International Journal of Communication 12(2018), 3814–3834 1932–8036/20180005

Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region

JACLYN A. KERR
Lawrence Livermore National Laboratory,[1] USA

This article examines Internet policies across the former Soviet region, showing that many of the region's nondemocratic regimes have adopted similar approaches to control Internet content and use within their territories. The implication that specific control practices are diffusing or being coordinated on within the region is substantiated by close examination of particular approaches and their origins. While these states have made relatively limited use of static content censorship, alternative, less overt controls have spread across the region. Tracing the roles of diffusion and coordination mechanisms, the article demonstrates how, even as overall Internet repression levels have increased, the particular legal frameworks, technical systems, and other control practices used have been deeply influenced by complex regional interdependencies.

Keywords: authoritarianism, Internet, censorship, surveillance

As the Internet's transformative social and political uses have proliferated across the former Soviet Union (FSU), the region's mostly nondemocratic regimes have responded in various ways to the perceived risks and benefits of the technology's further development. Though approaches adopted across the region are not identical, we see significant areas of similarity, with evidence both of uncoordinated diffusion, learning, and emulation, as well as direct collaboration or coercion mechanisms driving this convergence. This article investigates the development of authoritarian and illiberal Internet control practices across the FSU region, analyzing the policies adopted and other approaches taken to managing Internet use within society. Looking at regional and international as well as domestic sources of Internet control practices, it examines dynamics of diffusion and coordination in the region, showing how the policies, legal frameworks and rhetorical postures states adopt influence and are influenced by those of their neighbors—especially among regimes bound by shared institutional and political history. It further suggests that such international diffusion and coordination dynamics play important roles in the ongoing adaptation of authoritarian regime types to the globalized digital environment.

Jaclyn A. Kerr: jackiekerr@gmail.com
Date submitted: 2017-12-07

[1] This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC. LLNL-JRNL-752097.

The article is divided into three sections. The first section introduces the core puzzle. Situating the study within the body of literature on authoritarianism, diffusion, and Internet controls, it addresses the need to better understand how authoritarian regimes adapt to growing Internet use in their societies and the inadequacy of existing "digital dictators' dilemma" unitary decision models for understanding the variety of distributed and transnational actors and interdependencies involved in the evolution of authoritarian state approaches to the Internet. The section provides a framework for understanding domestic, regional, and international influences on state Internet policy development, emphasizing potential interdependencies between the practices of neighboring states, the mechanisms by which control innovations spread, and reasons why they spread to some states and not others.

The second section puts this framework to work, examining Internet control practices adopted in the FSU region and indicating the emergence of a set of shared characteristics suggesting intraregional diffusion or coordination dynamics. Drawing on this Special Section's framework for conceptualizing different nondemocratic Internet control practices, the section examines three significant instances of illiberal or authoritarian Internet practices, variations on which are common across the region. Examining the emergence of (1) limited-censorship approaches to the control and manipulation of online information and discourse, (2) the spread of specific legal and technical surveillance mechanisms, and (3) the development and spread of the "information security" conceptualization of online content's role in national security, the section demonstrates the widespread adoption of several very similar practices in the region and traces the roles of key diffusion and coordination mechanisms facilitating their spread as well as those factors limiting adoption.

The article concludes with a discussion of the importance of the FSU model of Internet control in the broader global context of authoritarian adaptation, suggesting that the distinctive practices examined have contributed to the development of new forms of stable authoritarian rule more fit to withstand the challenges of the digital age.

Domestic, Regional, and International Drivers of Internet Policy Choice

The growth of the Internet has posed challenges for territorial states seeking to manage the impact of the technology within their society and lay down rules for its governance domestically and globally. Offering new forums for public discourse, association, and protest mobilization, the technology has posed particularly significant challenges to nondemocratic states seeking to balance potential economic and societal benefits with the risks of increased political instability. This has prompted a period of experimentation and adaptation globally as Internet use levels—and the stakes for political stability and security—have risen. The approaches adopted have differed dramatically, however, with a wide variety of different practices emerging even across states of similar nondemocratic regime types.

In some ways, the ongoing period of experimentation with regard to Internet control in nondemocratic regimes resembles and extends the period of authoritarian adaptation and "upgrading" in the 1990s and 2000s (Heydemann, 2007). The nature and variety of authoritarian regime types globally changed dramatically during the two decades of increased globalization following the end of the Cold War. Despite the significant teleological hopes that had been attached by many observers to the global collapse

of Communism, the "Third Wave of Democratization" (Huntington, 1991) and the supposed "End of History" (Fukuyama, 1989), this period ultimately ushered in the development of new forms of relatively stable authoritarian regimes more capable of dealing with the more permeable borders, less controlled information flows, and other pressures of globalization. These "hybrid," "electoral" or "competitive authoritarian," "illiberal democratic," or "managed pluralist" regimes typically combined some formal democratic institutions with some characteristics of authoritarian rule (Balzer, 2003; Karl, 1995; Levitsky & Way, 2010; Schedler, 2010; Zakaria, 1997). While allowing more space for some forms of free association, expression, and media than had been permitted by dominant earlier forms of closed authoritarianism, these regimes worked astutely to limit and manage the roles of civil society, protest activism, and independent media in their societies—effectively controlling the framing of more abundant information and activity while accepting the loss of the total control sought by older closed regime types. There often were also limits on the degree or overtness of the abuses in these regimes, basing part of their domestic and international legitimacy on their status as "democracies" and ability to participate in the global system. Compared with closed authoritarian models, they tended to make less systematic use of "high-intensity coercion" (such as violent repression and overt rights abuses) to maintain control. Instead, they were characterized as selecting from a "menu of manipulation" involving many subtle, quasilegalistic, and plausibly deniable forms of control over society—"low-intensity coercion" techniques less likely to evoke global condemnation or erode domestic support (Levitsky & Way, 2010; Schedler, 2002).

These new, seemingly more adaptable regime types also had vulnerabilities, however, best exemplified by the Color Revolutions, Arab Spring, and other popular protest movements of the 2000s and 2010s—movements using the available spaces for public speech and association and often organized in protest around fraudulent elections and other violations of the supposed democratic rules. The growing global use of networked information technologies has further challenged the viability of these regime forms. The literature concerning hybrid and electoral authoritarian regimes and their strategies for "managing" society thus constitutes an important theoretical starting point in an examination of the role and governance of the Internet within contemporary authoritarian regimes. But this scholarly field has done little as yet to explicitly address the role of Internet control practices in the ongoing regime type adaptation.

More recent work on authoritarian learning and diffusion, policy transfer, "diffusion proofing" against protest contagion, and "authoritarianism promotion" takes critical next steps in examining how the emerging alternative regime models spread, and how they have further adapted in confronting the risk of mass-protest mobilization. This work examines how nondemocratic states learn from each other's successes and failures, attempting to emulate those policies that appear to alleviate instability pressures. Work has shown that, in response to the Color Revolution and Arab Spring, government officials have used explicit rhetoric about avoiding similar events at home, and regimes have adopted new laws and control techniques aiming to deter and constrain the abilities of activists to emulate protest movements observed in other states. The widespread adoption of illiberal civil society and media laws, for example, have been widely noted in the late 2000s and early 2010s (Ambrosio, 2010, 2017; Hall & Ambrosio, 2017; Koesel & Bunce, 2013; Way, 2015).

