

REPORT DOCUMENTATION PAGE					<i>Form Approved</i> OMB No. 0704-0188	
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.						
1. REPORT DATE (DD-MM-YYYY) 01-05-2020		2. REPORT TYPE Master of Military Studies (MMS) thesis			3. DATES COVERED (From - To) AY 2019-2020	
4. TITLE AND SUBTITLE Surveillance technologies and digital authoritarianism: Examining the global impact of surveillance technology proliferation and how democracies can fight back				5a. CONTRACT NUMBER N/A		
				5b. GRANT NUMBER N/A		
				5c. PROGRAM ELEMENT NUMBER N/A		
6. AUTHOR(S) Murray, Tristan J. (Major)				5d. PROJECT NUMBER N/A		
				5e. TASK NUMBER N/A		
				5f. WORK UNIT NUMBER N/A		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) USMC Command and Staff College Marine Corps University 2076 South Street Quantico, VA 22134-5068					8. PERFORMING ORGANIZATION REPORT NUMBER N/A	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A					10. SPONSOR/MONITOR'S ACRONYM(S)	
					11. SPONSOR/MONITOR'S REPORT NUMBER(S) N/A	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited.						
13. SUPPLEMENTARY NOTES						
14. ABSTRACT Authoritarian governments that have embraced and adapted to the evolving digital domain have given rise to a new phenomenon called digital authoritarianism. This paper provides an overview of what motivates traditionally authoritarian governments to become digital authoritarians and most importantly, it discusses the negative effects of digital surveillance technologies when used as a tool for suppression. In addition, this paper addresses the challenges for democracies to adopt stronger export control measures to stem the spread of these surveillance technologies. Using the case study method, this paper presents an analysis of the impact of surveillance technologies in two import authoritarian regimes. The results indicate that in a world where digital interconnectedness would suggest otherwise, digital authoritarians have developed new deterrents to social and political change through the integration of online surveillance into their broader strategies of repression. These results illustrate how the proliferation of these technologies are entrenching digital authoritarianism across the world. Finally, proposed changes to the current global export governance are discussed, revealing what role democracies must assume to reverse the trend of declining privacy and expression freedoms globally.						
15. SUBJECT TERMS digital authoritarianism, government surveillance, ICT surveillance, mobilization, repression, export controls, human rights, policy review, privacy freedoms, democracy						
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 39	19a. NAME OF RESPONSIBLE PERSON USMC Command and Staff College	
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include area code) (703) 784-3330 (Admin Office)	
Unclass	Unclass	Unclass				

*United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068*

MASTER OF MILITARY STUDIES

**SURVEILLANCE TECHNOLOGIES AND DIGITAL AUTHORITARIANISM:
EXAMINING THE GLOBAL IMPACT OF SURVEILLANCE TECHNOLOGY
PROLIFERATION AND HOW DEMOCRACIES CAN FIGHT BACK**

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

**MAJOR TRISTAN J. MURRAY
UNITED STATES MARINE CORPS**

AY 2019-20

Mentor and Oral Defense Committee Member: Dr. Craig Hayden

Approved: //SIGNED//

Date: 1 May 2020

Oral Defense Committee Member: Dr. Claire Metleis

Approved: //SIGNED//

Date: 1 May 2020

Executive Summary

Title: Surveillance technologies and digital authoritarianism: Examining the global impact of surveillance technology proliferation and how democracies can fight back

Author: Major Tristan J. Murray, United States Marine Corps

Thesis: In the absence of a strong international response by the Western democracies, surveillance technology proliferation to oppressive regimes will continue to advance digital authoritarianism globally.

Discussion: Authoritarian governments that have embraced and adapted to the evolving digital domain have given rise to a new phenomenon called digital authoritarianism. This paper provides an overview of what motivates traditionally authoritarian governments to become digital authoritarians and most importantly, it discusses the negative effects of digital surveillance technologies when used as a tool for suppression. In addition, this paper addresses the challenges for democracies to adopt stronger export control measures to stem the spread of these surveillance technologies. Using the case study method, this paper presents an analysis of the impact of surveillance technologies in two import authoritarian regimes. The results indicate that in a world where digital interconnectedness would suggest otherwise, digital authoritarians have developed new deterrents to social and political change through the integration of online surveillance into their broader strategies of repression. These results illustrate how the proliferation of these technologies are entrenching digital authoritarianism across the world. Finally, proposed changes to the current global export governance are discussed, revealing what role democracies must assume to reverse the trend of declining privacy and expression freedoms globally.

Conclusion: Existing approaches to stop the globalization of surveillance technologies to repressive regimes are not reinforced with direct challenges to foreign governments that undermine democracy. Only a united front among the world's democratic nations can seriously oppose the advance of digital authoritarianism.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Illustrations

	Page
Figure 1. Concentric Circles of Influence.....	14

Tables

	Page
Table 1. Democracy Index 2019, by regime type.....	6

Table of Contents

	Page
DISCLAIMER	i
LIST OF ILLUSTRATIONS AND TABLES	ii
PREFACE	iv
INTRODUCTION	1
Digital authoritarianism's toll	3
From liberation to control	4
DISCUSSION	7
Authoritarians go digital	7
Surveillance meets the internet	9
Competing ideologies on digital surveillance	12
CASE STUDIES	16
Uganda	16
Kyrgyzstan	19
GLOBAL RESPONSE	20
Wassenaar Arrangement	21
Freedom Online Coalition	22
Other global initiatives	23
Proposed international governance	24
DISCUSSION	27
IMPLICATIONS	27
CONCLUSION	29
BIBLIOGRAPHY	36

Preface

The basis for this research originally stemmed from my curiosity about the role of government surveillance in contentious politics. More specifically, I wanted to better understand where the line between “democratic” surveillance ended and “repressive” surveillance began. We are now beginning to observe the negative consequences of surveillance in the hands of governments that wield it as an impressive tool for population control. As we progress further into the digital age, the notion that privacy is a fundamental right is beginning to fade away. How can democracies ensure that this right is not just retained for a precious few who have the luxury of being born free, but for every citizen in the world? This is the question that drives my research and compels me to uncover ways that can give people back opportunities to enact change.

I would like to thank Dr. Craig Hayden for his immeasurable patience and guidance throughout this process. His ability to challenge my assertions and offer me valuable feedback made me a better writer and stronger critical thinker. I am grateful to have him as my mentor. I also want to thank Dr. Claire Metelis for her support, encouragement and endless knowledge. She motivated me to keep going when I did not want to. I am fortunate to have her as a role model. Finally, this paper would not have been possible without the support of my family. My husband, Dr. Robert Murray, and our children, Emma, Bruce, Elias, and Madeline all offered me the love and inspiration I needed to see this through. In truth, I could not have achieved this level of success without my husband’s patient advice, endless proofreading without complaint, and tolerance of my long days glued to a computer. It is because of him that I am a better Marine officer, wife, and mother. Thank you, my love, for being my person.

Introduction

“In the old days at least, you had somewhere you could hide, or where you can do your private things. But now the assumption is people know where you are.”

Feng Xiang, Chinese legal scholar¹

In October 2013, Vince Cerf, widely recognized as the “Father of the Internet,” stated rather provocatively that “privacy may actually be an anomaly.”² Although his comments were unsettling for democracies, authoritarian governments like China and Russia were already hard at work tightening their grip on power through the development and abuse of information and communications technologies. Autocratic governments that embrace and adapt to the evolving digital domain have given rise to a new phenomenon called digital authoritarianism.³ Digital authoritarianism is defined as a regime of governance that undermines democratic processes and violates human rights through a multi-faceted state repression strategy, which leverages surveillance, propaganda, disinformation, manipulation, and censorship across the cyberspace domain.⁴

In light of this emerging phenomenon, there has been a growing international concern over the globalization of surveillance technologies that are increasingly finding their way into the hands of oppressive governments.⁵ As a result of this largely unchecked proliferation, export controls have become the topic of contested debate between democratic governments and private industry as stakeholders struggle to find agreeable solutions aimed at limiting authoritarian states’ abuse of surveillance technologies.⁶ In her testimony before the Senate Judiciary Subcommittee on Crime and Terrorism on 5 November 2019, Kara Frederick, a Fellow at the Center for a New American Security, affirmed that, “If democratic societies do not establish the rules of the road for data security and privacy protections, authoritarians will do it for us.”⁷

Digital tools for repression have the unique ability to extend a government's reach that was not possible before.⁸ Surveillance technologies, specifically, provide oppressive governments the means of access to make the other facets of digital authoritarianism more effective.⁹ Without surveillance, governments are unable to determine what content to censor and issues that could potentially threaten political survival remain hidden, unable to be redirected or manipulated. What has centrally changed is the broadening availability of these digital surveillance technologies to less sophisticated authoritarian regimes that now appears to be tipping the scales in favor of an illiberal world order.¹⁰ While all of the elements of digital authoritarianism are worthy of our attention, this paper explores the particular ways surveillance technologies are being used to globally advance digital authoritarianism and how democracies are responding to this rising trend.

To address these subjects, this paper begins by uncovering the social cost of advancing digital authoritarianism to show the negative relationship between suppression technologies and political and social change. It then explores how some traditionally authoritarian governments exploit the internet to evolve their form of governance into what is recognized today as digital authoritarianism. Next, it sheds light on the impact of digital surveillance technologies when used as a tool for suppression to explain how it undermines democratic values by discouraging and intimidating citizens' political participation. It then considers the consequences of proliferated digital surveillance technologies to less sophisticated authoritarian governments through country case studies that illustrate how these technologies enable the effective suppression of political dissent and entrench digital authoritarian governance. Finally, this paper focuses on how democracies are responding to the expanding digital authoritarian phenomenon

through export control measures and explores what more can be done to limit the proliferation of surveillance technologies to curtail the rise of digital authoritarianism worldwide.

Digital authoritarianism's toll

During an interview in December 2019, Natalia Antelava, co-founder and co-editor of Coda Story, an online news organization that investigated the impact of technology on society, reflected on the nature of the information revolution on authoritarian governments: “soon the digital will become ‘just life’...digital authoritarianism at some point is just going to be authoritarianism and it’s going to be *different* from the authoritarians we’ve known before.”¹¹ An expanding scholarly body of literature is already making the connection between authoritarian control over the internet and the decline of citizens’ fundamental freedoms.¹² The issues at stake in the rise of digital authoritarianism are multidisciplinary in nature, as evidenced by the attention they receive from scholars of political science, sociology, surveillance, and information technology. These fields recognize, for example, that less sophisticated authoritarians are not only acquiring technologies for surveillance from far more advanced authoritarians like China and Russia, but they are also imitating their strategies for repression.¹³ As Anne-Marie Slaughter observes, “dictators are creating and sharing tools for greater population control than ever before.”¹⁴

Scholars have observed the intimidation of political discourse and the suppression of mobilization as harmful effects of online surveillance.¹⁵ Marlies Glasius and Marcus Michaelsen, research Fellows on the Authoritarianism in a Global Age Project, make clear that, “no other practice has been as pervasive in the digital sphere as arbitrary surveillance.”¹⁶ Extensive, opaque internet monitoring has distinct consequences for the ability of the citizenry to participate in politics, through protests, peaceful assembly and mobilization—all cornerstones of a

functioning democracy. Current research suggests that the abuse of surveillance technologies may have a greater role in increasing the cost of mobilization over other digitally repressive tools, like censorship, and warrants further investigation into the extent of this impact.¹⁷ In short, digital authoritarianism shuts off routes to social and political change that are crucial to a thriving democracy.

