011; "Untitled" 2012). Individuals who can pay with foreign currency reportedly get more than three times the minutes that they would by paying the equivalent amount in North Korean won (Park and Lee 2011). One report on the North Korean Samjiyon tablet suggests that maker Chosun Computer also accepts American cash in payment (Ramstad 2012). Extrapolating from Koryolink's estimated 80% gross margin ($33.1 million in one quarter of 2011 alone; "Mobile Phones" 2012), a 25% interest in the company could earn the regime more than $60 million a year even before the charges to visiting foreigners are considered. Mobile phones, therefore, may serve the dual purpose of attracting foreign investment and helping siphon cash earned through less official cross-border channels into state or party coffers.

Second, evidence also suggests that North Korea's creation of official ICT infrastructure may be motivated by the desire to preempt citizen use of unauthorized networks, which have of late played an increasing role in bringing outside information to ordinary North Koreans (Kretchum and Kim 2012). The recent expansion of state-sponsored ICT networks has occurred in parallel with campaigns to clamp down on foreign media and information (Sullivan 2012), suggesting that the regime is attempting to substitute one for the other. Former North Korean computer scientist Kim Heong-Kwang has called North Korea's approach a "mosquito net": it lets foreign investment in, but

Former North Korean computer scientist Kim Heong-Kwang has called North Korea's approach a "mosquito net": it lets foreign investment in, but keeps foreign culture and political ideas out (Bruce 2012a). It also allows the regime to earn money while acquiring a channel to monitor those who are making it for them, and reaps the gains from increased domestic efficiency without sacrificing social stability.

keeps foreign culture and political ideas out (Bruce 2012a). It also allows the regime to earn money while acquiring a channel to monitor those who are making it for them, and reaps the gains from increased domestic efficiency without sacrificing social stability. In short, substituting officially provided ICTs for those obtained on the black market would have surveillance advantages for the North Korean regime.

Third, the advent of cell phones provides an opportunity for digital activism on the part of the regime in ways that could strengthen rather than weaken its ideological and informational hold. North Korea's cell phone owners now receive daily propaganda via text message ("Mobile Phones" 2012). And given that the domestic Intranet shares information among party cadres in a fashion similar to the newsletters circulated (and not available to the wider public) in North Korea's pre-Intranet era, Kim Jong Un's call for its use may simply be a call for making the old propaganda and information system more efficient, not replacing it with something else.[3]

The political impact of technology in North Korea will depend not just on its presence, but how it is used and who sees the information it provides. It is, as yet, unclear that the presence of ICTs in North Korea will alter the current dynamics. In fact, several factors suggest that the introduction of state-sponsored ICTs may, at least in the short term, strengthen the regime's hand.

Two factors are especially pertinent here. First, the overall level of ICT penetration remains low. One million subscribers is less than 5% of North Korea's approximately 23 million citizens; even 1.8 million is still in the single digits.[4] Second, the demographic profile of these users is unclear, and it is likely to be important in predicting how they will use ICT access.

Users of Chinese cell phones, for example, are likely to have a different profile than users of the official North Korean network. Official users are reported to be largely urban and educated, many of them in Pyongyang. They are also people who have enough hard currency to pay the monthly usage fees. Residential status in Pyongyang and a professional position where one might earn hard currency are both privileges typically granted to North Koreans with good family/class background (*songbun*)—in other words, to trusted members of the elite (Collins 2012). Indeed, in North Korea the size of the official Koryolink subscriber network may indicate of the size of the selectorate—the pool of people from whom Kim Jong Un gets the coalition that he needs to remain in power. This claim is necessarily speculative, but if true, it would be a useful empirical referent for a concept that is theoretically central to regime stability, but politically sensitive and, in practice, difficult to observe.[5] By contrast, use of Chinese cell phones rather than North Korean ones is most likely among the part of the population that has been willing to step outside the approved boundaries to engage in market activity and trading, and who have succeeded in the realm of private economic activity that has weakened the correlation between political privilege and economic status over the course of the past two decades.