This work builds on a broader body of research on the impacts of diffusion and coordination on state policy choices that has examined the adoption of a range of policies, technologies, and innovations.

From financial rules to military weapons systems, this body of literature has sought to demonstrate causal linkages between the ostensibly autonomous choices of different states, noting appropriate methodologies for studying such interdependencies, and theorizing the underlying causes and mechanisms. Regime decisions, it is argued, can be influenced by uncoordinated diffusion processes, when decision makers observe and learn from the policy choices of other states or when the policy choices of some states alter the costs and pressures associated with similar policy choices. They can also be impacted by coordination processes, where states collaborate in the development and implementation of shared policy frameworks and approaches or where states are subject to coercion to comply with group norms or the will of one powerful state. Some characteristics of particular policies or innovations—including the cost, human capital, and organizational requirements—have been indicated as key determinants of the extent and speed of their diffusion, limiting which of the states that might wish to emulate an approach are capable of doing so successfully. When, during a relatively short period of time, states are seen as disproportionately adopting similar policy approaches despite differences in their domestic characteristics or international positions, this "policy clustering" can be evidence of the impact of diffusion and coordination on state behavior. Such interdependency is most evident when specific innovations, such as particular legal frameworks, technologies, or other policy innovations are copied by numerous states following their initial introduction, and when causal processes can be traced showing a direct line of influence (Hall & Ambrosio, 2017; Horowitz, 2010; Levitsky & Way, 2010; Simmons & Elkins, 2005).

Though the literature on policy diffusion and coordination has yet to significantly address the spread of Internet control practices, many of the causally significant mechanisms and characteristics identified seem particularly relevant. From the early 2000s onward, nondemocratic states have experimented with a wide variety of approaches for addressing a complex new technology, the social and political repercussions of which have been poorly understood but highly consequential, and for which many have lacked immediate relevant expertise or organizational capacity for the development of in-house control solutions. Global norms on "Internet freedom," linking Internet censorship with democratic norm violations and efforts to name and shame norm-violating states, particularly heightened the pressure on hybrid regimes facing potential legitimacy costs at home and abroad for adopting overt restrictions, but also facing the simultaneous risk of mass protest mobilization if no control measures were developed. While overt systemic censorship approaches were adopted early by China and many closed authoritarian states, the "low-intensity coercion" equivalents for Internet control practices were not immediately evident.

Today, government efforts to control the use of the Internet draw on an ever-widening variety of technical, legal, and extralegal tools. Much of the existing research on authoritarian Internet restrictions is the work of advocacy groups cataloguing rights abuses, or technical experts demonstrating the use of particular control technologies—excellent empirical contributions, but without a theoretical focus on explaining the role of control practices in the broader context of authoritarian rule. Some work has made particularly valuable contributions to the field's development. The University of Toronto's Citizen Lab delineated different "generations" of controls, comparing a family of static "first generation" censorship approaches by filtering and site blocking (techniques that were becoming increasingly common by the late 2000s) with more subtle "next generation" approaches they saw emerging at the time, in which censorship was often temporary or plausibly deniable, and which used content-generation and surveillance in addition to censorship, or relied on quasidemocratic legal mechanisms (Deibert & Rohozinski, 2010). Research on

significant cases such as China and Russia has contributed to a more holistic understanding of how control mechanisms combine in particular national settings (King, Pan, & Roberts, 2013; Soldatov & Borogan, 2015). Studies tracking the emergence and global use of particular control technologies, such as surveillance equipment and computational propaganda, have increased awareness of the widespread use of these techniques. But there is still little understanding of the role of Internet control in the broader development of political regimes or the dynamics driving the spread of illiberal and authoritarian practices internationally.

Some theoretical analyses have attempted to explain regime Internet policy development by focusing on individual states and factors influencing policy choice. Decisions about how much to restrict the Internet are stylized as "digital dictator's dilemma" trade-offs, whereby regimes select optimal restriction levels so as to balance the potential destabilizing risks of unfettered Internet use with the economic and legitimacy costs of restriction (Drezner, 2010; Shirky, 2011). Such models are clearly helpful for understanding some of the dynamics driving difficult policy decisions. But the focus on individual state decisions downplays the extent to which the behavior of groups of states is often interdependent, with mechanisms of diffusion and coordination playing key roles in spreading particular practices between states. The focus on a decision about restriction level likewise underemphasizes the importance of specific Internet control innovations—sometimes varying more in approach than level—and the impact of their introduction on other states globally. Modeling the emergence of Internet control practices as a rational decision process by a unitary actor with near-perfect information is likewise problematic. This approach fails to appreciate the multitude of actors and institutions potentially involved, the iterative mimetic development of some practices without conscious centralized deliberation, and the significant uncertainties, information shortages, and learning heuristics informing actual reasoning about policy trade-offs. To fully explain individual regime Internet policy development, it is still useful to take account of the factors and processes likely to influence such a decision calculus. But such a model should be regarded as a useful fiction, with clear attention to the variety of actors and less rational and less centralized mechanisms driving the actual development and adoption of particular control practices. Special attention should be payed to regional and international interdependencies, the roles of transnational networks and markets, and how a regime's awareness of and reaction to existing Internet control innovations introduced by other states or collaboration or coercion between states can influence the adoption of particular control practices.

Overall, while regime type and the perceived instability threat emerging from growing Internet use are likely to be highly predictive of a regime's attempt to implement some forms of Internet restriction, all other things being equal, the specific policies attempted and their successful implementation, as well as the development of more decentralized control practices, are likely to be driven at least as much by the internationally available Internet control solutions of which a regime is aware, a regime's financial and organizational capacity to implement these or to access assistance in their implementation, and the policies selected by other states in the regime's reference group or endorsed by regional and international organizations with which a state is closely engaged.

The following section examines how, in spite of significant instability concerns relating to growing Internet use, most states of the FSU region were late and only partial adopters of overt Internet controls through censorship. In tracing the spread of alternative Internet control innovations through much of the region, however, it demonstrates the significance of regime type and cultural appropriateness, reference

group learning, market forces, and the roles of support groups and regional collaboration in driving the spread of particular Internet control approaches. The section shows how—despite internal variation between states—the mechanisms of diffusion and coordination have led to the emergence of a somewhat unique FSU regional approach to Internet control across the nondemocratic regimes of the former Soviet region.