Digital authoritarianism and surveillance are not only a concern for scholarship. Digital authoritarian methods play a role in enabling the revisionist ambitions of rising great powers. Therefore, policymakers and advocacy experts need a clear-eyed view of the consequences of surveillance technologies exports, and what role democracies must assume to confront the rise of digital authoritarianism. Authoritarian governments have fundamentally altered their boundaries of power and have evolved into the authoritarians we recognize now through tools of digital suppression.

From liberation to control

In the absence of the internet, oppressive regimes had the ability to effectively control domestic populations by isolating their citizens from one another and the outside world. The opening of the digital age was optimistically viewed by social scientists, human rights advocates, and foreign policy makers as the medium that would liberate society.¹⁸ In January of 2010, then Secretary of State Hilary Clinton, gave a speech on “Internet Freedom,” during which she discussed America’s vision of an open and free global internet that would serve as the bedrock for democracy in the twenty-first century.¹⁹ She said:

The freedom to connect is like the freedom of assembly, only in cyberspace. It allows individuals to get online, come together, and hopefully cooperate. Once you’re on the internet, you don’t need to be a tycoon or a rock star to have a huge impact on society.²⁰

Secretary Clinton was not wrong. The coordinated mobilization of individuals witnessed in the Arab Spring demonstrated that information and communication technologies made possible by the internet could now play a significant role in enabling political change among oppressed publics. However, Secretary Clinton also warned that authoritarian governments inherently feared for their political survival and, if given the opportunity, would exploit the internet to surveil and target their opposition.²¹ For example, Chinese citizens are familiar with the Chinese Communist's Party's (CCP) extensive digital repression tools in their daily lives. These tools include, but are not limited to: state-wide censorship via "The Great Firewall of China," ubiquitous online surveillance, mandatory citizen ID numbers for the purpose of eliminating online anonymity, and an expanding artificial intelligence program, all designed to enhance and reinforce China's domestic stability and authority.²² The CCP's technological innovations and ingenuity demonstrates its commitment to establish jurisdiction over the digital domain that the Western world had not thought was possible. President Bill Clinton's quip in a speech delivered in March 2000 was a misplaced prediction that the Chinese party's control over the internet would be akin to "trying to nail jello to the wall."²³ These extensive digital control measures over China's roughly 1.4 billion people have made the CCP the most sophisticated digital authoritarian regime in the world, dispelling any present notion that the internet would be its undoing.

Even though the internet fundamentally altered the landscape of contentious politics, it did not usher in widespread democratization as some would have hoped.²⁴ For instance, the Arab Spring began with enthusiasm for democracy, but after eight years only one country—Tunisia—actualized that goal.²⁵ While the future remains uncertain, the current trend in governance appears to be leaning toward autocracies. In part due to the rise of authoritarianism

around the world, The Economist’s *Democracy Index Report for 2019* (Table 1) goes so far as to declare a global “democracy recession.”²⁶ In the report, the authors cite “a decline in civil liberties, including media freedom and freedom of speech” as a contributing factor.²⁷ In addition, Freedom House’s 2019 annual report on *Freedom on the Net*, announced that global internet freedom declined for the ninth consecutive year.²⁸ These results further identified how the increasing acquisition of surveillance technologies facilitated governments in the arrest of citizens whose political, social, and religious speech was deemed counter to the states’ views.²⁹

Table 1: Democracy Index 2019, by regime type

	No. of countries	% of countries	% of world population
Full democracies	22	13.2	5.7
Flawed democracies	54	32.3	42.7
Hybrid regimes	37	22.2	16.0
Authoritarian regimes	54	32.3	35.6

Note. “World” population refers to the total population of the 167 countries covered by the index. Since this excludes only micro states, this is nearly equal to the entire estimated world population.

Source: The Economist Intelligence Unit.

Source: Economist Intelligence Unit, *Global Democracy in Retreat*, (New York, NY: The Economist, January 21, 2020), <https://www.eiu.com/n/global-democracy-in-retreat/>.

Across the world, the way people communicate has been transformed in ways that open up opportunities for digital surveillance and suppression. Online applications like WhatsApp dominate everyday discourse between individuals and groups. Both reports reveal that the privacy and expression freedoms that are being exercised online are being restricted in parallel with the decline of democracies across the world; demonstrating the inextricable connection between the two. Although the internet offers the ability to organize online and mobilize for political change, authoritarian regimes—as Secretary Clinton forewarned—are proving remarkably adept at harnessing the digital environment to root out perceived threats to their political survival.

Authoritarians go digital

Many theories have been proposed to explain what authoritarianism is, or is not.³⁰ Vast nuances in authoritarian governance exist because the variables that impact a regime's behavior are influenced by a country's historical context, its culture and its leaders' personalities among many others.³¹ Although the literature covers a wide variety of authoritarian definitions, this paper will primarily focus on a broad definition of authoritarianism to enable the identification of governments that would most likely misuse information and communication technologies as they seek to become modernized. What then makes a government authoritarian and how is this definition different from the emerging phenomenon of digital authoritarianism?

Political scientists agree that, at a minimum, authoritarian governments are defined by the absence of free and fair competitive elections.³² In addition, in their landmark publication, *The Internet and Political Protest in Autocracies*, Nils Weidmann and Espen Rod consider a regime autocratic “[if the government came to power] through a competitive election but changed the rules while in office to prevent future elections from being competitive.”³³ This inclusion emphasizes Glasius' challenge to the traditional scholarly acceptance of authoritarianism. She argues, “We should be able to judge the ‘authoritarianness’ of governments not solely by how they [come] to power, or by the supposed personality traits of the electorate, but also by what they do once they are in power.”³⁴ What Weidmann and Rod argue, as does much of the literature on authoritarianism, is that no two autocracies are alike.³⁵ This paper uses the 1) absence of free and fair elections and 2) changing the rules to prevent future elections to be competitive, as a broad definition of what is authoritarian.

Understanding regime objectives can similarly be useful to help identify a state as authoritarian in the present context. Notable political scientists, Natasha Ezrow and Erica Franz'

analysis of authoritarian governments examines the state's primary drivers for action.³⁶ They assert that, "[t]he main goals of authoritarian regimes are political demobilization and depoliticization. Authoritarian regimes do not seek to homogenize society, and instead allow for some degree of pluralism."³⁷ For example, when focused on demobilizing motivations, researchers investigating China's extensive online censorship strategy discovered that language that foments mobilization is much more likely to be removed over one-way criticism of the party.³⁸ The American political sociologist, Larry Diamond, and Harvard Fellow and Fullbright scholar, Rebecca MacKinnon, explain that some autocracies permit limited pluralism because they recognize the necessity of possessing some forms of "pseudodemocratic" processes that offer their citizens a sense of political participation that may serve as a release valve to deter any significant challenges to the regime.³⁹ An authoritarian government that holds an election, like Vietnam, is an illustration of a pseudodemocratic process in that candidates are strictly vetted by the government, thus signaling the absence of "free and fair," but at the same time projecting the façade of "choice."⁴⁰ Knowing the specific aims of authoritarian regimes reveals their digital agenda in the face of information and communication diffusion via the internet.

Internet access broadened the tools available to authoritarian regimes to demobilize and depoliticize on a mass scale.⁴¹ For instance, Russia revived and upgraded its Soviet-era surveillance System of Operative Search Measures (SORM), originally developed to monitor telephone conversations. SORM has been expanded to monitor citizens' emails and browsing data.⁴² Russia uses this technology to target political opposition with the demonstrated intent to intimidate, harass, and jail its citizens, all of which is designed to shut down their participation in the political process.⁴³ This new level of invasiveness into private communication among citizens signals the elimination of an individual private sphere under authoritarian rule.

However, there is a key distinction that makes digital authoritarianism stand apart from its traditional academic interpretation. The difference between traditional and digital authoritarian governance, according to McKinnon, can be understood as:

In the networked authoritarian state, the single ruling party remains in control while a wide range of conversations about the country's problems nonetheless occurs on websites and social-networking services. The government follows this online chatter, and sometimes people are able to use the Internet to call attention to government policies. As a result, the average person with Internet or mobile access has a much greater sense of freedom—and may feel that he has the ability to speak and be heard—in ways that were not possible under classic authoritarianism.⁴⁴

In other words, people who live under contemporary authoritarian rule are routinely subjected to the arbitrary surveillance, censorship, disinformation and propaganda that their government engages in online. Yet, the presence of internet access, however limited, offers these people a sense of relative freedom that can only be experienced digitally. By this logic, digital authoritarian governments make calculations on how much, or how little, they will respond to public discourse; balancing repression and appeasement online to maintain their hold on legitimacy.⁴⁵ Inherent in digital authoritarianism's survivability is the capability to, in MacKinnon's words, "follow this online chatter."⁴⁶ Expansive online state surveillance introduces the means to do just that.

Surveillance meets the internet

In 2020, it is difficult to imagine the modern world without the omnipresence of surveillance that has penetrated and situated itself into the routine workings of our everyday lives.⁴⁷ As our reliance on technology grows for communication and information sharing, it makes sense that the internet has become the medium in which surveillance evolves.⁴⁸ Online state surveillance plays a vital role in daily governance to protect citizens through domestic policing, support of national security, and is relied upon for administration that enables governments to function more effectively.⁴⁹ For example, the Center for Disease Control uses public health surveillance

as a means to prevent and track diseases and monitor the environment to keep Americans safe.⁵⁰ Democracies and authoritarians alike adopt digital surveillance practices for benign government purposes; however, where and when does this relationship depart and become something more sinister?

The sheer scope of the collection and aggregation of online information, now understood as metadata surveillance, has placed the value of privacy at an all-time high.⁵¹ In the last three decades scholars, lawyers, and policymakers have debated the moral, ethical, and lawful application of surveillance technologies.⁵² Democracies are not immune to this criticism. The Snowden controversy in 2013 put America's domestic internet surveillance practices centerstage as a form of unacceptable governmental overreach and an erosion of public trust that to this day possesses lingering effects.⁵³ For example, one of the largest technology companies in the world, Apple, changed the design of its products to ensure that not even their employees could have access to user data in response to Snowden's disclosures.⁵⁴ This was a significant step towards strengthening data security and a direct challenge to weak democratic surveillance oversight.⁵⁵ At the core of all democracies is a requirement for government accountability and transparency. States' abuse of online surveillance is detrimental to both. Anita Gohdes, an International and Cyber Security professor at the Hertie School of Governance, explaining why internet surveillance is so appealing to authoritarian governments, maintains that, "Digital surveillance of entire populations, in particular of those identified as potential threats, is a highly rational policy option for governments [that] fear for their political survival."⁵⁶ For this reason, digital surveillance is a compelling tool for control because populations are so accustomed to it, and in many cases welcome the conveniences it provides.

Digital authoritarian governments exploit surveillance technologies to target political dissidents with the intent to harass, harm, imprison, and even murder.⁵⁷ The assassination of journalist and known political activist Jamal Khashoggi garnered international attention in 2018 when the extent of Saudi Arabia's digital surveillance practices was revealed as the method used to track him.⁵⁸ When total surveillance, supported by digital technology, is integrated into broader state repression strategies it suffocates any viable opposition to a digital authoritarian regime.⁵⁹ Elizabeth Stoycheff's Wayne State University research group observes, "While censorship systematically blocks collective action opportunities, surveillance intimidates them."⁶⁰ Surveillance scholars call this intimidation the "chilling effect," whereby continuous government observation can lead citizens to self-censor out of fear of coercion or prosecution for expressing personal beliefs or new ideas that are viewed as discordant with the ruling party.⁶¹ Moreover, other surveillance research has similarly demonstrated that citizens' political and more sensitive conversations begin to decline as a result of state monitoring.⁶² These studies show that merely the perception of online surveillance curbs political participation, offering authoritarian governments that desire these new technologies a lucrative means to discourage, and even silence the opposition.

