CENTRE FOR
TECHNOLOGY &
GLOBAL AFFAIRS

www.ctga.ox.ac.uk

UNIVERSITY OF
OXFORD

Working Paper Series – No. 11

September 2019

The Worldwide Web of Chinese and Russian Information Controls

Valentin Weber
Research Affiliate, Centre for Technology and Global Affairs
University of Oxford
valentin.weber@worc.ox.ac.uk

Working Paper Series – No. 11

ABSTRACT

The global diffusion of Chinese and Russian information control technology and techniques has featured prominently in the headlines of major international newspapers.[1] Few stories, however, have provided a systematic analysis of both the drivers and outcomes of such diffusion. This paper does so – and finds that these information controls are spreading more efficiently to countries with hybrid or authoritarian regimes, particularly those that have ties to China or Russia. Chinese information controls spread more easily to countries along the Belt and Road Initiative; Russian controls spread to countries within the Commonwealth of Independent States. In arriving at these findings, this working paper first defines the Russian and Chinese models of information control and then traces their diffusion to the 110 countries within the countries' respective technological spheres, which are geographical areas and spheres of influence to which Russian and Chinese information control technology, techniques of handling information, and law have diffused.

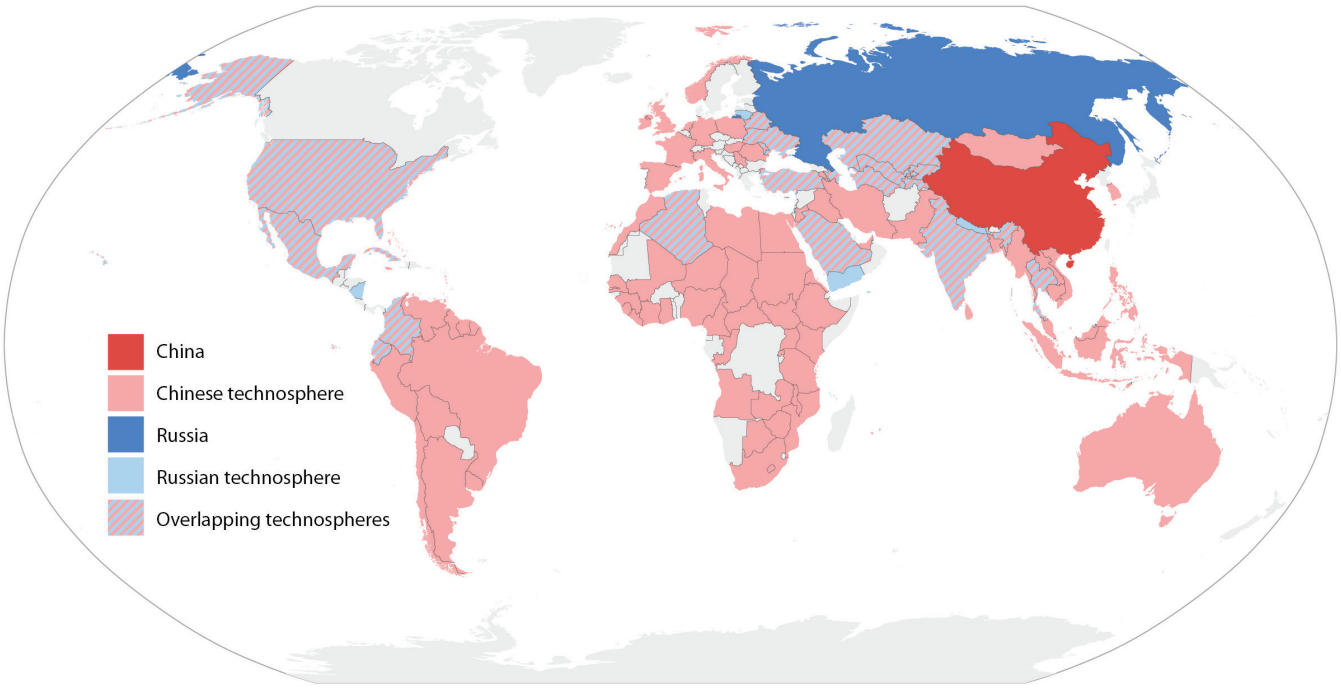
INTRODUCTION

Beijing's and Moscow's information control technology (e.g., the export of censorship equipment, safe cities) and techniques (e.g., the imitation of Chinese/Russian surveillance laws by other countries) have gone global. They have impacted small island nations in the Caribbean such as Antigua and Barbuda, with a mere 80,000 and 100,000 inhabitants, respectively, and a country with a sizeable population of over 1 billion in South Asia (India).[2] While journalists from the Bahamas, Lesotho, and Peru participate in propaganda trainings in Beijing, Chinese surveillance gear is used in a military command in the East of Brazil, and in Jordan's House of Parliament.[3] Russian surveillance equipment, for its part, is deployed in bordering countries like Belarus, Kazakhstan, and Ukraine as well as farther abroad in states like Algeria, Cuba, Mexico, and Palestine.[4]

In examining this significant diffusion, it is important to understand why Russian rather than Chinese information controls have spread to certain countries but not others. What makes the controls more likely to spread to different regions? Does it make a difference if one set of controls rather than the other diffuses to a country? How does this international proliferation benefit Beijing and Moscow?

To answer these questions, this paper first establishes an information control typology. The second section applies the typology to the Russian and Chinese approaches to information controls. The third section sheds light on how diffusion is measured. The fourth section is dedicated to illustrating the causes of diffusion. The fifth section traces and analyses the international diffusion of Chinese and Russian technology, including the imitation of techniques, laws, and training. The sixth section of the paper identifies the political, economic, and intelligence advantages that China and Russia gain from exporting their information

Map 1: Diffusion of Russian and Chinese information controls.



controls as well as the impact that diffusion has on importing countries. The paper's conclusion offers recommendations on how democracies can mitigate the potential abuse of information control technology in the future.