The Post-Soviet Internet: Regional Diversity and Similarity

Authoritarian adaptation to Internet development in the FSU region in the 1990s through the 2010s provides a valuable case study for gaining greater insight into the factors driving Internet control policy choices and their implementation in nondemocratic states. The region demonstrated several predictable patterns based on the domestic characteristics of states. The relative degrees of restriction of Internet use and content in the region in many regards paralleled overall differentiations of regime type during this period, with the most closed authoritarian regimes adopting stricter Internet content censorship, while the more open hybrid regimes permitted greater online freedom. Internet control measures increased with growing Internet use. New restrictions and policy shifts likewise responded to growing domestic stability concerns, with more restrictive policies often adopted during the months or year immediately following major mass protest movements within the country in question (Kerr, 2016).

Yet the region also demonstrated some unique tendencies, with certain Internet control innovations (such as systemic technical content filtering) showing relatively limited uptake compared with other global regions, while other innovations (such as the use of legal and temporary restrictions, surveillance technologies, and unique conceptual frameworks for "information security") emerged in the region and spread rapidly, reflecting similarities of regime type, but also common institutional legacies and patterns of mutual learning, diffusion, and cooperation within the region.

The remainder of this section examines the spread or nonspread of several Internet control innovations across the FSU region, examining how regime characteristics, diffusion, and coordination impacted the adoption and implementation of these innovations across the region's nondemocratic regimes. First I examine how legalistic or plausibly deniable "next generation" measures—including content production and manipulation—took root in the region, often in partial substitution for emulation of cutting-edge approaches to pervasive Internet censorship being implemented in other regions. I then examine the roles of diffusion and collaboration in the spread of particular approaches to surveillance and the conceptualization of Internet content's relationship to national security.

Limited Content Censorship and Discourse Manipulation

While experiencing relatively limited Internet censorship compared with authoritarian regimes in other regions, the FSU region emerged by the early 2010s as exemplary of what the OpenNet Initiative had dubbed "next generation" approaches to Internet control. Rather than leaving the Internet completely uncontrolled or unmonitored, many states of this region had developed similar economic, legal, technical, and institutional arrangements that facilitated alternative forms of state control over Internet content and users (Deibert, Palfrey, Rohozinski, Zittrain, & Haraszti, 2010). Even as controls over the Internet in the region have tightened considerably in the 2010s, many of these unique characteristics have persisted,

including, notably, a relatively low level of static censorship paired with significant degrees of proregime content production and manipulation, and, where content is blocked, a reliance either on plausibly deniable temporary takedowns or the use of legal rules and processes to legitimize targeted censorship.

Although mostly abstaining from Chinese-style pervasive censorship regimes, countries in the FSU region have used various temporary or deniable techniques to block access to critical sites and resources at politically sensitive moments. Occasionally, this action is overt, as in Armenia in February 2008, following postelection protests, when the government declared a state of emergency, temporarily shutting down numerous online resources and restricting media coverage. Less overt techniques frequently have been used for a similar purpose, however. During elections in Belarus (in 2006), Kyrgyzstan (in 2005), and Russia (in 2008–9, 2011–12), proregime actors mounted distributed denial of service (DDoS) attacks against the sites of opposition groups, independent media outlets, political blogs, and nongovernmental organizations, making these sites inaccessible at critical moments. Such outages are sometimes reported as resulting from technical failures or overuse.

Proregime content production has been extensively used by countries in the region, disrupting or drowning out critical speech, leaking compromising content about opposition figures, and providing the appearance of authentic discourse. Proregime hackers, youth groups, trolls, bloggers, and other actors mount hard-to-attribute informational or cyberattack campaigns on behalf (or at the behest) of the regime, while seeking to maintain plausible deniability as to the government's actual involvement. Such campaigns have been used to target activists and change narratives in Russia, for example, where, in 2011, sensitive private phone calls of then opposition leader Boris Nemtsov were published online and contributors to Alexei Navalny's anticorruption organization were called and harassed by individuals with Nashi youth-group connections. Hip Kremlin-funded videos supporting Vladimir Putin have been targeted at young Internet users, and trolls paid to intervene in online discussions on topics and disrupt critical discourse (Elder, 2012; Fedor & Fredheim, 2017; Ragan, 2012; Subbotovska, 2015). Similar proregime blogging and commenting campaigns were used in Kazakhstan in 2011–12 to muddy the waters as to the correct narrative of events surrounding the bloody crackdown on an oil worker strike in the western city of Zhanaozen (Kerr, 2016; Lillis, 2011).

Various types of legal restrictions have also played a significant role in the approach to Internet control in the FSU region. "Laws, decrees, and administrative orders" are used to single out particular categories of content as illegal, prosecute content producers or intermediaries, promote self-censorship, and block particular sites or force the removal of content (Deibert, Palfrey, Rohozinski, Zittrain, & Haraszti, 2010, p. 124). But they do so while maintaining a semblance of democratic process and constitutional freedom of expression. Laws against defamation or slander, against offensive comments about state officials, or for the protection of copyright are commonly applied to online content. Belarus, Uzbekistan, Kazakhstan, Tajikistan, and Russia have all used legal measures to "protect moral values, public order, national security, state secrets, and other privileged data" (Deibert, Palfrey, Rohozinski, Zittrain, & Haraszti, 2010, p. 124). Belarus, Kazakhstan, Uzbekistan, and Russia have each adopted laws requiring some categories of websites to register as "mass media"—subjecting their content to more onerous regulations. Laws often use poorly defined terms and provide no clear procedure for suspended sites to regain their

status. Following Russia's 2011–12 "White Ribbon" protest movement, numerous new laws with ostensible goals, ranging from the protecting children online to preventing terrorism, have been used to target critical voices.

Some quite specific legal and technical mechanisms for handling issues of Internet control have diffused widely across the FSU region. Here, Russia has played a significant role as exemplar to some of its neighbors, with its legal and technical frameworks for permitting wiretapping and surveillance as "lawful interception" and its 2000 Doctrine of Information Security both being widely emulated by neighboring similar-regime-type countries. Russia's mass surveillance system, System for Operative Investigative Activities (SORM), which is grounded in a legal framework for permitting "lawful interception" of communications by KGB[2]-successor security organs and other government entities, but also involves specific technological systems and infrastructures, has proven widely influential. Russia's broad conceptualization of security concerns around protecting a "national informational space"—going beyond the protection of data and computer networks to encompass media, online discourse, and other flows of information within a country—has likewise spread across the region, implicitly or explicitly influencing policy and conceptual frameworks in many countries.

Lawful Interception and Surveillance Technology

The mechanisms of within-region learning and diffusion are particularly apparent in relation with the development of national surveillance systems and capabilities. Here, the emulation of the Russian approach to "lawful interception" and surveillance has taken legal, institutional, and technological forms. Connections between Russian private-sector security technology producers, the FSB, and the security services of neighboring post-Soviet states can be traced to the period of the Soviet collapse and continue to foster collaboration and technical and legal diffusion across the FSU region. Before the breakup of the union, the KGB had a large research budget, but the successor FSB's budget for research was only one-tenth the size, prompting an exodus of skilled technical researchers and developers into the private sector (Bourgelais, 2013). Many of the firms that emerged in the growing computer security market, therefore, had longstanding relationships with the FSB that fostered patterns of ongoing collaboration. Likewise, before the collapse, the KGB had a vast network of regional branches across the Soviet republics. After the collapse, many of these became the national security agencies of the emerging independent states. They continued to often follow the FSB's lead, adopting similar laws and technologies to allow for surveillance and embracing the same language of "information security" for discussion of national data networks (Soldatov & Borogan, 2012).