In both cases, mobile phones are an indicator of an individual's place in the socioeconomic structure, whether that status is granted by traditional privilege or clout in the new unofficial economy ("Cellphones" 2012). The political effects of official ICT introduction, however, should be expected to be very different for these two groups. Cracking down on black market traders who use Chinese cell phones and forcing them to switch to official networks for which they have to pay in hard currency provides the regime with twin benefits: it siphons away these individuals' economic power, while simultaneously removing their ability to get information and communication from outside official channels. Offering cell phones to the selectorate, by contrast, or even to a wider group of relative "loyalists," rewards with ICT access those people who are least likely to use it for antiregime mobilization. It trades the low risk of empowering them for the benefit of earning hard currency to continue their patronage.

In sum, a close examination of North Korea's ICT policies suggests that the risks incurred by increased ICT penetration may be more than offset by political benefits accrued to the regime, and that controlled expansion may work in favor of the North Korean regime rather than to its detriment. The case also demonstrates that even in countries where Internet penetration is too low to generate large-scale data for analysis, important insights can be drawn from the political, economic, and social context within which information and communication technologies are used.

CONCLUSION

Authoritarian political systems are not all alike, and this includes their attitude toward the Internet. As the previous pages have argued, variations in control, surveillance, and activism on the part of different regimes shapes ICT-generated data in different ways in different places. As political scientists take advantage of the growing volume of ICT data, researchers should be aware that these data require careful interpretation based on how they are shaped by social and political context. The Chinese and North Korean case studies also indicate that, when examined carefully, authoritarian ICT policies—and particularly, how these policies balance control, surveillance, and activism—can provide political scientists with unexpected leverage on some of the most difficult and pertinent questions about authoritarian political systems, including the reasons why some of them might last longer than the teleology of Internet freedom would otherwise indicate. Initial scholarly attention was drawn to ICTs because of their purported prodemocratic effects on authoritarian political systems. What is likely to sustain that attention, however, is not only that their effects appear to be far more varied than initially proposed, but also that they generate data that can help us understand a range of political outcomes of interest—whether those outcomes are prodemocratic or not.

ACKNOWLEDGMENTS

Thanks to Gabriel Koehler-Derrick, Steven Levitsky, Jonathan Mellon, Rich Nielsen, Jennifer Pan, and Molly Roberts. ■

NOTES

1. In these arguments, the boundary between empirical and normative is seldom clearly delineated.
2. The first use of this term appears to have been Barmé and Ye 1997.

3. Thanks to Chris Green for pointing out this similarity to me.

4. This statistic omits the unknown number of phones used along the Chinese border, which typically do not work farther south.

5. Current work on the selectorate and winning coalitions uses expert surveys, which means that one pilot study relied on four expert opinions to estimate its size in North Korea (Bueno de Mesquita and Smith 2007).

REFERENCES

Aday, Sean, Henry Farrell, Marc Lynch, John Sides, and Deen Freelon. 2012. *Blogs and Bullets II: New Media and Conflict after the Arab Spring*. Washington, DC: United States Institute of Peace.

Aday, Sean, Henry Farrell, Marc Lynch, John Sides, John Kelly, and Ethan Zuckerman. 2010. *Blogs and Bullets: New Media in Contentious Politics*. Washington, DC: United States Institute of Peace.

Allnut, Luke. 2011. "Forget the Nexus 7, Meet the Samjiyon, North Korea's Tablet." *Radio Free Europe*, June 28.

Bamman, David, Brendan O'Connor, and Noah A. Smith. 2012. "Censorship and Deletion Practices in Chinese Social Media." *FirstMonday* 17 (3). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/3943/3169.

Barmé, Geremie, and Sang Ye. 1997. "The Great Firewall of China." *Wired*, June. http://www.wired.com/wired/archive/5.06/china.html.