If chilling effects are the result of passive surveillance measures, then Yale legal scholar, Jack Balkin, calls attention to the increasingly dangerous effects of technological advances.⁶³ He states, "Government's most important technique of control is no longer watching or threatening to watch. It is analyzing and drawing connections between data."⁶⁴ Today's technologies are capable of monitoring, collecting, and aggregating on a scale that was practically incomprehensible a decade ago, generating detailed records of citizens' lives.⁶⁵

Director of the Surveillance Studies Centre at Queen's University, David Lyon, and prominent sociologist, Zygmunt Bauman, call this emergent phenomenon “liquid surveillance.”⁶⁶ That is, even when surveillance may “chill” specific behaviors, metadata surveillance technologies are able to collect and collate to discern a person's preferences, attitudes, and beliefs entirely from his/her digital footprint.⁶⁷

China's experimental social credit system serves as an example of this technology's implementation. A citizen's “social credit score” is created by data collected from their social media accounts, online browsing preferences, and their social network's online browsing habits—among other surveilled behaviors—to determine their “trustworthiness” from the perspective of the CCP.⁶⁸ Individuals who demonstrate poor citizenry receive lower trustworthiness scores that can lead to exclusion from travel, job opportunities, and even from the pursuance of higher education.⁶⁹ Digital authoritarian governments design these surveillance tools to serve their primary objective of regime survival. Based on the research it is clear that these technologies make surveillance an effective means of control that displays little signs of weakening.

Competing ideologies on digital surveillance

Surveillance technologies' maturation and increasing ubiquity has driven the cost of state surveillance down, making a once out-of-reach option for less sophisticated countries now widely accessible.⁷⁰ In light of this broadening access, in December 2013 the United Nations General Assembly adopted Resolution 68/167, the right to privacy in the digital age.⁷¹ This resolution formally recognized the negative impacts of unlawful and arbitrary online surveillance practices on a country's citizens by affirming that “the rights held by people offline must also be protected online.”⁷² In continued defiance of this resolution, 15 additional countries in 2019

adopted laws or directives to increase surveillance or prohibit the online anonymity of their citizens.⁷³ For example, in January 2019 the government of Vietnam adopted strict cybersecurity laws that criminalized propaganda against the ruling party—the Communist Party of Vietnam—and granted the government significant access to its citizens’ information and communications platforms for the purpose of surveilling and censoring content and data.⁷⁴ As governments continue to assert that they should have sovereign control over their internet content, the digital authoritarian model is an attractive and validated set of practices worth considering. Justin Sherman, a non-resident Fellow at the Atlantic Council’s Cyber Statecraft Initiative, details China’s level of influence on Vietnam:

China’s global influence on internet governance remains strong, and it continues to grow through foreign investments, political pressure, diplomatic engagement in international forums, technology trainings and exports, the leveraging of China’s economic power, and other mechanisms. While not every country exerting tight internet control should be compared entirely to China—and while Vietnam in particular is resisting Chinese influence in many domains—Vietnam’s tightening internet regulation demonstrates just what could happen when a country has the capability and the will to begin to follow in China’s internet control footsteps.⁷⁵

In his published Open Technology Fund report, Senior Information Controls Fellow, Valentin Weber, discovered that “over 100 countries have purchased, imitated, or received training” on technologies that enable the control of internet content from China and Russia.⁷⁶ Figure 1 summarizes Weber’s findings and shows China’s growing span of influence through the diffusion of information controls compared to Russia.⁷⁷

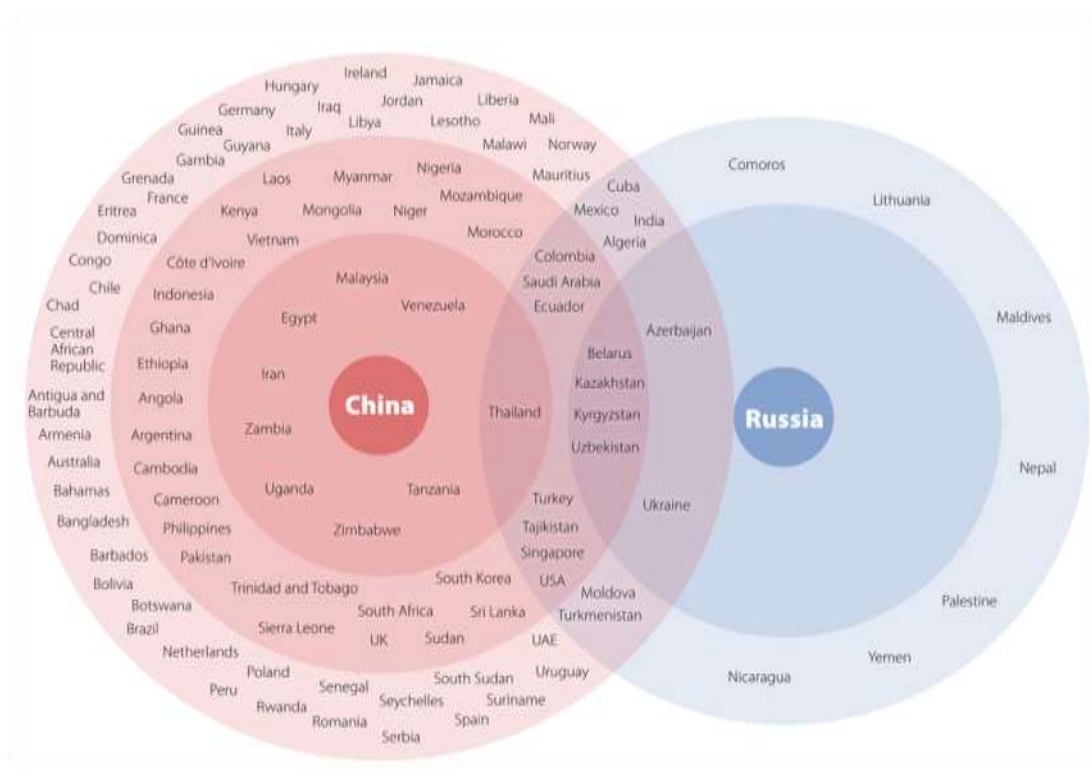


Figure 1: Concentric Circles of Influence. The inner circle represents the core, and the outer circles the periphery of respective technospheres.

Source: Valentin Weber, “*The worldwide web of Chinese and Russian information controls*,” (Washington, DC: Open Technology Fund, September 2019), <https://www.opentech.fund/news/examining-expanding-web-chinese-and-russian-information-controls/>.

The abuse and proliferation of surveillance technologies for political purposes has gained the attention of the United Nations Office of the High Commissioner for Human Rights, calling into focus the increased targeting of journalists, political activists, and minorities who express criticism of their ruling parties in two separate reports published in 2014 and 2019.⁷⁸ This prompted United Nations Special Rapporteur, David Kaye, to remark, “It is insufficient to say that a comprehensive system for control and use of targeted surveillance technologies is broken. It hardly exists.”⁷⁹ To emphasize Kaye’s point, a September 2019 report published by the United States think tank Carnegie Endowment for International Peace revealed that China exported surveillance technologies to over 60 countries such as Myanmar, Venezuela, Uganda, Kenya, and others with long track records of human rights abuses.⁸⁰

While authoritarians are frequently vilified for exporting technologies to other like-minded governments, it is important to point out that democracies are also complicit in this practice. Western countries have developed and exported surveillance technologies to some of the most repressive regimes in the world.⁸¹ For instance, surveillance technologies developed by the American company Blue Coat were used in Syria to clamp down on dissidents opposing the Assad regime.⁸² Revelations such as these have drawn the ire of nongovernmental organizations (NGOs), human rights and privacy activists calling on democracies to do more to prevent the spread of these technologies.⁸³ In May 2011, President Obama articulated a vision for an International Strategy for Cyberspace:

We encourage people all over the world to use digital media to express opinions, share information, monitor elections, expose corruption, and organize social and political movements, and denounce those who harass, unfairly arrest, threaten, or commit violent acts against the people who use these technologies.⁸⁴

If democracies desire to counter growing digital authoritarian influence and strengthen international norms against the misuse of surveillance technologies, arguably they must first hold themselves accountable.

This accountability process begins with compelling companies to reevaluate their role in privacy considerations for their users. Internet surveillance is built into the revenue structure that drives the biggest internet companies in the world.⁸⁵ Companies, like Google LLC, make considerable profit collecting, collating and selling data.⁸⁶ Adopting more transparent and regulatory privacy practices will be important if democracies desire to have other countries subscribe to a democratic model of internet governance. Finally, accountability also entails prohibiting companies in all democratic countries from exporting surveillance technologies to governments that demonstrate the propensity to use them in bad faith. As Diamond asserts, “...the struggle for electronic access is really just the timeless struggle for freedom by new

means. It is not technology, but people, organizations, and governments that will determine who prevails.”⁸⁷

Case studies & global response

Case studies can be a powerful way to describe the digital authoritarian phenomenon. Through the consolidation of investigative journalism and NGO reports, the negative consequences of surveillance can now be observed in the hands of repressive governments that wield it as an impressive tool for population control. The two selected case studies are designed to show how surveillance technologies enable the effective suppression of political dissent, and perhaps more importantly, illuminate how surveillance technologies advance digital authoritarianism around the world. The final section examines how democracies presently respond to the digital authoritarian phenomenon as well as proposed global governance initiatives to counter this troubling trend. The purpose of this analysis is to show how it is possible to reverse the rise of digital authoritarianism.