The SORM system is a technical infrastructure built to substantiate a legal framework of "lawful interception" in which "communications service providers . . . and telecommunications equipment manufacturers are required to ensure that their network and equipment [are] compatible and made accessible to a monitoring facility from which analysts request, receive, store, and analyze intercepted data"

[2] The KGB, standing for Komitet Gosudarstvennoy Bezopasnosti (or Committee for State Security), was the Soviet Union's main security agency from the 1950s until its collapse. In Russia, it was succeeded by the FSB, the Federalnaya Sluzhba Bezopasnosti or Federal Security Service.

(Omanovic, 2014, para. 6). Internet service providers (ISPs) are required to pay for and install "black box" monitoring nodes on their networks, each known as a "*Punkt Upravlenia*" or "Control Point," and provide separate cables directly connecting these nodes to local FSB centers. In Russia, a whole industry has developed around the production of hardware and software products to meet the SORM standards. As the model has spread through surrounding states, Russian companies such as MFI-Soft and PROTEI often have served as suppliers to the region. Multinational equipment manufacturers based in Israel, the United States, and Europe also have played roles, working with local companies and authorities to guarantee that products they sell are compatible with the SORM system. Local companies in the various countries have developed market niches certifying network components and other hardware and software products as SORM compliant, sourcing and reselling these products, and serving as the "prime bidders for SORM-related contracts" (Omanovic, 2014, para. 14).

Today, at least nine states (in addition to Russia) of the former Soviet Union have emulated aspects of the Russian legal, technical, and institutional approach to electronic surveillance.[3] Some of these systems—either underlying legal frameworks or technical implementations—have been in place for years, while others have been adopted or significantly updated in the late 2000s or early 2010s, apparently in response to growing concern in the region about the role of digital communications in political unrest. Following the Russian lead in the 2000s, for example, Belarus, Moldova, and Ukraine all established similar specialized units known as Department K under their respective Ministries of Internal Affairs, tasked with confronting "computer crime" (Rohozinski & Haralampieva, 2007).

Ukraine, Belarus, Kazakhstan, and Uzbekistan each have implemented sophisticated SORM-based systems, with Kyrgyzstan, Tajikistan, Turkmenistan, and Azerbaijan having made varying degrees of progress toward developing similar technical surveillance systems. In Belarus, President Alexander Lukashenko introduced SORM by executive order in March 2010, building on a 1999 law, On Operative Investigative Activities, which provided for this type of "lawful interception." The system was installed on the Byfly digital network (largest broadband provider in the country) by national telecom company Beltelecom in April 2012, with much of the equipment supplied by the Russian company Digiton ("Beltelecom Installs," 2012). Ukraine, which already had a SORM system in place, adopted stricter SORM system requirements in 2010, leading to roll-out of new SORM equipment in 2011, supplied by the Israeli company Iskratel and approved by the Ukraine's Security Service, the SBU ("Freedom on the Net," 2012; "Human Rights in Ukraine," 2007; Soldatov & Borogan, 2012).

In Central Asia, Kazakhstan and Uzbekistan have the most advanced technical surveillance abilities, "capable of interception of landline telephone communications, Internet traffic, semi-structured data such as SMS, MMS, and forum posts, and automated voice and facial recognition" (Bourgelais, 2013, pp. 6–7). The Israel-based offices of the multinationals NICE Systems and Verint Israel have helped these two countries develop cutting-edge monitoring centers, contracting directly with their respective KGB-successor security agencies, the KNB in Kazakhstan and the SNB in Uzbekistan (Omanovic, 2014; Privacy International, 2014).

[3] The only exceptions among the non-Baltic FSU states are Armenia and Georgia.

Other FSU countries in Central Asia and the Caucasus have made efforts to implement similar surveillance systems, with varying degrees of progress and success. Kyrgyzstan followed the Russian lead when, in August 2012, the State Committee of National Security announced a draft national regulation for lawful interception modeled on the SORM system. In a subsequent evaluation of potential equipment suppliers, the Kyrgyz parliament's Defense and Security Committee found Russian devices much more affordable than those of the Israeli company, Verint (Soldatov & Borogan, 2012). Tajikistan's government has developed the ability to intercept both landline phones and Internet traffic, while Turkmenistan's less researched system has at least the ability to collect extensive data through mobile phones (Bourgelais, 2013). Azerbaijan has made an unsuccessful attempt in the 2000s to employ SORM-type Internet surveillance technologies, but uses less sophisticated measures (such as visits by security officials to ISPs and Internet cafes) to acquire similar information as needed (Rohozinski & Haralampieva, 2007).

Information Security Doctrines and Internet Content

In addition to the influence of uncoordinated diffusion and emulation processes, approaches to Internet control in the FSU region also have been the subject of more coordinated efforts, with states collaborating with neighbors through bilateral agreements, regional organizations, and international organizations to develop and promote common strategies, legal postures, and normative agendas. These mechanisms are particularly apparent in the spread of the "information security" conceptual framework for connecting online content to national security policy. Summit agreements, cooperation pacts, joint security operations, and international conduct proposals have all been used as vehicles for building regional "information security" cooperation, framed not only around protection from data breaches, cyberattacks, and other threats to computer networks and data, but also against the fear of Internet-leveraging Arab Spring and Color Revolution-type events. The conceptual convergence within the region also demonstrates the significance of the "logic of appropriateness," as this approach fits well with the region's cultural and historical perspective on the risks emerging from free flows of information. Coordination efforts emerge as part of a global normative contestation with Western democracies over the appropriate understandings of the relationship between state sovereignty, the Internet, and security.

The "information security" approach has spread broadly within the FSU region, with doctrines and formal national security documents of many countries in the region having integrated language similar to that of the Russian 2000 (and 2016) Doctrine of Information Security. Since 2001, for example, Belarus's law implementing the country's Concept of National Security has included explicit discussion of the Internet as a possible threat to "information security" (Deibert, Palfrey, Rohozinski, Zittrain, & Haraszti, 2010; Republic of Belarus, 2001). In Ukraine, in 2009, a Doctrine of Information Security (President of Ukraine, 2009) was passed by presidential decree (Ivzhenko, 2009), which defined its scope broadly to encompass "protection of the vital interests of the individual, society, the state, preventing damage caused through incomplete, untimely or unreliable information" (Coynash, 2011, para. 4). Uzbekistan's 2002 Law on Principles and Guarantees on Access to Information allowed government restriction of an individual's information access when it was deemed critical to protecting that person "from negative informational psychological influence" and allowed other government controls over information to balance against "threats in the sphere of information security" and "ideas of terrorism and religious extremism" (Deibert, Palfrey, Rohozinski, Zittrain, & Haraszti, 2010, p. 270). A 2006 "recommendation on filtering," issued by the Tajik

government's Communications Regulation Agency before presidential elections urged ISPs to "engage in filtering and block access to Web sites that aim to undermine the state policy in the sphere of information . . . for the purpose of information security" (Deibert, Palfrey, Rohozinski, Zittrain, & Haraszti, 2010, p. 232). Kazakhstan has a "multilevel" information security policy involving the work of multiple government ministries and agencies. Young Internet users in Moldova were charged, in 2008, with using critical online comments to threaten the country's stability and territorial integrity and attempt to "overthrow the constitutional order" (Ben Gharbia, 2008, para. 2). Kyrgyzstan's 2005 Program for Information Security used vague language with potential application to Internet content restrictions (Deibert, Palfrey, Rohozinski, Zittrain, & Haraszti, 2010).