1. A TYPOLOGY OF INFORMATION CONTROLS

Various scholars have proposed different definitions of information controls. Some thinkers have conceptualized information controls as "actions conducted in and through cyberspace that seek to deny, disrupt, manipulate, and shape information and communications for strategic and political ends."[5] Others have categorised information controls into fear (i.e. self-censorship), friction (akin to censorship), and flooding (similar to strategic information dissemination).[6] This paper distinguishes itself from these studies by putting surveillance at the core of its concept of information controls and by analysing how surveillance affects other forms of managing information. Information controls can take various forms, including surveillance, censorship, self-censorship, and strategic information dissemination. Different models of information controls emerge once one takes into account the extent to which a country *uses* the various forms of information control and assesses how many *options* (tools) a country has to control information.

Surveillance

Surveillance is essential for a holistic conception of information controls. It enables censorship, self-censorship, and strategic information dissemination. Without surveillance there is no intimidation. Governments do not know which websites to block, and authorities remain unaware of what online conversations need "political guidance."

Surveillance can be observed as well as unobserved. When surveillance is perceived by a population, it can induce self-censorship. Notably, manifestations of surveillance need not actually conduct surveillance to be effective. A government can install fake cameras and still frighten its citizens. Even when surveillance is unobserved by citizens, however, it may still produce effects. Even when unperceived, surveillance can be used to block specific content (censorship) or direct strategic information dissemination at specific targets.

Any theory that omits surveillance when addressing information control is incomplete. Focusing too much on content and what happens *online* (e.g., keyword filtering) fails to account for technology's significant impact on the *offline* world (e.g., physical control through surveillance cameras). In recent years, cyberspace (online) has merged with the physical world (offline). Bits and bytes, 1s and 0s, have become the defining features of everyday objects. In a world where CCTV cameras, smart cities, and other cyber-physical systems are omnipresent, *information control* is therefore increasingly becoming *physical control*. Bruce Schneier, a cybersecurity expert, put it succinctly: "The internet is no longer a web that we connect to. Instead, it's a computerized, networked, and interconnected world that we live in. This is the future, and what we're calling the Internet of Things."[7] A car is now an assembly of computers with steel and wheels attached to it, and everyday tools have now been added to the toolkit of surveillance. Carmakers in China, for instance, send real-time location and other information on electric vehicles to the government.[8] Electric cars are currently a tool for surveillance in today's China, but it is likely only a matter of time before they become a tool of physical control as well. Because the online and offline worlds have merged so much, what a person says, writes, and listens to online is inextricably interwoven with what they "do" in their everyday life (what would have previously been considered the offline world).