Barnes, Julian E., Siobhan Gorman, and Jeremy Page. 2013. "U.S., China Ties Tested in Cyberspace." *Wall Street Journal*, February 19.

Bellin, Eva. 2012. "Reconsidering the Robustness of Authoritarianism in the Middle East: Lessons from the Arab Spring." *Comparative Politics* 44 (2): 127–49.

Bruce, Scott. 2012a. "The Information Age: N. Korean Style." *The Diplomat*, November 11.

Bruce, Scott Thomas. 2012b. "A Double-Edged Sword: Information Technology in North Korea." *Analysis from the East-West Center* 105 (October).

Bueno de Mesquita, Bruce, and Alastair Smith. 2007. "Dimensions of Governance: A Selectorate Pilot Study." http://alexanderhamilton.as.nyu.edu/page/pilotstudy

"Cellphones No Signal of Reforms." 2012. *Radio Free Asia*, January 19.

Chen, Cheng, Kyungmin Ko, and Ji-Yong Lee. 2010. "North Korea's Internet Strategy and its Political Implications." *The Pacific Review* 23 (5): 649–70.

Chen, Xiaoyan, and Peng Hwa Ang. 2011. "Internet Police in China: Regulation, Scope and Myths." In *Online Society in China: Creating, Celebrating, and Instrumentalising the Online Carnival*. ed. D. Herold and P. Marolt. New York: Routledge.

Chestnut, Sheena. 2007. "Illicit Activity and Proliferation." *International Security* 32 (1): 80–111.

Choe, Sang-hun. 2012. "South Korean Law Casts Wide Net, Snaring Satirists in the Hunt for Spies." *New York Times*, January 7.

Chung, Jongpil. 2008. "Comparing Online Activities in China and South Korea: The Internet and the Political Regime." *Asian Survey* 48 (5): 727–51.

———. 2011. "Weibo and 'Iron Curtain 2.0' in China: Who Is Winning the Cat-and-Mouse Game?" *EAI Issue Briefing* No. MASI 2011-07. December.

Clinton, Hillary Rodham. 2010. "Remarks on Internet Freedom." Newseum, Washington, DC. January 21. http://www.state.gov/secretary/rm/2010/01/135519.html.

Collins, Robert. 2012. *Marked for Life: Songbun, North Korea's Social Classification System*. Committee on Human Rights in North Korea.

Dale, Helle C., and Jessica Zuckerman. 2011. "U.S. Must Improve Internet Freedom Outreach Effort." Washington, DC: Heritage Foundation, January 28.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. 2010. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT Press.

Deibert, Ronald, John Palfrey, Rafal Rohozinsky, and Jonathan Zittrain. 2008. *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge, MA: MIT Press.

Diamond, Larry. 2010. "Liberation Technology." *Journal of Democracy* 21 (3): 69–83.

Drezner, Daniel W. 2010. "Weighing the Scales: The Internet's Effect on State-Society Relations." *Brown Journal of International Affairs* 16 (2): 31–44.

Edmond, Chris. 2012. "Information Manipulation, Coordination, and Regime Change." Unpublished manuscript, July. http://www.chrisedmond.net/Edmond%20Information%20Manipulation%202012.pdf.

Egorov, Georgy, Sergei Guriev, and Konstantin Sonin. 2009. "Why Resource-poor Dictators Allow Freer Media: A Theory and Evidence from Panel Data." *American Political Science Review* 103 (4): 645–68.

Esfandiari, Golnaz. 2010. "Misreading Tehran: The Twitter Devolution." *Foreign Policy*, June 7.

"Exclusive: Foreigners Now Permitted to Carry Mobile Phones in North Korea." 2013. *NK News*, January 19.

Faris, David. 2008. "Revolutions Without Revolutionaries? Network Theory, Facebook, and the Egyptian Blogosphere." *Arab Media and Society* 6.

Farrell, Tad. 2012. "Cell Phones in North Korea: Understanding the Boom," *NKNews*, 16 November.