Although diffusion through emulation has clearly played a significant role in spreading these measures, more deliberate coordination has also played a role in the spread of the "information security" approach, including both coercive pressure from Moscow as well as collaboration through regional and international organizations. Such efforts can be seen in recent undertakings of the Commonwealth of Independent States (CIS), the Eurasian Economic Union (EEU), the Collective Security Treaty Organization (CSTO), and the Shanghai Cooperation Organization (SCO). At a CIS[4] summit in September 2012, for example, heads of state of the CIS countries announced support for a plan to found a CIS Center of Cybersecurity similar to the Community Emergency Response Team (CERT) model used in many countries and regions. Earlier that year, the Russian Ministry of Communications' Moscow-based research center, VNIIPVTI, had been charged with training information security experts for the CIS.[5] There can be little doubt, given the common conceptual understanding of "information security" in the region, that the center and training program envisioned were based on a broad understanding of security threats, including much from the Internet's content layer.

Although the EEU is ostensibly an economic union—not focused on matters of media or political control—discussion of a "single information space" within the union suggests that this organization might also provide mechanisms for coordination on control of the Internet and media (European Parliament Members' Research Service, 2015). In March 2015, for example, Russian Minister of Telecom and Mass Communications, Nikolay Nikiforov, met Belarusian Minister of Information, Liliya Ananich, to discuss the role of a single information space in the two countries' economic union (Dorozhkina, 2015).

More ominously, at a September 22 meeting in Bishkek, titled "Informational Cooperation Between Russia and Kyrgyzstan in the Framework of Eurasian Integration," Rossiya Segodnya (Russia Today) state media conglomerate director Dmitry Kiselyov discussed his vision for the future of the Eurasian media system with Kyrgyz journalists while implicitly threatening the Central Asian country's continued existence. Kiselyov, a sensationalist TV personality sometimes referred to as Russia's "chief propagandist," is known

[4] The CIS was founded in 1991, after the breakup of the Soviet Union. Its full and associate members have included all former Soviet states, except for the three Baltic countries. Tensions with Russia have led Georgia (August 2009) and Ukraine (May 2018) to withdraw from the organization, and Moldova has also considered doing so ("Georgia Finalizes," 2009; "Moldova Says," 2018; "President Signed a Decree," 2018).

[5] As of December 2012, the regional CERT project had been postponed, with an eye to first developing national-level centers (Soldatov & Borogan, 2012).

for extreme public statements (including comments about reducing the U.S. to a mound of radioactive dust and burning the hearts of deceased homosexuals) and is a master espouser of anti-Western conspiracy theories ("Dmitry Kiselyov's Meeting," 2015; "Russia Media Boss," 2015). Kyrgyzstan had only joined the union the previous month and has a history of more independent media and political turnover than most EEU members, and its journalists were warned that their country "has a choice," stressing the importance of journalism as an instrument of promoting national values and stability. "Following the path of Eurasian economic integration is the choice of national interests," Kiselyov explained. "Unfortunately we see today how countries simply disappear and there is no guarantee that Kyrgyzstan will also not disappear" (Michel, 2015, para. 5).

The CSTO and SCO have played particularly important roles in regional coordination around and promotion of a unified approach to control of information and the Internet in the name of "information security." The CSTO, a military alliance of Russia, Armenia, Kazakhstan, Kyrgyzstan, Tajikistan, and Belarus,[6] founded in 1992 and sometimes referred to as the "NATO of the East," took steps in the early 2010s to develop a unified system for control of threatening online content—framed explicitly as a reaction to the role of the Internet in the Arab Spring and Color Revolutions ("CSTO Grapples," 2011; Kucera 2010, 2011). In December 2010, then-CSTO General Secretary Nikolay Bordyuzha announced that, in an operation called PROXI, the CSTO had discovered and was going to shut down 2,000 problematic websites that were "spread[ing] information which may cause political damage to our states [by stirring] national or religious hatred or suppl[ying] information for terrorist groupings" in CSTO countries. Bordyuzha described the operation as "the first experience of fighting against criminals in the virtual space on a scale of the whole CIS." Borduyzha specifically addressed the political nature of the website selection, explaining that "practically all post-Soviet republics [had seen] cases when certain political forces widely used Web resources to manipulate people's moods—Moldova, Georgia, Ukraine, and recently Kirgizstan" (Kucera, 2010, paras. 2–5).[7]

An August 2011 CSTO summit in Astana, Kazakhstan, furthered the development of the alliance's "information security" program, with participants vehemently endorsing their cooperation to protect each other from events akin to those of the Arab Spring. While stepping up efforts to develop a "Collective Rapid Reaction Force" to intervene at moments of crisis, CSTO country leaders also announced further plans to "jointly counter potential threats in cyber space." Discussing plans for stepped-up information security cooperation, Bordyuzha explained the shared concern. "No military contingents or groups of gunmen are needed to destabilize the situation in this or that state when information technologies are at their disposal," he explained. In his statement endorsing the plan, Belarusian President Lukashenko, the CSTO's rotating chair at the time, was very clear about the connection with the Arab Spring. "Many new goals have appeared in light of recent world events, including those in the Arab states and in North Africa," he explained. "We

[6] Uzbekistan was a member, but withdrew in 2012 (Kilner, 2012).

[7] Explaining that "information can be a weapon" and that "people use the Web to stir nationalistic feelings—or, to calm down people whom they consider to be too active," Borduyzha justified CSTO plans for ongoing "information war against terrorism and drug trafficking" and joint "operations to close extremist Web sites" (Kucera, 2010, paras. 4–5).

have agreed that our countries will work out measures to fight potential threats, primarily in the information sphere and cyber space" (Kucera, 2011, paras. 4–7).