Self-censorship

Self-censorship stems from concerns relating to legal and extra-legal (intimidation) punishment as well as the fear of surveillance being used against individuals/entities in the future (e.g., being labelled by authorities as a non-conformist).[9] Although fear can be a major factor driving self-censorship, it does not accompany every act of self-censorship. "There are many reasons why a person may choose to withhold an opinion from a potentially hostile audience, such as attempting to avoid an argument, concerns about offending someone or hurting their feelings, potential retribution such as losing one's job or risk of physical assault, or concerns about appearing to be deviant."[10] For the purposes of this paper, self-censorship is defined as the "withholding of one's true opinion from an audience perceived to disagree with that opinion."[11] The more surveillance tools a government has at its disposal, the more avenues it has to nudge its population towards self-restraint.

Censorship

Censorship, "the suppression *by others* [emphasis in original] of the communication of viewpoints perceived by those others to be considered hostile or offensive," can take on various forms.[12] It can be subtle when it comes as an increase in the costs of accessing information, such as slowing down certain online services (e.g., Tor), or downranking undesired political content in search engines.[13] Censorship can also be large-scale and more indiscriminate through the shutting down of social media platforms, cell phone services, or internet connectivity.[14]

Censorship changes with surveillance capabilities. More monitoring capacity means more options to censor. A less sophisticated government may have to resort to network shutdowns to restrict information. A more sophisticated government, on the other hand, can choose instead to make information less accessible by downranking critical content.

Strategic information dissemination

Strategic information dissemination entails governments' use of *propaganda* and *disinformation* to manipulate public opinion on a strategic level. Here, the term propaganda means "publicly disseminated information that serves to influence others in belief and/or action," while disinformation is understood as "false information that is knowingly disseminated with malicious intent.[15] In the context of this paper, an example of disinformation is Russia's fabrication and dissemination of the "news" that AIDS was a result of U.S. government experiments.[16] An example of propaganda is the Chinese government's use of microblogs,[17] which are usually used to share pictures, videos and texts. A popular microblogging platform is Sina Weibo.[18] Like with censorship, strategic information dissemination can change with the surveillance capabilities of the disseminator. The more a country knows about its citizens, the more options it has to manipulate them.

Extent of use

The extent of use of different forms of information controls often depends on context-specific factors. To some extent, countries are restricted by the tools at their disposal. Russia, for instance, has fewer options than China to impose stringent censorship online, because it has a technologically less sophisticated internet monitoring infrastructure.[19] It therefore relies predominantly on intimidating its population (e.g. by imprisoning opposition candidates) and manipulating the public through propaganda and disinformation. Russia's reliance on these techniques may be because they require less technological sophistication.

Options

A country's surveillance capabilities define the number of information control options that are available to authorities. For example, a country that uses spyware to infiltrate mobile phones may have access to information that it can use to intimidate opposition figures. Yet without deep packet inspection technology (used for online filtering and surveillance), other information likely remains inaccessible – limiting the country's ability to target other dissidents. More surveillance capabilities do not necessarily translate into more effective information control, but authorities with sophisticated surveillance technology can choose from a wider toolkit to enforce information controls. Including surveillance as part of the information control typology thus allows for more robust comparisons of information controls between countries. China, for instance, has more surveillance capabilities than Russia and therefore has more options to implement information controls; the paper discusses this further in the next section. Hence, the amount and diversity of surveillance tools is a major factor in understanding the distinctness of the Chinese and Russian models of information control.

Together, surveillance, self-censorship, censorship, and strategic information dissemination constitute mechanisms and forms of information control. How strongly a country relies on each mechanism, coupled with how many options it has to implement them, defines its information control model.

The following section shows that Russia relies on pervasive surveillance, self-censorship, and strategic information dissemination to retain domestic stability, whereas China predominantly uses censorship and strategic information dissemination, underpinned by extensive surveillance. Overlaps between the two control models exist. To some extent, like Russia, China also propels self-censorship through regulations that require real name registration on online platforms and the incarceration of VPN owners.[20] And Russia, like China, also relies on censorship through its list of banned websites.[21]

2. THE CHINESE AND RUSSIAN MODELS OF INFORMATION CONTROL

When comparing the Russian and Chinese information control models, it is useful to examine the extent to which they rely on various mechanisms as well as how many tools are available to implement them.[22]