Case Study 1: Uganda

Uganda has experienced significant levels of corruption since the country’s ruling party, the National Resistance Movement, came into power after a violent overthrow in 1986.⁸⁸ Uganda’s president, Yoweri Museveni, has served in his position for 34 years. Under his rule, Museveni has eliminated presidential term limits (2005) and removed presidential age requirements (2017), paving the way for him to secure the presidency for life.⁸⁹ Elections in Uganda are internationally recognized as neither free nor fair, with frequent reporting on the abuse of state resources, flawed electoral management, and violence and intimidation against voters and government opponents.⁹⁰ Digital authoritarian tools have enabled and sustained the Ugandan government’s controlling practices. In 2015, Privacy International uncovered the National

Resistance Movement's use of a surveillance technology called FinFisher to infiltrate protesters and opposing party leaders' information and communications platforms.⁹¹ FinFisher was developed by the German-UK company known as Gamma Group that exported and subsequently provided training to Ugandan officials on the technology's capabilities.⁹² According to the report, once the software is introduced on a person's personal device (e.g., cell phone, laptop, etc.), all of the content can be viewed in real time, including access to files, passwords, microphones and cameras without the knowledge of the owner.⁹³ To gain access to its targets, the National Resistance Movement bribed and recruited officials, business and hotel managers, and the people closest to them to install the hardware.⁹⁴ Museveni and his party used FinFisher to crack down on social movements and prominent opposition leaders that were protesting widespread corruption and the high cost of living standards after the 2011 election. Namely in response to peaceful protests across the country, "[o]ver 600 people were arrested and detained without charge. Some bore marks consistent with allegations of whipping and beatings. Members of Parliament were arrested, manhandled and placed under 24-hour surveillance and preventative detention."⁹⁵ These actions ultimately deterred any genuine opposition to Museveni's National Resistance Movement and as a result, support for the protests diminished and perceived viable opposition groups were declared illegal.⁹⁶

In 2014, The National Resistance Movement became the benefactor of Chinese surveillance under the auspices of China's Digital Silk Road initiative that serves as a subset of the Belt and Road Initiative to expand digital connectivity abroad.⁹⁷ Through this initiative, Museveni continued to abuse surveillance technologies to remain in power. The Chinese-owned telecommunications giant, Huawei, and the government of Uganda formally entered into a \$126 million-dollar contract for a state-of-the-art facial recognition surveillance system in 2019.⁹⁸

Although the National Resistance Movement has argued that such sophisticated surveillance measures were necessary to combat high rates of violent crime, a 2019 investigative report by the *Wall Street Journal* revealed that similar surveillance tactics used in 2011 still continued to be extensively practiced by the party.⁹⁹ Huawei technicians stationed inside Uganda in 2018 helped government officials surveil, track, and target political opponents and protesters.¹⁰⁰ The report found that the surveillance support included “intercepting their encrypted communications and social media, and using cell data to track their whereabouts.”¹⁰¹ Weakened privacy laws permitted Uganda’s cyber-crime unit to target and arrest a key oppositional leader, known as Booby Wine, and spoil plans for an anti-government protest. Ugandan security officials produced for reporters “screenshots of Mr. Wine’s WhatsApp chats with the Firebase crew where participants were exchanging details on the planned events.”¹⁰² Ugandan police gained real-time training and access to encrypted communications and location data of Ugandan citizens with the help of Huawei.

Despite the report becoming public, Uganda and China deny any wrongdoing.¹⁰³ Uganda’s multi-million-dollar relationship with China grants the ruling party unprecedented access to its population’s personal data and communications in ways that were impossible before now. While the government’s application of FinFisher suppressed free speech and intimidated the Ugandan peoples’ political participation, it required complicit actors to help facilitate the introduction of the malware. With Huawei’s surveillance technology and training, Museveni and his party can become more repressive, illustrating surveillance’s instrumental role in demobilizing Uganda’s citizens.

Case Study 2: Kyrgyzstan

Kyrgyzstan's government has been challenged by persistent instability since declaring its independence from the former Soviet Union in 1991.¹⁰⁴ Plagued by widespread corruption, the first two post-Soviet presidents were ousted from office after mass protests forced their removal. While Kyrgyzstan's elections are not internationally recognized as free and fair, dissenting views are able to materialize into a large-scale mobilization capable of forcing change.¹⁰⁵ The current president, Sooronbai Jeenbekov, ascended to power in 2017, propped up by the country's ruling party, the Social Democratic Party of Kyrgyzstan (SDPK). The SDPK has been accused of centralizing power through the mismanagement of state resources and voter harassment and intimidation to solidify President Atambaev's position.¹⁰⁶

Since 2012, Kyrgyzstan's government uses Russia's latest System of Operative Search Measures (SORM) technology as its method of state-wide surveillance.¹⁰⁷ According to the independent news organization, Eurasianet, "The [state] agencies with access to SORM technology are able to monitor and record all of Kyrgyzstan's Internet traffic and, according to CIIP [Civil Initiative on Internet Policy] research, all mobile and landline phone calls."¹⁰⁸ In the last decade the SDPK has taken several legislative steps that require all internet service providers (ISPs) and mobile services providers to install the latest version of SORM, providing the government the means to digitally surveil its citizens and target political opposition as a way to hold onto power.¹⁰⁹

Under the guise of public safety, Kyrgyzstan's citizens are subjected to indiscriminate and, in some cases, targeted surveillance. In 2016, Jeenbekov's predecessor, Almazbek Atambayev, was the leader of the SDPK when leaked telephone recordings brought down oppositional party leaders from the People's Parliament who were conspiring to overthrow

him.¹¹⁰ In the audio files published online, opposition party leader Bekbolot Talgarbekov is heard saying to his fellow party members, “[f]irst of all, we must get rid of Atambayev. Without getting rid of [Atambayev] we cannot fix the personnel policy, and then, for example, we will achieve victory. We will come to power. We must create a new coalition.”¹¹¹ Talgarbekov goes on to discuss his plans for organizing protests across Kyrgyzstan to demonstrate citizens’ weak support for the SDPK. He continues, “I’ll bring out a meeting of 20 thousand people. What kind of meeting there will be 20 thousand - 350 thousand.”¹¹² While the online source for these recordings is nonattributable, according to Freedom House, “...the pattern of targeting opposition leaders suggests abuse of SORM equipment by the government.”¹¹³ After the files were released, Talgarbekov and his co-conspirers were arrested and convicted for their attempt to forcibly seize power from the SDPK.¹¹⁴

These examples demonstrate how Kyrgyzstan’s government abuse surveillance technologies to target politicians for the purpose of suppressing dissent. The SDPK exploits weak judicial oversight to surveil oppositional party members to secure its own political survival. As this case study shows, the use of the Russian SORM technology offers an effective system for state-wide digital surveillance.

Global response

The expansion of digital authoritarianism depends on technology exports. These technologies include surveillance software and the associated hardware that enables authoritarian countries to implement more sophisticated repression strategies with the objective of securing regime survival.¹¹⁵ To contextualize on a global scale, the surveillance industry is colossal, estimated at approximately \$37 billion in 2018 and is projected to almost double by 2023.¹¹⁶ Findings that implicate democracies in the proliferation of surveillance technologies to countries where human

rights are being grossly violated has prompted governments, along with industry input, to reexamine export control measures in an effort to limit states' abuse of these technologies.¹¹⁷ In sum, digital authoritarian regimes such as China and Russia are not alone in spreading these technologies.

Wassenaar Arrangement

At present, the most significant international response that exists to manage surveillance technologies can be found in the Wassenaar Arrangement. Made up of 42 participating member states, the Wassenaar Arrangement is the largest and most comprehensive international export control regime that governs dual-use information and communications technologies.¹¹⁸ Participants meet twice per year and work together to control exports through the creation of a common list of dual-use technologies that is not legally binding and is left for each government to voluntarily implement through its own regulatory processes.¹¹⁹ Members also agree to exchange information regarding specific export denials and licensing.¹²⁰

Limited success governing surveillance technologies came in 2013 with the formal adoption of human rights considerations into the Wassenaar Arrangement. Specifically, according to Fabian Bohnenberger, a PhD candidate at King's College, "member States, staying within the arrangement's narrow mandate, justified the measures arguing that these technologies, 'under certain conditions, may be detrimental to international and regional security and stability.'"¹²¹ Inextricably linking human rights to national security interests. This recognition was articulated in a 2013 amendment to the Wassenaar Arrangement adopting the first controls on cyber-surveillance technologies that identified "intrusion software" and "IP network communications surveillance systems," as threats to human rights and privacy.¹²² Almost immediately, however, this amendment met stiff resistance from information technology experts

and private industry, who argued that “unduly stringent or ill-defined controls on cyber-surveillance technologies can hurt legitimate business interests and have harmful effects on computer security research.”¹²³ The definitions of surveillance technologies continue to be refined during the bi-annual meetings to help policy-makers and industry leaders craft targeted initiatives or regulations. However, current surveillance technology export controls under the Wassenaar Arrangement continue to be implemented piecemeal by individual member states.¹²⁴

Agreeable definitions are only one of several challenges the Wassenaar Arrangement faces; members still continue to disagree on where exports should and should not be allowed.¹²⁵ The central problem is that balancing the economic, political, and security interests of the diverse Wassenaar Arrangement membership increases opposition to a unified multinational effort. For example, Russia is a member that remains subject to American and European Union sanctions, creating further roadblocks in the arrangement.¹²⁶ Adopting cyber-surveillance technology export control measures was a significant step forward for the international community, but these ongoing challenges call further attention to the need for a more robust response.

The Freedom Online Coalition

The Freedom Online Coalition was formed in 2011 and is comprised of 31 governments from around the world that include developed and developing countries alike.¹²⁷ The Coalition’s objective is to proactively bring together civil society, non-governmental organizations, and industry stakeholders to promote their agenda of supporting internet freedom and safeguarding human rights online.¹²⁸ Specifically, the Freedom Online Coalition states their aim is to ensure these issues “are on the international policy agenda as a way to drive concrete policy changes and outcomes.”¹²⁹ In 2014, the Coalition published a joint statement addressing the harmful effects of exporting surveillance technologies, explicitly calling attention to its abuse for the

purpose of “political repression.”¹³⁰ In the statement, the Coalition appealed to governments and industry to engage in an international multi-stakeholder effort, which “should include the development of appropriate and consistent national laws and policies governing the use and export of such technologies.”¹³¹ The Freedom Online Coalition serves as an illustration of a strong and well-connected governmental advocacy group for greater export control measures. However, without a regulatory backbone to this Coalition, meaningful governance has not been effective.

Other global initiatives

Parallel efforts by international, civil society, NGOs, and private industry organizations have stepped up their advocacy for greater restrictions on the exportation of surveillance technologies. The global Coalition Against Unlawful Surveillance Exports (CAUSE), for example, is comprised of global leaders in human rights and other NGOs that collaborate to investigate and expose surveillance transfers to governments that use them to violate privacy and commit human rights abuses.¹³² Their work calls on governments to “establish strict trade controls” and to enforce a “Core Rule” that mandates human rights due diligence for all surveillance technology exports.¹³³

In a similar vein, the United Nations Internet Governance Forum (IGF) aims to bring together international stakeholders to discuss and inform policy dialogue on internet governance.¹³⁴ In 2013, the IGF took on the “emergent issue” of expanding internet surveillance, recognizing that the abuse of surveillance technologies by repressive regimes undermines democratic values of a free internet.¹³⁵ While the IGF may not have decision-making mandates, it has been successful in giving stakeholders from developing countries “the opportunity to engage in the debate on Internet governance,” providing a medium that builds these countries

“knowledge and skills that will facilitate their participation in existing Internet governance institutions and arrangements.”¹³⁶ In sum, this forum attempts to prevent the abuse of surveillance technologies in vulnerable nation states by “promoting participatory democratic bottom-up processes.”¹³⁷

These two efforts serve as integral parts of the many coordinated actions that seek to combat the proliferation and abuse of surveillance technologies. Other multilateral United Nations-level forums—like the International Telecommunications Union, think tanks—such as Carnegie Endowment for International Peace, NGOs—such as Electronic Frontier Foundation—and private sector initiatives—like DIGITALEUROPE—pursue issues related to the negative impacts of pervasive surveillance.¹³⁸ Yet, while they all possess a common goal to protect the rights of people online, there is no sufficient international framework to enforce comprehensive legal controls to stop the proliferation of these technologies to repressive regimes.