Although the terminology used to advocate various controls on the Internet's content layer often sounds similar to that used in discussion of narrower "cybersecurity" objectives, such as securing computers, data, and computer networks, this CSTO emphasis on "information security" is understood in the much broader sense. Lest there be any misunderstanding as to the intended meaning of "information security" in these discussions, in a 2012 interview, Vladislav Shushin, counselor of the secretariat of the CSTO and an expert of information security, is quoted explaining that:

> The CSTO member-states look at information security from the international point of view, from the perspective of protecting national interests. It's not about the technology only (i.e., the protection of computer networks, commanding systems and so on). But it's also the political-ideological area—combating the misuse of information technology to undermine the political situation, and creating confrontational relationships. The CSTO is making sure that such crimes are investigated jointly. (Soldatov & Borogan, 2012, para. 40)

The SCO, founded in 1996 to "[promote] Central Asian cooperation on security issues . . . and energy" (European Parliament Members' Research Service, 2015, para. 20), has taken similar measures to promote a common understanding of and commitment to this control-oriented conception of information security. The organization includes China, alongside Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan. At their 2009 summit in Yekaterinburg, member states signed an agreement on Cooperation in the Field of International Information Security that was later ratified by four members and came into force in June 2011 (McKune, 2015; "SCO Responds," 2011). At the June 2011 SCO summit in Astana, Kazakh president, Nursultan Nazarbayev, used his opening address to promote the development of "an alliance-wide cyber police force" and the "[inclusion of the concepts] of 'electronic borders' and 'e-sovereignty' into international law." In a 2012 summit, the SCO countries then reached an agreement for "joint measures to be taken by their secret services to 'prevent and disrupt the usage of the Internet for terrorist, separatist and extremist purposes'" (Soldatov & Borogan, 2013, para. 27).

SCO countries have also collaborated to promote these regional concepts and norms on the international level. In September 2011, Russia, China, Tajikistan, and Uzbekistan submitted a joint proposal for an "International Code of Conduct for Information Security" to the 66th session of the United Nations General Assembly. The proposal stressed the "sovereign right of states" in determining Internet-related policy (as opposed to the civil society, business, or engineering communities that also participate in the Internet's various multistakeholder governance institutions). It asked states to voluntarily pledge to support each other in combating the use of the Internet for "criminal and terrorist activities" and to also pledge to abstain from "carry[ing] out hostile activities or acts of aggression" via the Internet. These promises carried with them the commitment to "[curb] the dissemination of information that incites terrorism, secessionism, or extremism, or that undermines other countries' political, economic, and social stability, as well as their spiritual and cultural environment" (Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan, 2011, pp. 3–4; see also McKune & Ahmed, this Special Section). The 2011

proposal failed to gain global support (Anderson, 2011; Carr, 2011; Farnsworth, 2011). In January 2015, all six SCO members (Russia, China, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan) submitted an updated version of the proposal, endorsing the same basic positions, however, apparently hoping to gain wider international approval in the more uncertain post-Snowden and post-Stuxnet global context of diminished U.S. Internet governance leadership legitimacy (Grisby, 2015; McKune, 2015; Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan, 2015; Rõigas, 2015).

These proposals have been widely interpreted by Western scholars, policy makers, and members of the Internet governance community as Russian- and Chinese-led attempts to legitimize greater state control over Internet content for the management of domestic protest and dissent such as observed in the Arab Spring. This is in keeping with other Russian- and Chinese-led efforts during this same period, such as the 2012 submission of a proposal at the International Telecommunications Union's WCIT-12 conference in Doha by Russia, China, Saudi Arabia, Egypt, Sudan, and the UAE. The Russia-led proposal called for alterations to the International Telecommunications Regulations, giving more legal authority over the Internet to national governments, and expanding the role of the International Telecommunications Union and UN (and multilateral processes) in Internet governance (Shackelford, Oti, Kerr, Korzak, & Kuehn, 2015).

The collaboration with non-FSU states in some of these overtures demonstrates the potential resonance of the "information security" conceptual framework with nondemocracies beyond the region. Russia and China have also collaborated bilaterally. At a May 8, 2015, summit preceding the 70th anniversary celebrations of World War II victory, Presidents Xi Jinping and Vladimir Putin met to discuss various areas of future collaboration between their two countries, each professing their shared heritage as the two countries that had borne the most costs of the war (Farivar, 2015; Roth, 2015). The talks, which included topics concerning both economic and military cooperation, resulted in the adoption of an "Information Security Non-Aggression Pact." The pact included plans to work jointly to counteract the use of information technologies to "'destabilize the internal political and socio-economic atmosphere,' 'disturb public order' or 'interfere with the internal affairs of the state'" (Razumovskaya, 2015, para. 1).

Conclusion: Diffusion, Coordination, and the FSU Model

The FSU example is telling for understanding how Internet policy evolution works not just in the world's most prominent powerful states but in other states of varying regime type, state capacity, and technical know-how, interacting in a global environment replete with patterns of authoritarian learning and diffusion, policy coordination, and technology transfer and in the face of international normative pressures. Some aspects of policy change in the region have followed expected patterns based on state domestic characteristics. More restrictive policies were adopted earlier by the most closed authoritarian regimes, with states of less closed regime types long avoiding overt censorship and tending toward more subtle forms of restriction. Growing Internet penetration and domestic political instability have generally led to expected increases in online restrictions. But the patterns of Internet policy adoption in the region have also clearly demonstrated the significance of interdependencies across states, with processes of diffusion and coordination playing important roles in spreading particular approaches to Internet control.

Given the degree of similarity of policies adopted by many states of the region, it is possible to identify a fairly unique approach to authoritarian Internet control emerging from the FSU region. Even as restrictiveness levels have grown, the states in the region have generally relied less heavily on overt, static forms of content censorship compared with states of similar regime types in other regions. On the other hand, regimes in the region have been early adopters of more subtle, temporary, legal, or plausibly deniable forms of "next generation" controls, increasing use of surveillance, proregime content production, behind-the-scenes pressures, and court cases or legal justifications to alter the online informational environment. Particular legal, technical, and institutional frameworks have spread across the region, with Russia's "lawful intercept" framework, SORM surveillance system, and Doctrine of Information Security being widely emulated. Coordination across the region through regional and international organizations has also further reinforced these shared approaches, particularly increasing the regional and international prominence of the "information security" conceptual framework.

The model for Internet control that emerged in the FSU region fit well with commonalities of states in the region—but also with the broader problems faced by many authoritarian regimes adapting to the new digital information environment. Although suited particularly to Soviet legacy institutions, the FSU approach has also been generally well suited to "hybrid regime" states. In keeping with other "low-intensity coercion" forms common across hybrid regimes, the emphasis on legal mechanisms, national security justifications, and less obvious forms of content manipulation is more equipped to maintain vestiges of democratic legitimacy and norm-abidance than the overt censorship-focused approaches pioneered by states like China in the 2000s. Although the FSU region has experienced considerable authoritarian backsliding, most of the nondemocratic states of the region have remained some type of hybrid regime, retaining formal electoral institutions, constitutions, and protections of democratic liberties, even though the actual functioning of such laws and institutions is severely limited. Regime hybridity has become common internationally as well in the post-Cold War era, as new democracies fail to consolidate and overtly nondemocratic regimes face normative pressure.