Russia's approach

Surveillance

Russia started laying the legal foundations for its extensive surveillance framework in 1995 with the Law on Operational Investigations, which allowed the Federal Security Service of the Russian Federation (FSB) to operationalise its online surveillance system — also known as SORM, the System for Operative Investigative Activities.[23] SORM-1 focused on intercepting phone and mobile calls. To cope with increasing internet penetration, SORM-2 was set up to monitor internet traffic. Later, SORM-3 added more

capabilities to the existing surveillance system, such as monitoring of social media and Wi-Fi.[24]

Self-censorship

In the early 2000s, the new Information Security Doctrine of the Russian Federation was developed, which framed information security as a matter of national security.[25] Further restrictions followed, such as the blogger's law in 2014, the anti-encryption law, also in 2014, and a law requiring data storage to be localised within Russia in 2016.[26] These laws were intended to showcase Russia's pervasive surveillance to its citizens and induce self-censorship.[27]

At the same time, Russian authorities have also intimidated artists, journalists, technology executives, and opposition representatives. Opposition figure Boris Nemtsov was killed, political activist Alexei Navalny is a regular visitor of the country's prisons, and Pavel Durov, the founder of VK and Telegram Messenger, was forced into exile after increasing pressure from the Russian government.[28] More subtle measures of intimidation have far-reaching effects, too. Russia's state-led discourse, emphasising the dangers of the internet, has been found to increase self-censorship.[29]

Strategic information dissemination

In Russia, the emphasis of propaganda and disinformation is on spreading pro-regime messages.[30] As Gallacher and Fredheim demonstrate, the Internet Research Agency, a Russian troll factory, focuses mostly on creating unifying language at home and divisive language abroad. The messages on Twitter targeted at domestic audiences focus on supporting Russia's engagement in Ukraine and Syria, and emphasising divisions in Western countries. Russian trolls are also very likely to spread content from state media channels, such as Channel One, Russia One, NTV, Komsomolskaya Pravda, and Izvestia.[31] These actions help amplify the Kremlin's strategic information dissemination reach. Bloggers paid by the Internet Research Agency and the *Nashi* youth movement, another organisation spreading propaganda, are largely composed of citizens who are employed covertly.[32] Some of them work full-time, spending twelve-hour shifts at their offices.[33]

Censorship

The Russian government has long paid less attention to censorship. Unlike China, Russia has not been able to create domestic substitutes for foreign media platforms. Russian technology companies fail to reach a sufficient share of the market to allow for an exclusion or replacement of foreign competitors. This includes Russian companies that run app stores, search engines, or social media platforms.[34]

Furthermore, Russia does filter online. It has a national blocklist and uses advanced surveillance capabilities, such as deep packet inspection technology, to do so.[35] Filtering, however, is less pervasive than in China. Alexei Navalny's YouTube channel, for instance, is allowed to operate despite his critical stance on the Kremlin.[36]

Recently, Russia has cracked down more harshly on its online environment; it attempted to block Telegram Messenger, but large parts of the Russian internet became unavailable because of the government's crude methods.[37] Telegram Messenger is still available in app stores, and the government has been notoriously ill-equipped to block it. This illustrates Russia's lesser sophistication in blocking than China, which is implementing censorship far more seamlessly and covertly. In 2017, amendments to a law were passed that were intended to restrict the usage of VPNs, but despite these new regulations, a plethora of circumvention apps are still available at the Apple Store and Google Play Store in Russia.[38]

China's approach

Surveillance

Compared to Russia, China has more options to monitor its citizens, because surveillance equipment is pervasive in modern Chinese society. In Xinjiang, for example, citizens are constantly monitored through a combination of intrusive apps, facial recognition cameras, and other types of technology.[39] Surveillance equipment has been deployed widely across society. This is visible in the Chinese education system, where pupils are monitored through facial recognition systems in classrooms and their whereabouts are traced by bracelets that record their geolocation.[40] Although this monitoring is carried out by schools, the government supports such deployments through the "intelligent education" initiative.

The government's initiatives encourage private actors in the surveillance apparatus to nudge people towards self-censorship. Private actors therefore play a complementary role in China's surveillance endeavours. Research has shown that such constant exposure to monitoring can induce self-censorship.[41] It is expected that similar effects take place in China due to the existence of extensive surveillance.