Proposed international governance

Analyzing the existing measures for implementing export controls reveals the enormous complexities of regulating surveillance technologies across the world. Some proponents for changes to the present global governance want the inclusion of “intent” adopted into control measures.¹³⁹ Bohnenberger explains:

By shifting the definition of ‘intrusion software’ to focus on intent, not functionality, the export authorization would rely more on contextual information. Manifest intent could, for example, be established by looking at the way the software is designed, i.e., whether it is designed to be used against a non-consenting other party, or the way the software is marketed.¹⁴⁰

Advocates of this proposal argue that exporters are in the best position to assess the intent of their customers.¹⁴¹ Ben Wagner, the Director of the Centre for Internet and Human Rights at European University, and his co-author, Joanna Bronowicka, emphasize that surveillance exports are rarely “one-off” transactions in that companies typically sell the training and updates

required to sustain the technology's use, making the relationship between the vendor and buyer generally long-term.¹⁴²

Incorporating intent into control measures would also satisfy efforts to mandate human rights due diligence into surveillance technology exports. According the United Nations Principles Reporting Framework, human rights due diligence can be understood as:

An ongoing risk management process...in order to identify, prevent, mitigate and account for how [a company] addresses its adverse human rights impacts. It includes four key steps: assessing actual and potential human rights impacts; integrating and acting on the findings; tracking responses; and communicating about how impacts are addressed.¹⁴³

The European Union has already taken steps toward implementing human rights considerations into its surveillance technology export control measures.¹⁴⁴ However, industry critics of the regulation argue that the human rights standards are too ambiguous and may “complicate licensing assessments, increase the need for information collection about their customers, and decrease legal certainty.”¹⁴⁵ Reluctance on behalf of exporters to take on comprehensive human rights due diligence is a significant challenge that is not unique to the European Union. The same industry criticism was received by the United States, which to date has delayed the adoption of the Wassenaar Arrangement's 2013 amendments while working with private industry and other stakeholders to find an agreeable solution to their implementation.¹⁴⁶ Instead, the United States manages the export of surveillance technologies through domestic administrative regulations that “do not mirror, but reflect the spirit, of the language of the Agreement.”¹⁴⁷ In 2019, the United States issued “draft” export guidelines for surveillance technologies recommending that American companies adopt human rights considerations into their export compliance programs.¹⁴⁸ Even if the guidelines become formally published, adherence will not be mandatory under United States law, further demonstrating the lack of uniformity in a response across the international community.

Additional proposals to strengthen export control governance come from foreign policy and human rights experts who stress that without complimentary international policy initiatives, export control measures will never be enough.¹⁴⁹ Collaborative policy responses from democratic countries would inform the international community of the ongoing issues that surround the proliferation of surveillance technologies and develop shared standards.¹⁵⁰ Moreover, foreign policy expert and Executive Vice President of Freedom House, Daniel Calingaert stresses that companies in democratic countries are not in a position to resist pressure from foreign governments that ask them to turn over users' personal data or to have back-door access to allow for interception and monitoring without assistance from their respective governments.¹⁵¹ Coordinated international policy efforts would present a united front against repressive regimes that solicit such information from surveillance technology exporters, giving companies greater confidence that their governments would intervene on their behalf.¹⁵² Until democratic countries coalesce with their efforts and come to exporters' defense, no recourse currently exists to withstand such blatant violations of privacy.

These examples demonstrate the limits of each of these initiatives to address the growing international concern over the globalization of surveillance technologies. We know there are inherent political, economic, and security challenges—beyond creating a global response—that interfere with establishing consistent regulations and policies. These challenges lie outside the scope of this paper, but further expose the uphill battle for democracies to internationally streamline surveillance technology export controls. This paper demonstrates that reversing the trend of expanding digital authoritarianism can be accomplished, though it will require democracies to do more.

Discussion

The evaluation of Uganda and Kyrgyzstan's abuse of imported surveillance technologies show how digital authoritarianism is becoming entrenched globally. In both countries, surveillance technologies enable repression. In particular, we observe that in Uganda the acquisition of more sophisticated surveillance technologies from China, such as real-time monitoring, facilitates increasing government repression. If a comprehensive and legally binding international export control measure was in existence to govern these technologies, Uganda and Kyrgyzstan may have found it difficult to gain access to such advanced monitoring; at the very least, there would have existed a mechanism to take action against the exporter and the originating government. Consensus that there is problem from democracies is not enough.

Nearly unrestricted global governance provided Uganda and Kyrgyzstan the means to shut-off access to political change before mobilization could materialize. In these instances, the spread of surveillance technologies strengthened the survivability of these authoritarian regimes. The examination of the global response shows us that walking back the expansion of digital authoritarianism is possible. However, until Western countries are prepared and willing to develop a consistent response—one that is capable of confronting a powerful country like China—making progress on an international level to stop the proliferation of surveillance technologies to repressive regimes will continue to be ineffective.

Implications

China and Russia are digital authoritarian regimes that leverage opportunities to propagate influence globally.¹⁵³ These countries have done this by perfecting and packaging “the authoritarian toolkit” for exportation to an eager and less sophisticated illiberal market.¹⁵⁴ Digital surveillance, in particular, offers governments an opportunity to enhance domestic

control and harden their political survival.¹⁵⁵ As Uganda and Kyrgyzstan show us, in a world where digital interconnectedness would suggest otherwise, digital authoritarians have developed new deterrents to social and political change through the integration of online surveillance into their broader repression strategies. Specifically, interfering with citizens' ability to mobilize.

However, it is not just China and Russia's surveillance technology that is enticing to repressive governments; like-minded regimes are also emulating invasive cyber-security laws and regulations that force domestic internet service providers and other technology companies to support their governments in the warrantless monitoring of the communication and metadata of their users.¹⁵⁶ As a case in point, Russia requires all of its domestic telecommunication companies to install SORM equipment.¹⁵⁷ Companies that do not comply are severely fined or shut-down.¹⁵⁸ In 2010, the authoritarian country of Belarus took similar steps by adopting laws that require a SORM-style system to be used by all of its internet service providers.¹⁵⁹ These internet-related laws and practices run counter to democratic values that promote a free and open internet.

Consequently, rising digital authoritarians are following in the footsteps of more sophisticated regimes, learning how they can use the internet for their own political ends. Justin Sherman and co-author, Robert Morgus, a senior policy analyst with the New America think tank, argue that the export of surveillance technologies to repressive regimes is promoting an "authoritarian model" of the internet that delivers governments an "insidious tool" for population control.¹⁶⁰ Online surveillance, if unrestrained, erodes government transparency and accountability, making control more effective and simultaneously increasing the cost of mobilization. As privacy freedoms continue to deteriorate around the world, it begs the question, can democracies fight back?

Through role modeling, exportation of surveillance technologies and training, digital authoritarian regimes are vying to promote their form of governance as a pragmatic alternative to the Western democracies.¹⁶¹ According to Freedom House's 2019 annual survey, freedom around the world has declined for the thirteenth consecutive year.¹⁶² Diamond argues that any corrective action must come from democracies, "[i]f authoritarian backsliding and impunity are to be slowed and ended, the Western democracies must recover their voice."¹⁶³ Existing approaches to stop the globalization of surveillance technologies to repressive regimes are not reinforced with direct challenges to foreign governments that undermine democracy. Only a united front among the world's democratic nations can seriously oppose the global advance of digital authoritarianism. According to Weber, if democracies remain silent, the spread of suppression technologies will continue to "reinforce and normalize the ideologies of autocratic regimes like China and Russia."¹⁶⁴

Conclusion

Digital authoritarian governments employ surveillance technologies within a larger framework of repression that violates the human rights and fundamental freedoms of their citizens. The human cost to this technology is undeniable. Through the exportation of these sophisticated technologies, digital authoritarianism is anchoring itself into like-minded regimes that unmistakably fracture democratic norms and putting at risk future chances for democratization. The Western democracies will have to become comfortable wielding diplomatic measures that force powerful countries like Russia and China to comply with an international export governance that respects the rights of citizens online. As surveillance technologies continue to proliferate practically unregulated to governments that are more prone to abuse them,

opportunities for citizens to enjoy privacy, in any domain, may in fact become Vince Cerf's

"anomaly."¹⁶⁵

¹ Feng Xiang (cited in) Louise Lucas and Emily Feng, "Inside China's Surveillance State." *Financial Times*, July 20, 2018. <https://www.ft.com/content/2182eebe-8a17-11e8-bf9e-8771d5404543>.

² Vince Cerf, "Opening remarks at the Internet of Things Workshop," (speech, Washington DC, November 19, 2013), Federal Trade Commission, https://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf.

³ Rebecca MacKinnon, "China's 'Networked Authoritarianism,'" in *Liberation Technology: Social Media and the Struggle for Democracy*, ed. L. Diamond and M.F. Plattner (Baltimore, MD: Johns Hopkins University Press, 2012), 78-92.

⁴ Alina Polyakova and Chris Meserole. *Exporting Digital Authoritarianism*. Democracy and Disorder Series, (Washington, DC: The Brookings Institution, August 2019), 1, https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190826_digital_authoritarianism_polyakova_meserole.pdf.

⁵ Adrian Shahbaz, *The Rise of Digital Authoritarianism*, Freedom on the Net (Washington, DC: Freedom House, 2018), 1-28, https://freedomhouse.org/sites/default/files/FOTN_2018_Final.pdf.

⁶ Fabian Bohnenberger, "The Proliferation of Cyber-Surveillance Technologies: Challenges and Prospects for Strengthened Export Controls." *Strategic Trade Review* 3, no. 4 (2017), 81-102, doi:10.1080/19331681.2019.1616646; Jukka Ruohonen and Kai K. Kimppa, "Updating the Wassenaar Debate Once Again: Surveillance, Intrusion Software, and Ambiguity," *Journal of Information Technology & Politics* 16, no. 2 (2019), 169-186, doi:10.1080/19331681.2019.1616646.

⁷ *How Corporations and Big Tech Leave Our Data Exposed to Criminals, China, and Other Bad Actors: Hearing before the Senate Judiciary Subcommittee on Crime and Terrorism*, 116th Cong., 4 (2019) (statement of Kara Frederick, Fellow, Technology and National Security Center for a New American Security).

⁸ Rebecca MacKinnon, "China's 'Networked Authoritarianism,'" Larry Diamond, "Liberation Technology," in *Liberation Technology: Social Media and the Struggle for Democracy*, ed. L. Diamond and M.F. Plattner (Baltimore, MD: Johns Hopkins University Press, 2012), 3-17.

⁹ Valentin Weber, "The worldwide web of Chinese and Russian information controls," (Washington, DC: Open Technology Fund, September 2019), <https://www.opentech.fund/news/examining-expanding-web-chinese-and-russian-information-controls/>; Elizabeth Stoycheff, G. Scott Burgess, and Maria Clara Martucci, "Online Censorship and Digital Surveillance: The Relationship between Suppression Technologies and Democratization across Countries," *Information, Communication & Society* 23, no. 4 (2020), 474-490, <https://doi.org/10.1080/1369118X.2018.1518472>.

¹⁰ Ronald Deibert, "The Road to Digital Unfreedom: Three Painful Truths About Social Media," *Journal of Democracy* 30, no. 1 (2019), 25-39, <https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-three-painful-truths-about-social-media/>; Larry Diamond, "Breaking out of the Democratic Slump," *Journal of Democracy* 31, no. 1 (2020), 36-50, doi:10.1353/jod.2020.0003.

¹¹ Natalia Antelava, "Authoritarian Technology and Disinformation: A Conversation with Natalia Antelava," interview by Christopher Walker. *Power 3.0*, National Endowment for Democracy, podcast audio, December 17, 2019, <https://www.power3point0.org/2019/12/17/authoritarian-technology-and-disinformation-a-conversation-with-natalia-antelava/>.