Fish, Isaac Stone, and Adam Cathcart. 2012. "The Slick PR Stylings of Kim Jong Un." *Foreign Policy*, July 11.

Fontaine, Richard, and Will Rogers. 2011. *Internet Freedom: A Foreign Policy Imperative in a Digital Age*. Center for a New American Security. Washington, DC: Center for a New American Security.

"Foreigners Visiting North Korea to Be Allowed to Bring Cellphones." 2013. *Xinhua/Global Times*, January 21.

Freelon, Dan. 2011. "The MENA Protests on Twitter: Some Empirical Data." http://dfreelon.org/2011/05/19/the-mena-protests-on-twitter-some-empirical-data/.

Fuller, Thomas, and Kevin Drew. 2012. "Thai Message Board Manager is Given Suspended Prison Sentence." *New York Times*, May 30.

Gause, Ken. 2012. *Coercion, Control, Surveillance, and Punishment: An Examination of the North Korean Police State*. Washington: Committee on Human Rights in North Korea.

Gladwell, Malcolm. 2010. "Small Change: Why the Revolution Won't be Tweeted." *New Yorker*, October 4. http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell.

Glionna, John M. 2012. "South Korea Security Law is Used to Silence Dissent, Critics Say." *Los Angeles Times*, February 5.

Haggard, Stephan, Jennifer Lee, and Marcus Noland. 2012. "Integration in the Absence of Institutions: China-North Korea Cross-Border Exchange." *Journal of Asian Economies* 23 (2): 130–45.

Haggard, Stephan, and Marcus Noland. 2008. "North Korea's Foreign Economic Relations." *International Relations of the Asia-Pacific* 8: 219–46.

Harwit, Eric, and Duncan Clark. 2001. "Shaping the Internet in China: Evolution of Political Control over Network Infrastructure and Content." *Asian Survey* 41 (3).

Hassanpour, Navid. 2011. "Media Disruption Exacerbates Revolutionary Unrest: Evidence from Mubarak's Natural Experiment." Paper prepared for the American Political Science Association Annual Meeting, Seattle, WA.

Heilmann, Sebastian, and Elizabeth J. Perry. 2011. *Mao's Invisible Hand: The Political Foundations of Adaptive Governance in China*. Cambridge, MA: Harvard University Press.

Herold, David Kurt, and Peter Marolt. 2011. *Online Society in China: Creating, Celebrating, and Instrumentalising the Online Carnival*. New York: Routledge.

Hounshell, Blake. 2011. "The Revolution Will Be Tweeted." *Foreign Policy*, July/August.

"How Widespread is Mobile Phone Use in North Korea?" 2012. *Chosun Ilbo*, April 23.

Howard, Phillip. 2010. *The Digital Origins of Dictatorship and Democracy*. Oxford: Oxford University Press.

Howard, Philip N., and Muzammil M. Hussain. 2011. "The Upheavals in Egypt and Tunisia: The Role of Digital Media." *Journal of Democracy* 22 (3): 35–48.

Howard, Philip N., Aiden Duffy, Deen Freelon, Muzammil Hussain, Will Mari, and Marwa Mazaid. 2011. "Opening Closed Regimes: What Was the Role of Social Media during the Arab Spring?" Seattle, WA: Project on Information Technology and Political Islam.

"Internet Freedom in Vietnam: An Odd Online Relationship." 2012. *The Economist*, August 9.

Kalathil, Shanthi. 2010. *Internet Freedom: A Background Paper*. Aspen Institute International Digital Economy Accords Project. http://www.aspeninstitute.org/policy-work/communications-society/programs-topic/global-projects/idea/blog/internet-freedom-backgro.

Kalathil, Shanthi, and Taylor C. Boas. 2003. *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*. Washington, DC: Carnegie Endowment for International Peace.

Kedzie, Christopher. 1997. *Communication and Democracy: Coincident Revolution and the Emergent Dictator's Dilemma*. Santa Monica, CA: RAND.