Censorship

The most prominent example of censorship in China is its Great Firewall, which bars Chinese citizens from accessing Google, Facebook, and Twitter. Within China, thousands of censors in the government and in private companies sift through masses of information to identify new keywords

to ban.[42] A significant portion of this censorship is still performed manually, but some tasks are now automated, such as known-keyword blocking.[43] At some point Ray Bradbury's question, posed in *Fahrenheit 451*, will come again to the forefront: "Do you ever read any of the books you burn?"[44] Or paraphrased, do censors read the content they censor? In the future they might not, as a large part of this task may become automated through artificial intelligence. Recently, China has increased censorship even for the elites and technology-savvy citizens who try to access foreign websites. Several legal measures have led to the elimination of non-government-approved VPNs from app stores, which has resulted in extremely limited availability of VPNs in China's two major app stores, the Apple Store and Tencent App Store.[45]

Strategic information dissemination

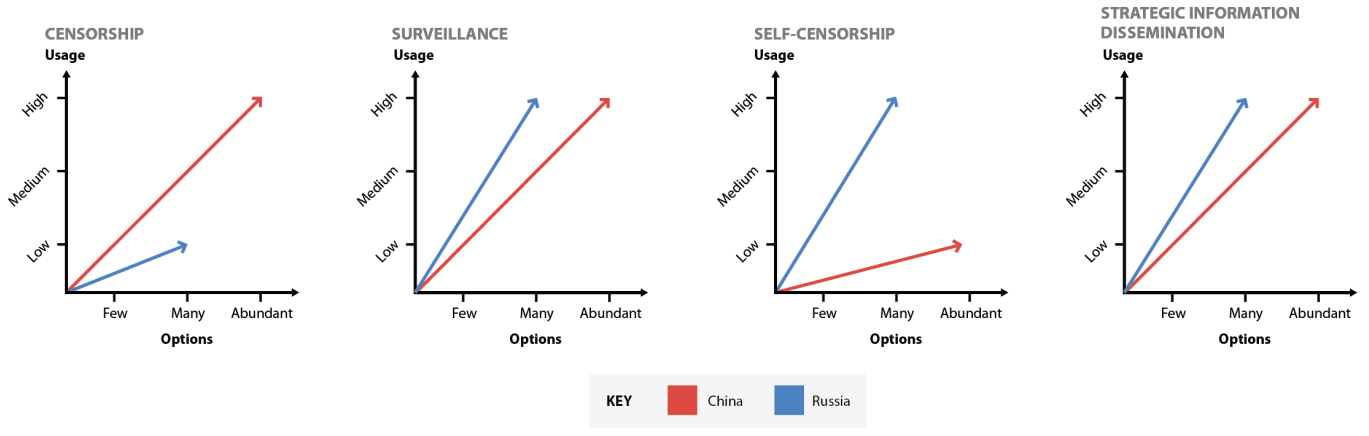
As in Russia, the strategic distribution of information plays a significant role in the Chinese government's strategy to distract from politically sensitive topics. In China, the goal is not to engage in controversial topics, but rather to steer content away from controversy and towards pro-government posts.[46] As far back as 2004, Chinese authorities employed people to sway public opinion online.[47] They recognised that it was not enough to decide what information is available; it is also important to shape the information that remains online. To achieve this, authorities tasked thousands of internet commentators with posting. Those were dubbed the 50 Cent Party.[48] It is estimated there are now up to two million such employees, creating around 450 million posts per year.[49]

The Russian and Chinese systems of strategic information dissemination share similarities. Both post pro-regime messages and seek to steer discussions away from contentious topics, and neither look to engage in meaningful discussions about politics. The 50 Cent Party appears to be composed predominantly of government employees, posting on the side-lines of their job, who are complemented by volunteers such as the youth members of the Communist Party, who are organized in the Volunteer Campaign to Civilise the Internet to post patriotic content free of charge.[50]

Self-censorship

Inducing self-censorship through intimidation was a widespread technique during the Mao era in China. Since then, however, methods have shifted towards information control based on censorship and strategic information dissemination.[51] The Chinese government is currently fostering self-censorship at the elite level, while employing censorship and strategic information dissemination to deal with the general population (these strategies work best to control the average citizen).[52] Examples of measures that induce self-censorship include the arrest of a man who provided VPN services (as a warning for other VPN providers), or the regulation making real-name registration of influencers on social media mandatory.[53] To further encourage self-censorship, Chinese internet laws are often left intentionally vague to create ambiguity as to what is punishable and what is not.[54]

Graphs 1 – 4: Chinese and Russian information control models.