¹² Rebecca MacKinnon, "China's 'Networked Authoritarianism,'" Adrian Shahbaz, *The Rise of Digital Authoritarianism*, Freedom on the Net; Marcus Michaelsen and Marlies Glasius, "Authoritarian Practices in the Digital Age: Illiberal and Authoritarian Practices in the Digital Sphere — Prologue," *International Journal of Communication* 12 (2018), 3795-3813. <https://ijoc.org/index.php/ijoc/article/viewFile/8899/2459>; Alina Polyakova and Chris Meserole, *Exporting Digital Authoritarianism*, 1-21; Adrian Shahbaz and Allie Funk, *The Crisis of Social Media*, Freedom on the Net (Washington, DC: Freedom House, 2019), 1-29, https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf; E. Stoycheff, S. Burgess and M. Martucci, "Online Censorship and Digital Surveillance," 474-490.

¹³ Rebecca MacKinnon, "China's 'Networked Authoritarianism,'" Alina Polyakova and Chris Meserole, *Exporting Digital Authoritarianism*; Justin Sherman, "The Long View of Digital Authoritarianism," *New America Weekly*, June 20, 2019. <https://www.newamerica.org/weekly/long-view-digital-authoritarianism/>;

- Jessica Chen Weiss, "Understanding and Rolling Back Digital Authoritarianism," *War on the Rocks* (blog), February 17, 2020, <https://warontherocks.com/2020/02/understanding-and-rolling-back-digital-authoritarianism/>.
- ¹⁴ Anne-Marie Slaughter (cited in) Justin Sherman, "The Long View of Digital Authoritarianism."
- ¹⁵ Neil M. Richards, "The Dangers of Surveillance," *Harvard Law Review* 126, no. 7 (2013), 1934-965, www.jstor.org/stable/23415062; Scott Robbins and Adam Henschke, "Designing for Democracy: Bulk Data and Authoritarianism," *Surveillance & Society* 15, no. 3/4 (2017), 582-589, <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/6606>; Jonathon W Penney, "Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study," *Internet Policy Review* 6, no. 2 (2017), 1-39, <https://doi.org/10.14763/2017.2.692>; Anita Rosemary Gohdes, "Repression in the Digital Age: Communication Technology and the Politics of State Violence" (DSSc diss., Fakultät für Sozialwissenschaften, 2014), 1-128, Universität Mannheim, <https://pdfs.semanticscholar.org/5990/a07deaf211e64c3e02a8450791d832efd7bc.pdf>.
- ¹⁶ M. Michaelsen and M. Glasius, "Authoritarian Practices in the Digital Age," 3802.
- ¹⁷ E. Stoycheff, S. Burgess and M. Martucci, "Online Censorship and Digital Surveillance," 474-490.
- ¹⁸ Larry Diamond, "Liberation Technology," 3-17.
- ¹⁹ Hilary Rodham Clinton, "Remarks on Internet Freedom," (speech, Washington, DC, January 21, 2010), <https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm>.
- ²⁰ Ibid.
- ²¹ Ibid.
- ²² Xiao Qiang, "The Road to Digital Unfreedom: President Xi's Surveillance State," *Journal of Democracy* 30, no. 1 (2019), 53-67, <https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-president-xis-surveillance-state/>.
- ²³ William J. Clinton, "China Trade Bill," (speech, Baltimore, MD, March 9, 2000), Institute for Agriculture and Trade Policy, https://www.iatp.org/sites/default/files/Full_Text_of Clintons_Speech_on_China_Trade_Bi.htm.
- ²⁴ Tufekci, Zeynep. *Twitter and Tear Gas: The Power and Fragility of Networked Protest* (New Haven, CT: Yale University Press, 2017).
- ²⁵ Larry Diamond, "Breaking out of the Democratic Slump," 36.
- ²⁶ Economist Intelligence Unit, *Global Democracy in Retreat*, (New York, NY: The Economist, January 21, 2020), <https://www.eiu.com/n/global-democracy-in-retreat/>.
- ²⁷ Ibid, 6.
- ²⁸ Adrian Shahbaz and Allie Funk, *The Crisis of Social Media, Freedom on the Net*, 1-29.
- ²⁹ Ibid.
- ³⁰ Larry Diamond, "Elections Without Democracy: Thinking About Hybrid Regimes," *Journal of Democracy* 13, no. 2 (2002): 21-35. doi:10.1353/jod.2002.0025; Natasha M. Ezrow and Erica Frantz, *Dictators and Dictatorships: Understanding Authoritarian Regimes and Their Leaders*, (New York, NY: Bloomsbury, 2011); M. Michaelsen and M. Glasius, "Authoritarian Practices in the Digital Age," 3795-3813; Marlies Glasius, "What authoritarianism is ... and is not: a practice perspective," *International Affairs* 94, no. 3 (2018), 515-533. <https://doi.org/10.1093/ia/iyy060>.
- ³¹ Ibid.
- ³² Adam Przeworski et al., *Democracy and Development: Political Institutions and Well-Being in the World, 1950-1990* (Cambridge: Cambridge University Press, 2000); N. Ezrow and E. Frantz, *Dictators and Dictatorships*.
- ³³ Nils B. Weidmann and Espen Geelmuyden Rød, *The Internet and Political Protest in Autocracies* (New York, NY: Oxford University Press, 2019), 54.
- ³⁴ Marlies Glasius, "What authoritarianism is ... and is not," 518.
- ³⁵ N. Weidmann and G. Rød, *The Internet and Political Protest in Autocracies*.
- ³⁶ N. Ezrow and E. Frantz, *Dictators and Dictatorships: Understanding Authoritarian Regimes and Their Leaders*.
- ³⁷ Ibid, 4.
- ³⁸ Tufekci, Zeynep. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*, 223.
- ³⁹ Larry Diamond, "Elections Without Democracy;" Rebecca MacKinnon, "China's 'Networked Authoritarianism.'"
- ⁴⁰ Freedom House, "Freedom in the World 2019: Vietnam," accessed January 21, 2020, <https://freedomhouse.org/country/Vietnam/freedom-world/2019>.
- ⁴¹ Anita Gohdes, "Repression in the Digital Age," 1-128; E. Stoycheff, S. Burgess and M. Martucci, "Online Censorship and Digital Surveillance," 474-490.
- ⁴² Alina Polyakova, "Russia is Teaching the World to Spy," *New York Times*, December 5, 2019, <https://www.nytimes.com/2019/12/05/opinion/russia-hacking.html>.
- ⁴³ Freedom House, "Freedom in the World 2020: Russia," accessed February 15, 2020, <https://freedomhouse.org/country/Russia/freedom-world/2020>.

-
- ⁴⁴ Rebecca MacKinnon, "China's 'Networked Authoritarianism,'" 79.
- ⁴⁵ N. Weidmann and G. Rød, *The Internet and Political Protest in Autocracies*.
- ⁴⁶ Rebecca MacKinnon, "China's 'Networked Authoritarianism,'" 79.
- ⁴⁷ Jack M. Balkin, "The Constitution in the National Surveillance State," *Minnesota Law Review* 93, no. 1 (2008), 1-25, https://www.minnesotalawreview.org/wp-content/uploads/2012/01/Balkin_MLR.pdf; David Lyon, "Surveillance, Power and Everyday Life," in *Emerging Digital Spaces in Contemporary Society: Properties of Technology*, ed. by Phillip Kalantzis-Cope and Karim Gherab-Martín, 107-120 (London: Palgrave Macmillan, 2010); Neil M. Richards, "The Dangers of Surveillance," 1934-965.
- ⁴⁸ Jack Balkin, "The Constitution in the National Surveillance State," 1-25.
- ⁴⁹ David Lyon, "Surveillance, Power and Everyday Life," 107-120.
- ⁵⁰ Centers for Disease Control and Prevention, "Lesson 5: Public Health Surveillance," in *Principles of Epidemiology in Public Health Practice*, 3rd ed, last modified May 18, 2012. <https://www.cdc.gov/csels/dsepd/ss1978/lesson5/section4.html>.
- ⁵¹ Neil M. Richards, "The Dangers of Surveillance," 1934-965.
- ⁵² Jack Balkin, "The Constitution in the National Surveillance State," 1-25; Zygmunt Bauman and David Lyon, *Liquid Surveillance: A Conversation* (Germany: Wiley, 2013); Anita Gohdes, "Repression in the Digital Age," 1-128.
- ⁵³ Yochai Benkler, "We Cannot Trust Our Government, So We Must Trust the Technology," *Guardian*, February 22, 2016, <https://www.theguardian.com/us-news/2016/feb/22/snowden-government-trust-encryption-apple-fbi>.
- ⁵⁴ Ibid.
- ⁵⁵ Ibid.
- ⁵⁶ Anita Gohdes, "Repression in the Digital Age," 13.
- ⁵⁷ David Kaye, "The surveillance industry is assisting state suppression. It must be stopped," *Guardian*, November 26, 2019, <https://www.theguardian.com/commentisfree/2019/nov/26/surveillance-industry-suppression-spyware>.
- ⁵⁸ Jason Koebler, "The Washington Post's New Columnist Consults for Spyware Firm That Helps Saudi Arabia Surveil Journalists," *Vice*, October 22, 2019, https://www.vice.com/en_us/article/d3aezq/the-washington-posts-new-columnist-consults-for-spyware-firm-that-helps-saudi-arabia-surveil-journalists.
- ⁵⁹ Rebecca MacKinnon, "China's 'Networked Authoritarianism.'" 79.
- ⁶⁰ E. Stoycheff, S. Burgess and M. Martucci, "Online Censorship and Digital Surveillance," 478.
- ⁶¹ Neil M. Richards, "The Dangers of Surveillance," 1934-965.
- ⁶² Jonathon W Penney, "Internet Surveillance, Regulation, and Chilling Effects Online," 1-39.
- ⁶³ Jack Balkin, "The Constitution in the National Surveillance State," 1-25.
- ⁶⁴ Ibid, 12.
- ⁶⁵ Z. Bauman and D. Lyon, *Liquid Surveillance*; S. Robbins and A. Henschke, "Designing for Democracy: Bulk Data and Authoritarianism," 582-589.
- ⁶⁶ Ibid.
- ⁶⁷ Jack Balkin, "The Constitution in the National Surveillance State," 1-25; Z. Bauman and D. Lyon, *Liquid Surveillance*; S. Robbins and A. Henschke, "Designing for Democracy: Bulk Data and Authoritarianism," 582-589.
- ⁶⁸ Xiao Qiang, "President Xi's Surveillance State," 53-67.
- ⁶⁹ Ibid.
- ⁷⁰ Alina Polyakova and Chris Meserole, *Exporting Digital Authoritarianism*.
- ⁷¹ General Assembly Resolution 68/167, *The Right to Privacy in the Digital Age*, A/RES/68/167 (18 December 2013) available from <https://undocs.org/A/RES/68/167>.
- ⁷² Ibid, 2.
- ⁷³ Adrian Shahbaz and Allie Funk, *The Crisis of Social Media, Freedom on the Net*, 16.
- ⁷⁴ Justin Sherman, "Vietnam's Internet Control: Following in China's Footsteps," *Diplomat*, December 11, 2019, <https://thediplomat.com/2019/12/vietnams-internet-control-following-in-chinas-footsteps/>.
- ⁷⁵ Ibid.
- ⁷⁶ Open Tech Fund, *Examining the Expanding Web of Chinese and Russian Information Controls*, News, updates, and announcements (Washington, DC: Open Tech Fund, September 17, 2019), <https://www.opentech.fund/news/examining-expanding-web-chinese-and-russian-information-controls/>.
- ⁷⁷ Ibid.
- ⁷⁸ Office of the United Nations High Commissioner for Human Rights to Permanent Missions to the United Nations Office at Geneva and New York, February 26, 2014, <https://www.ohchr.org/EN/HRBodies/HRC/Regular>

Sessions/Session27/Documents/A.HRC.27.37_en.pdf; United Nations General Assembly Human Rights Council. *Surveillance and human rights* (New York, New York: United Nations General Assembly, 2019), 10, <https://digitallibrary.un.org/record/3802433?ln=en>.