Drawing on the special section's framework, the mix of Internet controls examined in the FSU region clearly contains elements of both "illiberal practices"—that violate individual autonomy, dignity, and human rights—and "authoritarian practices"—which undermine the functioning of democratic institutions and processes, particularly through breaking mechanisms of public accountability (Glasius & Michaelsen, this Special Section). But the focus on the highly targeted, legally justified, and minimally visible measures arguably leans the balance more heavily toward authoritarian effects. Regimes maintain a façade of democratic freedoms and processes, while undermining the bases of democratic accountability. It is this accountability and consequent public mobilization against hypocrisy and abuses that most endangers hybrid regime stability and survival. By limiting overt rights abuses to those handful of targets most critical to accountability processes, while avoiding widespread and obvious abuses that would be evident to the majority of the population, these regimes are best able to maintain a low-intensity coercion approach to nondemocratic rule, which maintains regime stability partly through the maintenance of public support.

The FSU model's subtlety fit particularly well with the international normative environment of the late 2000s and early 2010s—a period of growing international normative consensus around the acceptance of "Internet freedom" as a universal right akin to freedom of expression and association. As this consensus has eroded somewhat in the 2010s, the FSU model has continued to evolve and spread, arguably influencing the

Internet politics of many states beyond the region. In this environment, it is more important than ever to be aware of and attentive to the role of complex interdependencies in shaping Internet policy adaptation and the spread of Internet control practices.

References

Ambrosio, T. (2010, 1 November). Constructing a framework of authoritarian diffusion: Concepts, dynamics, and future research. *International Studies Perspectives*, *11*(4), 375–392.

Ambrosio, T. (2017). The fall of Yanukovych: Structural and political constraints to implementing authoritarian learning. *East European Politics*, *33*(2), 184–209.

Anderson, N. (2011, September 20). Russia, China, Tajikistan propose UN "code of conduct" for the 'net. *Ars Technica*. Retrieved from http://arstechnica.com/tech-policy/news/2011/09/russia-china-tajikistan-propose-un-code-of-conduct-for-the-net/

Balzer, H. (2003, January 1). Managed pluralism: Vladimir Putin's emerging regime. *Post-Soviet Affairs*, *19*(3), 189–227.

Beltelecom Installs User Control System (SORM). (2012, April). *Charter 97*. Retrieved from https://charter97.org/en/news/2012/4/30/51553/

Ben Gharbia, S. (2008, June 13). Moldavia: Sequestration of personal computers of 12 young people for posting critical comments online. *Global Voices Advocacy*. Retrieved from https://advox.globalvoices.org/2008/06/13/moldavia-destruction-of-personal-computers/

Bourgelais, P. (2013, June). Commonwealth of surveillance states. *Access Now*. Retrieved from https://s3.amazonaws.com/access.3cdn.net/279b95d57718f05046_8sm6ivg69.pdf

Carr, J. (2011, September). 4 problems with China and Russia's international code of conduct for information security. *Digital Dao*. Retrieved from http://jeffreycarr.blogspot.com/2011/09/4-problems-with-china-and-russias.html

Coynash, H. (2011, December). A dangerous law, indeed. *KyivPost*. Retrieved from http://www.kyivpost.com/opinion/op-ed/a-dangerous-law-indeed-118078.html

CSTO grapples with cyber security. (2011, August 15). *RT International*. Retrieved from https://www.rt.com/politics/csto-cyber-threat-bordyuzha/

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

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

Dmitry Kiselyov's meeting with Kyrgyz journalists. (2015, September). *KLOOP.KG*. Retrieved from http://kloop.kg/blog/2015/09/22/live-vstrecha-dmitriya-kiseleva-s-kyrgyzskimi-zhurnalistami/

Dorozhkina, A. (2015, March). Russia–Belarus single information space. *RussiaIC*. Retrieved from http://www.russia-ic.com/news/show/21017/#.V6qFwI7bDO6

Drezner, D. W. (2010, Spring/Summer). Weighing the scales: The Internet's effect on state-society relations. *Brown Journal of World Affairs*, *16*(2), 31–44.

Elder, M. (2012, February 7). Polishing Putin: Hacked emails suggest dirty tricks by Russian youth group. *The Guardian*. Retrieved from https://www.theguardian.com/world/2012/feb/07/putin-hacked-emails-russian-nashi

European Parliament Members' Research Service. (2015, January). *At a glance: Regional organisations in the post-Soviet space.* Retrieved from http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/545718/EPRS_ATA%282015%29545718_REV1_EN.pdf

Farivar, C. (2015, May). What could go wrong?—Russia, China are totally BFFs when it comes to Internet security. *Ars Technica*. Retrieved from http://arstechnica.com/tech-policy/2015/05/russia-china-are-totally-bffs-when-it-comes-to-internet-security/

Farnsworth, T. (2011, November 2). China and Russia submit cyber proposal. *Arms Control Today*. Retrieved from https://www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal

Fedor, J., & Fredheim, R. (2017). We need more clips about Putin, and lots of them: Russia's state-commissioned online visual culture. *Nationalities Papers*, *45*(2), 161–181.

Freedom on the Net: Annual reports. (2012). Retrieved from https://freedomhouse.org/report-types/freedom-net

Fukuyama, F. (1989, Summer). The end of history? *The National Interest*, *16,* 3–18.

Georgia finalizes withdrawal from CIS. (2009, August). *RadioFreeEurope—RadioLiberty*. Retrieved from https://www.rferl.org/a/Georgia_Finalizes_Withdrawal_From_CIS/1802284.html

Glasius, M., & Michaelsen, M. (2018). Illiberal and authoritarian practices in the digital sphere. (This Special Section).

Grisby, A. (2015, January). Net politics: Will China and Russia's updated code of conduct get more traction in a post-Snowden era? *Council on Foreign Relations—Net Politics*. Retrieved from http://blogs.cfr.org/cyber/2015/01/28/will-china-and-russias-updated-code-of-conduct-get-more-traction-in-a-post-snowden-era/

Hall, S., & Ambrosio, T. (2017). Authoritarian learning: A conceptual overview. *East European Politics*, *33*(2), 143–161.

Heydemann, S. (2007, October). Upgrading authoritarianism in the Arab world. *The Brookings Institution*. Retrieved from http://www.brookings.edu/research/papers/2007/10/arabworld

Horowitz, M. (2010). *The diffusion of military power: Causes and consequences for international politics*. Princeton, NJ: Princeton University Press.

Human Rights in Ukraine—2006. V. Right to privacy. (2007). *Human Rights in Ukraine*. Retrieved from http://www.khpg.org/index.php?id=1186147137

Huntington, S. P. (1991). Democracy's third wave. *Journal of Democracy*, *2*(2), 12–34.

Ivzhenko, T. (2009, July). Yushchenko will protect Ukraine from Russian media. *The Current Digest of the Post-Soviet Press*, *61*(27). Retrieved from http://www.eastviewpress.com/Files/FROM%20THE%20CURRENT%20ISSUE_No.27.pdf

Karl, T. L. (1995). The hybrid regimes of Central America. *Journal of Democracy*, *6*(3), 72–86.

Kerr, J. (2016). *Authoritarian management of (cyber-) society: Internet regulation and the new political protest movements*. (PhD dissertation.) Georgetown University, Washington, DC.