Kelly, Sanja, and Sarah Cook. 2011. *Freedom on the Net 2011: A Global Assessment of Internet and Digital Media*. New York: Freedom House. www.freedomhouse.org/sites/default/files/FOTN2011.pdf.

Kern, Holger Lutz, and Jens Hainmueller. 2009. "Opium for the Masses: How Foreign Media Can Stabilize Authoritarian Regimes." *Political Analysis* 17: 377–99.

Kim, Jong Un. 2012. "Speech on Land Management." April.

Kim, Kwang-Jin. 2011. "The Defector's Tale: Inside North Korea's Secret Economy." *World Affairs Journal* 174 (3): 35–46.

Kim, Tae Hong. 2012. "No State Secrets on Koryolink!." *DailyNK*, February 12.

Kim, Young-jin. 2012. "North Korean Students Get Rare Access to the Internet." *Korea Times*, March 11.

King, Gary, Jennifer Pan, and Molly Roberts. 2012. "How Censorship in China Allows Government Criticism but Silences Collective Expression." Paper prepared for the American Political Science Association Annual Meeting. New Orleans, LA: August.

Kretchum, Nat, and Jane Kim. 2012. *A Quiet Opening: North Koreans in a Changing Media Environment*. Washington, DC: Intermedia.

Lee, Dave. 2012. "North Korea: On the Net in the World's Most Secretive Nation," *BBC News*, December 16.

Lee, Jean H. 2012. "Kim Blazes a Brand New Trail with His Rule." *Associated Press*, July 18.

Levitsky, Steven, and Lucan Way. 2010. *Competitive Authoritarianism: Hybrid Regimes After the Cold War*. Cambridge, MA: Cambridge University Press.

Lynch, Marc. 2011. "After Egypt: The Limits and Promise of Online Challenges to the Authoritarian Arab State." *Perspectives on Politics* 9 (2): 301–10.

MacKinnon, Rebecca. 2009. "China's Censorship 2.0: How Companies Censor Bloggers." *First Monday* 14 (2).

———. 2011. "China's 'Networked Authoritarianism.'" *Journal of Democracy* 22 (2): 32–46.

———. 2012. *Consent of the Networked*. New York: Basic Books.

Martin, Alexander. 2012. "Mobile Phones Proliferate in North Korea." *Wall Street Journal*, July 28.

Meier, Patrick. 2011. "Do 'Liberation Technologies' Change the Balance of Power Between Repressive States and Civil Society?" PhD diss, Tufts University.

"Mobile Phones in North Korea: Also Available to Earthlings." 2012. *The Economist*, February 12.

Mozorov, Evgeny. 2011. *The Net Delusion: The Dark Side of Internet Freedom*. New York: Public Affairs.

Mozorov, Evgeny, and Philip N. Howard. 2011. "Critical Dialogue." *Perspectives on Politics* 9 (4): 895–900.

Mozur, Paul. 2012. "China's Baidu Strikes Back against Web-Search Upstart." *Wall Street Journal*, August 30.

"News Summary: North Korea to Allow Mobile Internet for Foreigners; Citizens Won't Have Access." 2013. *Associated Press*, 22 February.

Norris, Pippa. 2001. *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*. New York: Cambridge University Press.

"One IP Address for All of PUST." 2012. *North Korea Tech*, August 24. http://www.northkoreatech.org/2012/08/20/one-ip-address-for-all-of-pust/.

Palatino, Mong. 2012. "Malaysia's New Internet Law." *The Diplomat*, August 30.

Park, Ju-Min. 2012. "University Brings Capitalism to Reclusive North Korea." *Reuters*, August 4.

Park, Jun Hyeong, and Seok Young Lee. 2011. "Phone Handset Prices Fall as Users Rise." *DailyNK*, May 20.

Perry, Elizabeth J., and Merle Goldman. 2007. *Grassroots Political Reform in Contemporary China*. Cambridge, MA: Harvard University Press.