⁷⁹ United Nations General Assembly Human Rights Council. *Surveillance and human rights*, 14.

⁸⁰ Steven Feldstein, “The Global Expansion of AI Surveillance,” (working paper, Carnegie Endowment for International Peace, 2019), 1, also available online at: https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf.

⁸¹ Robert Morgus and Justin Sherman, “How U.S. surveillance technology is propping up authoritarian regimes,” *Washington Post*, January 17, 2019, <https://www.washingtonpost.com/outlook/2019/01/17/how-us-surveillance-technology-is-propping-up-authoritarian-regimes/>.

⁸² Sari Horwitz, “Syria using American software to censor Internet, experts say” *Washington Post*, October 22, 2011, https://www.washingtonpost.com/world/national-security/syria-using-american-software-to-censor-internet-experts-say/2011/10/22/gIQA5mPr7L_story.html.

⁸³ David Kaye, “The surveillance industry is assisting state suppression,” *Guardian*. Freedom Online Coalition, “About Us,” accessed January 21, 2020, <https://freedomonlinecoalition.com/about-us/>; United Nations, “Internet Governance Forum: About the IGF,” accessed January 21, 2020, <https://www.intgovforum.org/multilingual/tags/about>.

⁸⁴ The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC, 2011), 23, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

⁸⁵ Ronald Deibert, “The Road to Digital Unfreedom: Three Painful Truths About Social Media,” *Journal of Democracy*.

⁸⁶ Ibid.

⁸⁷ Larry Diamond, “Liberation Technology,” 16.

⁸⁸ Freedom House, “Freedom in the World 2019: Uganda,” accessed January 21, 2020, <https://freedomhouse.org/country/Uganda/freedom-world/2019>.

⁸⁹ Ibid.

⁹⁰ Ibid.

⁹¹ Privacy International. *For God and My President: State Surveillance In Uganda*, (London, UK: Privacy International, October 2015), https://privacyinternational.org/sites/default/files/2017-12/Uganda_Report_1.pdf.

⁹² Ibid.

⁹³ Ibid.

⁹⁴ Ibid.

⁹⁵ Ibid, 6.

⁹⁶ Ibid.

⁹⁷ Samuel Woodhams, “Huawei, Africa and the global reach of surveillance technology,” *Deutsche Welle*, December 9, 2019, <https://www.dw.com/en/huawei-africa-and-the-global-reach-of-surveillance-technology/a-50398869>.

⁹⁸ Elias Biryabarema, “Uganda's cash-strapped cops spend \$126 million on CCTV from Huawei,” *Reuters*, August 15, 2019, <https://www.reuters.com/article/us-uganda-crime/ugandas-cash-strapped-cops-spend-126-million-on-cctv-from-huawei-idUSKCN1V50RF>.

⁹⁹ Joe Parkinson, Nicholas Bariyo, and Josh Chin, “Huawei Technicians Helped African Governments Spy on Political Opponents,” *Wall Street Journal*, August 15, 2019, <https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017>.

¹⁰⁰ Ibid.

¹⁰¹ Ibid, 1.

¹⁰² Ibid, 6.

¹⁰³ Ibid.

¹⁰⁴ Freedom House, “Freedom in the World 2019: Kyrgyzstan,” accessed March 15, 2020, <https://freedomhouse.org/country/Kyrgyzstan/freedom-world/2019>.

¹⁰⁵ Ibid.

¹⁰⁶ Ibid.

¹⁰⁷ Freedom House, “Freedom on the Net 2018: Kyrgyzstan,” last modified November 1, 2018, https://www.refworld.org/docid/5be16b0aa.html#_ftn49.

¹⁰⁸ Eurasianet, “Kyrgyzstan: Bishkek Snoops Relying on Russian Spyware,” Eurasianet.org, November 7, 2012, <https://eurasianet.org/kyrgyzstan-bishkek-snoops-relying-on-russian-spyware>.

-
- ¹⁰⁹ Freedom House, “Freedom on the Net 2018: Kyrgyzstan,” last modified November 1, 2018.
- ¹¹⁰ Kaktus Media, “Talks ostensibly members of ‘People’s Parliament’ leaked to the network,” May 12, 2016, https://kaktus.media/doc/338066_v_set_slili_peregovory_iakoby_chlenov_narodnogo_parlamenta.html.
- ¹¹¹ Ibid.
- ¹¹² Ibid.
- ¹¹³ Freedom House, “Freedom on the Net 2018: Kyrgyzstan,” last modified November 1, 2018.
- ¹¹⁴ Ibid.
- ¹¹⁵ Justin Sherman, “The Long View of Digital Authoritarianism,” *New America Weekly*.
- ¹¹⁶ PR Newswire, “Video Surveillance Market Worth 68.34 Billion USD by 2023,” *PRNewswire.com*, last modified May 7, 2018. <https://www.prnewswire.com/news-releases/video-surveillance-market-worth-6834-billion-usd-by-2023-681933911.html>.
- ¹¹⁷ Ben Wagner and Joanna Bronowicka, *Between International Relations and Arms Controls: Understanding Export Controls for Surveillance Technologies*, Export Controls of Surveillance Technologies (Frankfurt, Germany: Centre for Human Rights at the European University Viadrina, August 2015), 153-165, doi: 10.14746/pp.2015.20.3.11; Fabian Bohnenberger, “The Proliferation of Cyber-Surveillance Technologies,” Garrett Hinck, “Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research,” *Lawfare*, January 5, 2018, <https://www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research>; United Nations, “Internet Governance Forum: About the IGF,” accessed January 21, 2020, <https://www.intgovforum.org/multilingual/tags/about>.
- ¹¹⁸ Arms Control Association, “The Wassenaar Arrangement at a Glance,” accessed December 15, 2019, <https://www.armscontrol.org/factsheets/Wassenaar>.
- ¹¹⁹ Ibid.
- ¹²⁰ Ibid.
- ¹²¹ Fabian Bohnenberger, “The Proliferation of Cyber-Surveillance Technologies,” 84.
- ¹²² Ibid, 83.
- ¹²³ Ibid, 86.
- ¹²⁴ Garrett Hinck, “Wassenaar Export Controls on Surveillance Tools.”
- ¹²⁵ Arms Control Association, “The Wassenaar Arrangement at a Glance.”
- ¹²⁶ Fabian Bohnenberger, “The Proliferation of Cyber-Surveillance Technologies,” 89.
- ¹²⁷ Freedom Online Coalition, “About Us,” accessed January 21, 2020.
- ¹²⁸ Ibid.
- ¹²⁹ Ibid.
- ¹³⁰ Freedom Online Coalition, “Freedom Online Coalition: Statement on the Use and Export of Surveillance Technology,” accessed January 21, 2020, <https://www.freedomonlinecoalition.com/wp-content/uploads/2014/10/2-FOC-Joint-Statement-on-the-Use-and-Export-of-Surveillance-Technology-October-2014.pdf>.
- ¹³¹ Ibid.
- ¹³² Amnesty International, “Q&A: Coalition Against Unlawful Surveillance Exports (CAUSE),” last modified April 4, 2014, <https://www.amnesty.org/en/latest/news/2014/04/questions-and-answers-coalition-against-unlawful-surveillance-exports-cause/>.
- ¹³³ Ibid.
- ¹³⁴ United Nations, “Internet Governance Forum: About the IGF,” accessed January 21, 2020, <https://www.intgovforum.org/multilingual/tags/about>.
- ¹³⁵ United Nations, “Taking Stock / Emerging Issues – Internet Surveillance,” accessed 1 April, 2020, <https://intgovforum.org/multilingual/content/taking-stock-emerging-issues-%E2%80%93-internet-surveillance>.
- ¹³⁶ United Nations, “Internet Governance Forum: The Global Multistakeholder Forum for Dialogue on Internet Governance Issues,” last modified August 4, 2014, <http://intgovforum.org/cms/2014/IGFBrochure.pdf>.
- ¹³⁷ United Nations, “Internet Governance Forum: About the IGF,” background paper accessed January 21, 2020, 7, <https://www.intgovforum.org/cms/2015/IGF.24.06.2015.pdf>.
- ¹³⁸ United Nations, “International Telecommunication Union,” accessed 4 May, 2020, <https://www.itu.int/en/about/Pages/default.aspx>; Carnegie Endowment for International Peace, accessed January 21, 2020, <https://carnegieendowment.org>; Electronic Frontier Foundation, accessed January 21, 2020, <https://www.eff.org>; DIGITALEUROPE, accessed January 21, 2020, <https://www.digitaleurope.org>.
- ¹³⁹ Fabian Bohnenberger, “The Proliferation of Cyber-Surveillance Technologies,” 87.
- ¹⁴⁰ Ibid.
- ¹⁴¹ B. Wagner and J. Bronowicka, *Between International Relations and Arms Controls*, 160.

¹⁴² Ibid.

¹⁴³ “UNGP Reporting Framework: Salient Human Rights Issues,” *Business & Human Rights Resource Centre*, video, October 2018, 4:20, <https://www.business-humanrights.org/en/un-guiding-principles/implementation-tools-examples/implementation-by-companies/type-of-step-taken/human-rights-due-diligence>.

¹⁴⁴ Fabian Bohnenberger, “The Proliferation of Cyber-Surveillance Technologies,” 95.

¹⁴⁵ Ibid, 97.

¹⁴⁶ Marc Rotenberg and Eleni Kyriakides, *The Surveillance Industry and Human Rights*, submission of the Electronic Privacy Information Center to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (Washington, DC: EPIC, February 13, 2019, <https://epic.org/privacy/intl/EPICUNSurveillanceIndustry20190213.pdf>).

¹⁴⁷ Ibid, 3.

¹⁴⁸ US Department of State. *Draft U.S. Government Guidance for The Export of Hardware, Software and Technology with Surveillance Capabilities and/or Parts/Know-How*. (Washington, DC, 2019), <https://www.state.gov/wp-content/uploads/2019/09/DRAFT-GUIDANCE-FOR-THE-EXPORT-OF-HARDWARE-SOFTWARE-AND-TECHNOLOGY-WITH-SURVEILLANCE-CAPABILITIES.pdf>

¹⁴⁹ Daniel Calingaert, “Challenges for International Policy,” in *Liberation Technology: Social Media and the Struggle for Democracy*, ed. Larry Diamond and Marc F. Plattner, 157-173, (Baltimore, MD: Johns Hopkins University Press, 2012); Fabian Bohnenberger, “The Proliferation of Cyber-Surveillance Technologies.”

¹⁵⁰ Fabian Bohnenberger, “The Proliferation of Cyber-Surveillance Technologies.”

¹⁵¹ Daniel Calingaert, “Challenges for International Policy.”

¹⁵² Ibid.

¹⁵³ Valentin Weber, “The worldwide web of Chinese and Russian information controls.”

¹⁵⁴ Richard Fontaine and Kara Frederick, “The Autocrat’s New Tool Kit,” *Wall Street Journal*, March 15, 2019, <https://www.wsj.com/articles/the-autocrats-new-tool-kit-11552662637>.