Kilner, J. (2012, July). Uzbekistan withdraws from Russia-lead military alliance. *The Telegraph*. Retrieved from https://www.telegraph.co.uk/news/worldnews/asia/uzbekistan/9369392/Uzbekistan-withdraws-from-Russia-lead-military-alliance.html

King, G., Pan, J., & Roberts, M. (2013, May). How censorship in China allows government criticism but silences collective expression. *American Political Science Review*, *107*(2), 1–18.

Koesel, K. J., & Bunce, V. J., (2013, September). Diffusion-proofing: Russian and Chinese responses to waves of popular mobilizations against authoritarian rulers. *Perspectives on Politics*, *11*(3), 753–768.

Kucera, J. (2010, December). CSTO fires salvo in information war. *EurasiaNet.org*. Retrieved from http://www.eurasianet.org/node/62639

Kucera, J. (2011, August). With eye to Arab Spring, CSTO strengthens cyber, military powers. *EurasiaNet.org*. Retrieved from http://www.eurasianet.org/node/64045

Levitsky, S., & Way, L. (2010). *Competitive authoritarianism: Hybrid regimes after the Cold War*. New York, NY: Cambridge University Press.

Lillis, J. (2011, December). Kazakhstan: Violence in Zhanaozen threatens Nazarbayev legacy. *EurasiaNet.org*. Retrieved from http://www.eurasianet.org/node/64745

McKune, S. (2015, September). An analysis of international code of conduct for information security. *Citizen Lab.* Retrieved from https://citizenlab.org/2015/09/international-code-of-conduct/

McKune, S., & Ahmed, S. (2018). Contestation and shaping of cybernorms through China's Internet sovereignty agenda (this Special Section).

Michel, C. (2015, September). The Eurasian Economic Union's 'single information field.' *The Diplomat*. Retrieved from http://thediplomat.com/2015/09/the-eurasian-economic-unions-single-information-field/

Moldova says it would leave CIS only after becoming EU candidate. (2018, January). *RadioFree Europe—RadioLiberty*. Retrieved from https://www.rferl.org/a/moldova-eu-candidate-cis-leanca/28998630.html

Omanovic, E. (2014, November). Private interests: Monitoring Central Asia. *Privacy International*. Retrieved from https://www.rivacyinternational.org/sites/default/files/2017-12/Private%20Interests%20with%20annex_0.pdf

Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan. (2015, January). *Developments in the field of information and telecommunications in the context of international security: Letter dated January 9, 2015, to the United Nations addressed to the secretary-general* (UN A/69/723). Retrieved from https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf

Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan. (2011, September). *Developments in the field of information and telecommunications in the context of international security: Letter dated September 12, 2011, to the United Nations addressed to the secretary-general* (UN A/66/359). Retrieved from https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf

President of Ukraine. (2009, July 8). *Decree of the president of Ukraine N514/2009: On the doctrine of information security of Ukraine.* Retrieved from http://zakon1.rada.gov.ua/laws/show/514/2009

President signed a decree on the final termination of Ukraine's participation in the statutory bodies of the CIS. (2018, May). *President of Ukraine Petro Poroshenko: Official Website*. Retrieved from http://www.president.gov.ua/en/news/prezident-pidpisav-ukaz-pro-ostatochne-pripinennya-uchasti-u-47554

Privacy International. (2014, November). Privacy International releases 'Private interests: Monitoring Central Asia.' *Privacy International*. Retrieved from https://privacyinternational.org/blog/1612/privacy-international-releases-private-interests-monitoring-central-asia

Ragan, S. (2012, February). Political activism gives way to hacktivism in Russia. *SecurityWeek.Com*. Retrieved from http://www.securityweek.com/political-activism-gives-way-hacktivism-russia

Razumovskaya, O. (2015, May 8). Russia and China pledge not to hack each other. *The Wall Street Journal*. Retrieved from http://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/

Republic of Belarus. (2001). *The national security concept of the Republic of Belarus.* Retrieved from http://www.mfa.gov.by/docs/en/bf_2006/04.National%20security.pdf

Rohozinski, R., & Haralampieva, V. (2007). Internet filtering in the commonwealth of independent states 2006–2007. *OpenNet Initiative.* Retrieved from https://opennet.net/studies/cis2007

Rõigas, H. (2015). An updated draft of the code of conduct distributed in the United Nations—What's new? *NATO CCDCOE International Cyber Developments Review*. Retrieved from https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html

Roth, A. (2015, May 8). Russia and China sign cooperation pacts. *The New York Times*. Retrieved from http://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html

Russia media boss talks journalism, gays and Eurasia in Kyrgyzstan. (2015, September). *EurasiaNet.org*. Retrieved from https://eurasianet.org/s/russia-media-boss-talks-journalism-gays-and-eurasia-in-kyrgyzstan

Schedler, A. (2002). The menu of manipulation. *Journal of Democracy*, *13*(2), 36–50.

Schedler, A. (2010, January). Authoritarianism's last line of defense. *Journal of Democracy*, *21*(1), 69–80.

SCO responds to cyber challenges. (2011, September). *InfoSCO*. Retrieved from infoshos.ru/en/?idn=8349

Shackelford, S., Oti, E., Kerr, J., Korzak, E., & Kuehn, A. (2015, June). Spotlight on cyber V: Back to the future of Internet governance? *Georgetown Journal of International Affairs*. Retrieved from

https://www.georgetownjournalofinternationalaffairs.org/online-edition/back-to-the-future-of-internet-governance

Shirky, C. (2011, February). The political power of social media: Technology, the public sphere, and political change. *Foreign Affairs*, *90*(1), 28–41.

Simmons, B., & Elkins, Z. (2005). On waves, clusters and diffusion: A conceptual framework. *Annals of the American Academy of Political and Social Science*, *598*, 33–51.

Soldatov, A., & Borogan, I. (2012, December). In ex-Soviet states, Russian spy tech still watches you. *WIRED*. Retrieved from https://www.wired.com/2012/12/russias-hand/

Soldatov, A., & Borogan, I. (2013, Fall). Russia's surveillance state. *World Policy Journal*, *30*(3). Retrieved from http://www.worldpolicy.org/journal/fall2013/Russia-surveillance

Soldatov, A., & Borogan, I. (2015). *The red Web: The struggle between Russia's digital dictators and the new online revolutionaries*. New York, NY: Public Affairs.

Subbotovska, I. (2015, May). Russia's online trolling campaign is now in overdrive. *Business Insider*. Retrieved from http://www.businessinsider.com/russias-online-trolling-campaign-is-now-in-overdrive-2015-5

Way, L. (2015). The limits of autocracy promotion: The case of Russia in the 'near abroad.' *European Journal of Political Research*, *54*, 691-706.

Zakaria, F. (1997, November–December). The rise of illiberal democracy. *Foreign Affairs,* 22–43. Retrieved from https://www.foreignaffairs.com/articles/1997-11-01/rise-illiberal-democracy