Qiang, Xiao. 2011. "The Battle for the Chinese Internet." *Journal of Democracy* 22 (1): 47–61.

Rahimi, Babak. 2011. "The Agonistic Social Media: Cyberspace in the Formation of Dissent and Consolidation of State Power in Postelection Iran." *The Communication Review* 14 (3): 158–78.

Ramstad, Evan. 2012. "Heads Up Android Fans: Here Comes North Korea." *Wall Street Journal*, September 27. http://blogs.wsj.com/korearealtime/2012/09/27/heads-up-android-fans-here-comes-north-korea/.

Rogin, Josh. 2012. "Eric Schmidt: The Great Firewall of China Will Fall." *Foreign Policy*, July 9.

Sanger, David E., David Barboza, and Nicole Perlroth. 2013. "Chinese Army Unit Is Seen as Tied to Hacking Against U.S." *New York Times*, February 18.

Schmidt, Eric, and Jared Cohen. 2010. "The Digital Disruption: Connectivity and the Diffusion of Power." *Foreign Affairs* 89 (6): 75–85.

Shen, Simon, and Shaun Breslin. 2010. *Online Chinese Nationalism and China's Bilateral Relations*. Lanham, MD: Lexington Books.

"South Korea." 2012. OpenNet Initiative, August 6.

Sullivan, Andrew. 2009. "The Revolution Will Be Twittered." *The Atlantic*, June 13.

Sullivan, Tim. 2012. "North Korea Cracks Down on Knowledge Smugglers," *ABC News*, December 31.

"Untitled." 2012. *Yonhap News Report*, July 28.

Timmons, Heather. 2011. "India Asks Google, Facebook to Screen User Content." *New York Times*, December 5. http://india.blogs.nytimes.com/2011/12/05/india-asks-google-facebook-others-to-screen-user-content/.

"Weird but Wired." 2007. *The Economist*, February 1.

Williams, Martyn. 2011. "Koryolink Hits a Million Subscribers." *North Korea Tech*, February 3.

Williams, Martyn. 2012. "Orascom CEO Back in Pyongyang." *North Korea Tech*, October 6.

Wilson, Christopher, and Alexandra Dunn. 2011. "Digital Media in the Egyptian Revolution: Descriptive Analysis from the Tahrir Data Sets." *International Journal of Communication* 5: 1248–72.

Wu, Guoguang. 2009. "In the Name of Good Governance: E-Government, Internet Pornography, and Political Censorship in China." In *China's Information and Communications Technology Revolution: Social Changes and State Responses*, eds. Xiaolong Zhang and Yongnian Zheng, 68–85. New York: Routledge.

Yang, Guobin. 2003. "The Internet and Civil Society in China: A Preliminary Assessment." *Journal of Contemporary China* 12 (36): 453–75.

———. 2009. *The Power of the Internet in China: Citizen Activism Online*. New York: Columbia University Press.

Zhang, Xiaoling, and Yongnian Zheng. 2009. *China's Information and Communications Technology Revolution: Social Changes and State Responses*. New York: Routledge.

Zheng, Yongnian. 2008. *Technological Empowerment: The Internet, State and Society in China*. Stanford, CA: Stanford University Press.

———. 2009. "The Political Cost of Information Control in China: The Nation-State and Governance." In *China's Information and Communications Technology Revolution: Social Changes and State Responses*, eds. Xiaolong Zhang and Yongnian Zheng, 136–55. New York: Routledge.

Zheng, Yongnian, and Joseph Fewsmith. 2008. *China's Open Society: The Non-State Sector and Governance*. New York: Routledge.

Zhou, Yongming. 2005. "Living on the Cyber Border: 'Minjian' Political Writers in Chinese Cyberspace." *Current Anthropology* 46 (5): 779–803.

———. 2006. *Historicizing Online Politics: Telegraphy, the Internet, and Political Participation in China*. Palo Alto, CA: Stanford University Press.