¹⁵⁵ Rebecca MacKinnon, “China’s ‘Networked Authoritarianism.’”

¹⁵⁶ Adrian Shahbaz, *The Rise of Digital Authoritarianism*.

¹⁵⁷ Zack Whittaker, “Documents Reveal How Russia Taps Phone Companies for Surveillance,” *Techcrunch.com*, September 18, 2019, <https://techcrunch.com/2019/09/18/russia-sorm-nokia-surveillance/>.

¹⁵⁸ Ibid.

¹⁵⁹ Alina Polyakova and Chris Meserole, *Exporting Digital Authoritarianism*.

¹⁶⁰ Justin Sherman and Robert Morgus, “Authoritarians Are Exporting Surveillance Tech, And With it Their Vision for the Internet.” *Council on Foreign Relations* (blog), December 5, 2018, <https://www.cfr.org/blog/authoritarians-are-exporting-surveillance-tech-and-it-their-vision-internet>.

¹⁶¹ Adrian Shahbaz, *The Rise of Digital Authoritarianism*.

¹⁶² Freedom House, *Democracy in Retreat: Freedom House’s 2019 annual survey*, Freedom in the World (Washington, DC: Freedom House, 2019), 1-27, https://freedomhouse.org/sites/default/files/Feb2019_FH_FITW_2019_Report_ForWeb-compressed.pdf.

¹⁶³ Larry Diamond, “Breaking out of the Democratic Slump,” 48.

¹⁶⁴ Open Tech Fund, *Examining the Expanding Web of Chinese and Russian Information Controls*.

¹⁶⁵ Vince Cerf, “Opening remarks at the Internet of Things Workshop.”

Bibliography

- Antelava, Natalia. "Authoritarian Technology and Disinformation: A Conversation with Natalia Antelava." By Christopher Walker. *Power 3.0*, National Endowment for Democracy, podcast audio, December 17, 2019, <https://www.power3point0.org/2019/12/17/authoritarian-technology-and-disinformation-a-conversation-with-natalia-antelava/>.
- Balkin, Jack M. "The Constitution in the National Surveillance State." *Minnesota Law Review* 93, no. 1 (2008). https://www.minnesotalawreview.org/wp-content/uploads/2012/01/Balkin_MLR.pdf.
- Bauman, Zygmunt, and David Lyon. *Liquid Surveillance: A Conversation*. Germany: Wiley, 2013.
- Bohnenberger, Fabian. "The Proliferation of Cyber-Surveillance Technologies: Challenges and Prospects for Strengthened Export Controls." *Strategic Trade Review* 3, no. 4 (2017), 81-102, doi:10.1080/19331681.2019.1616646.
- Calingaert, Daniel. "Challenges for International Policy." In *Liberation Technology: Social Media and the Struggle for Democracy*. Edited by Larry Diamond and Marc F. Plattner, 157-173. Baltimore, MD: Johns Hopkins University Press, 2012.
- Cerf, Vince. "Opening Remarks at Internet of Things Workshop. Washington DC: Federal Trade Commission, 2013. https://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf.
- Clinton, William J. "China Trade Bill." Speech. Baltimore, MD, March 9, 2000. Institute for Agriculture and Trade Policy, https://www.iatp.org/sites/default/files/Full_Text_of_Clinton_Speech_on_China_Trade_Bi.htm.
- Deibert, Ronald. "The Road to Digital Unfreedom: Three Painful Truths About Social Media." *Journal of Democracy* 30, no. 1 (2019), 25-39, <https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-three-painful-truths-about-social-media/>.
- Diamond, Larry. "Elections Without Democracy: Thinking About Hybrid Regimes." *Journal of Democracy* 13, no. 2 (2002): 21-35. doi:10.1353/jod.2002.0025.
- Diamond, Larry. "China's 'Liberation Technology.'" In *Liberation Technology: Social Media and the Struggle for Democracy*. Edited by L. Diamond and M.F. Plattner. Baltimore, MD: Johns Hopkins University Press, 2012.
- Diamond, Larry. "Breaking out of the Democratic Slump." *Journal of Democracy* 31, no. 1 (2020), 36-50, doi:10.1353/jod.2020.0003.
- Economist Intelligence Unit. *Democracy Index 2019*. New York, NY: The Economist, January 21, 2020. https://www.eiu.com/public/topical_report.aspx?campaignid=democracyindex2019&zid=democracyindex2019&utm_source=blog&utm_medium=

blog&utm_name=democracyindex2019&utm_term=democracyindex2019&utm_content=bottom_link.

Ezrow, Natasha M., and Erica Frantz. *Dictators and Dictatorships: Understanding Authoritarian Regimes and Their Leaders*. New York, NY: Bloomsbury, 2011.

Feldstein, Steven. "The Global Expansion of AI Surveillance." Working Paper. Carnegie Endowment for International Peace, September 17, 2019. Also available online at: https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf.

Freedom House. *Democracy in Retreat: Freedom House's 2019 annual survey*. Freedom in the World. Washington, DC: Freedom House, 2019. https://freedomhouse.org/sites/default/files/Feb2019_FH_FITW_2019_Report_ForWeb-compressed.pdf.

Glasius, Marlies. "What authoritarianism is ... and is not: a practice perspective." *International Affairs* 94, no. 3 (2018), 515-533. <https://doi.org/10.1093/ia/iyy060>.

Gohdes, Anita Rosemary. "Repression in the Digital Age: Communication Technology and the Politics of State Violence." DSSc diss., Fakultät für Sozialwissenschaften, 2014. Universität Mannheim. <https://pdfs.semanticscholar.org/5990/a07deaf211e64c3e02a8450791d832efd7bc.pdf>.

Lichtenbaum, Peter, David W. Addis, and Doron O. Hindin. "Cyber-surveillance export control reform in the United States." *WorldECR* 75 (December 2018). <https://www.worldecr.com/archive/cyber-surveillance-export-control-reform-in-the-united-states/>.

Lyon, David. "Surveillance, Power and Everyday Life." In *Emerging Digital Spaces in Contemporary Society: Properties of Technology*. Edited by Phillip Kalantzis-Cope and Karim Gherab-Martín, 107-120. London: Palgrave Macmillan, 2010.

MacKinnon, Rebecca. "China's "Networked Authoritarianism." In *Liberation Technology: Social Media and the Struggle for Democracy*. Edited by L. Diamond and M.F. Plattner. Baltimore, MD: Johns Hopkins University Press, 2012.

Michaelsen, Marcus, and Marlies Glasius. "Authoritarian Practices in the Digital Age- Introduction." *International Journal of Communication* 12 (2018), 3788-3794, <https://ijoc.org/index.php/ijoc/article/view/8536>.

Michaelsen, Marcus, and Marlies Glasius. "Authoritarian Practices in the Digital Age: Illiberal and Authoritarian Practices in the Digital Sphere — Prologue." *International Journal of Communication* 12 (2018), 3795–3813. <https://ijoc.org/index.php/ijoc/article/viewFile/8899/2459>

Office of the United Nations High Commissioner for Human Rights to Permanent Missions to the United Nations Office at Geneva and New York, February 26, 2014.

Open Tech Fund. *Examining the Expanding Web of Chinese and Russian Information Controls*. News, updates, and announcements. Washington, DC: Open Tech Fund, September 17, 2019. <https://www.opentech.fund/news/examining-expanding-web-chinese-and-russian-information-controls/>

- Penney, Jonathon W. "Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study." *Internet Policy Review* 6, no. 2 (2017), <https://doi.org/10.14763/2017.2.692>.
- Polyakova, Alina, and Chris Meserole. *Exporting Digital Authoritarianism*. Democracy and Disorder Series. Washington, DC: The Brookings Institution, August 2019. <https://www.brookings.edu/research/exporting-digital-authoritarianism/>.
- Privacy International. *For God and My President: State Surveillance In Uganda*. London, UK: Privacy International, October 2015. https://privacyinternational.org/sites/default/files/2017-12/Uganda_Report_1.pdf.
- Przeworski, Adam, Michael E. Alvarez, Jose Antonio Cheibub, and Fernando Limongi. *Democracy and Development: Political Institutions and Well-Being in the World, 1950–1990*. Cambridge: Cambridge University Press, 2000.
- Qiang, Xiao. "The Road to Digital Unfreedom: President Xi's Surveillance State." *Journal of Democracy* 30, no. 1 (2019), 53-67. <https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-president-xis-surveillance-state/>.
- Richards, Neil M. "The Dangers of Surveillance." *Harvard Law Review* 126, no. 7 (2013), 1934-965. www.jstor.org/stable/23415062.
- Robbins, Scott, and Adam Henschke. "Designing for Democracy: Bulk Data and Authoritarianism." *Surveillance & Society* 15, no. 3/4 (2017), 582-589, <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/6606>.
- Rotenberg, Marc, and Eleni Kyriakides. *The Surveillance Industry and Human Rights*. Submission of the Electronic Privacy Information Center to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. Washington, DC: EPIC, February 13, 2019. <https://epic.org/privacy/intl/EPICUNSurveillanceIndustry20190213.pdf>.
- Ruohonen, Jukka, and Kai K. Kimppa. "Updating the Wassenaar Debate Once Again: Surveillance, Intrusion Software, and Ambiguity." *Journal of Information Technology & Politics* 16, no. 2 (2019), 169-186, doi:10.1080/19331681.2019.1616646.
- Shahbaz, Adrian, and Allie Funk. *The Crisis of Social Media*. Freedom on the Net. Washington, DC: Freedom House, 2019. <https://freedomhouse.org/report/freedom-net/2019/crisis-social-media>.
- Soldatov, Andrei, and Irina Borogan. "In Ex-Soviet States, Russian Spy Tech Still Watches You." *Wired*, December 21, 2012. <https://www.wired.com/2012/12/russias-hand/>.
- Stoycheff, Elizabeth, G. Scott Burgess, and Maria Clara Martucci. "Online Censorship and Digital Surveillance: The Relationship between Suppression Technologies and Democratization across Countries." *Information, Communication & Society* 23, no. 4 (2020), 474-490, <https://doi.org/10.1080/1369118X.2018.1518472>.
- Tufekci, Zeynep. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. New Haven, CT: Yale University Press, 2017.

United Nations General Assembly Human Rights Council. *Surveillance and human rights* (New York, New York: United Nations General Assembly, 2019), 10, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement>.

US Department of State. *Draft U.S. Government Guidance for The Export of Hardware, Software and Technology with Surveillance Capabilities and/or Parts/Know-How*. Washington, DC, 2019. <https://www.eff.org/files/2019/10/29/draft-guidance-for-the-export-of-hardware-software-and-technology-with-surveillance-capabilities.pdf>

Wagner, Ben, and Joanna Bronowicka. *Between International Relations and Arms Controls: Understanding Export Controls for Surveillance Technologies*. Export Controls of Surveillance Technologies. Frankfurt, Germany: Centre for Human Rights at the European University Viadrina, August 2015. DOI: 10.14746/pp.2015.20.3.11.

Weber, Valentin. *The worldwide web of Chinese and Russian information controls*. Washington, DC: Open Technology Fund, September 2019. <https://www.opentech.fund/news/examining-expanding-web-chinese-and-russian-information-controls/>.

Weidmann, Nils B., and Espen Geelmuyden Rød. *The Internet and Political Protest in Autocracies*. New York, NY: Oxford University Press, 2019.

The White House. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington, DC, 2011. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.