3. METHODOLOGY: MEASURING DIFFUSION

In this paper, the diffusion of Russian and Chinese information control technology and techniques is traced through open-source research, including data gathered from company reports, technical network measurements, newspaper and journal articles, and government-issued laws and regulations.

Diffusion is measured through three indicators: technology, imitation, and training. The purpose of using these three indicators is to measure the breadth and depth of the spread of China's and Russia's tactics to other nations. The breadth can be seen in how many countries get exposed to at least one of the indicators. The depth of diffusion can be seen in how many indicators one single country adopts. If a country adopts only one indicator of diffusion, it is deemed to be located at the periphery of a technosphere. If a country checks the maximum amount of indicators (two indicators for Russia, three for China),[55] the diffusion is deemed to be profound, and the country is located at the core of the technosphere.

Indicator 1: Technology

The first indicator of diffusion is technology. For the purpose of this paper, I focused on Chinese and Russian surveillance and censorship technology exports to entities abroad that control large numbers of people or public buildings and are assumed to be operated primarily by the police or other government authorities. Examples of this type of technology include cameras installed in prisons, harbours, cities, railway stations, airports, and filtering equipment deployed by Internet Service Providers abroad. This indicator, however, does not encompass projects where it is assumed that the police or government are not the primary operators of a surveillance system, such as Hikvision's CCTV provision for a Japanese public university.[56]

In addition to observing surveillance exports through company statements and media articles, I identified a chosen set of surveillance middleboxes via network measurements in cooperation with Vasilis Ververis, Nguyen Phong Hoang, and Marios Isaakidis.[57] OONI Explorer and Censys were used to find Huawei middleboxes that have the fingerprint "V2R2C00-IAE/1.0." This fingerprint or header was associated with Huawei's eSight product, which is able to analyse network traffic and discover IpSec VPN services – allowing it to be used to monitor and censor traffic.[58] An inspection of OONI Explorer and Censys's data revealed Huawei middleboxes in use in Colombia, Cuba, Italy, Mexico, Nigeria, Pakistan, Spain, and Turkey.[59]

Indicator 2: Imitation

For the purpose of this paper, imitation is defined as the replication of Chinese or Russian information control laws and techniques by another country. An example is Uzbekistan copying Russia's law on state surveillance;[60] or Tanzanian and Zimbabwean government officials announcing that they intend to mimic China's replacement of foreign online content providers with homegrown ones to exert greater control.[61] Data gathered in this paper suggests that imitation very rarely (if ever) occurs without concurrent diffusion of technology and training, while technology and training can sometimes be the only indicators diffusing. Thus imitation demonstrates deep diffusion. Notably, all countries that imitate Russia or China are within their respective core technospheres.

Indicator 3: Training

Two types of training are included for this indicator: first, training of law enforcement, government officials, and private companies (which often implement information controls for governments) and second, training of journalists. The former group is educated in how to broaden its access to information on citizens (digital forensics, safe-city projects) or how to implement censorship more efficiently. All smart-city implementations or selling of deep packet inspection technology come most certainly with some kind of training of how the techniques work. This paper, however, includes only those cases where documents specifically mention that training was provided to a given country. A news report about Huawei implementing a safe city in Spain, for instance, does not qualify as training.

The second group, overseas journalists in China, may remain unnoticed by governments, as some of these trainings are handled by private institutions or news organisations. The trainings are aimed at increasing positive coverage of China abroad. As many cases demonstrate, they reach these intended political effects.[62]

> "Training" is a word that can be easily misinterpreted. In the Western world, it would typically mean bringing someone to a certain standard of proficiency, and would probably be academic in nature. However, in China, media trainings are in actuality free public-relations trips to China that follow a conveniently pro-government agenda…. Such efforts in the media sector are central to the Chinese soft power strategy. Therefore, China's intent to "train" hundreds of Latin American journalists in the years to come is probably best understood as a way of exposing influential opinion makers to Beijing's propaganda."[63]

Furthermore, journalist trainings often contain practical exposure to the implementation of information control methods. The Baise Leadership Academy in Guangxi, which is run by the Guangxi Communist Party's Personnel Unit, is a flagship example of this. Officials and journalists from Southeast Asia are trained there on how to "guide public opinion" online.[64]

4. CAUSES OF INFORMATION CONTROLS DIFFUSION

The following section is dedicated to providing empirical diffusion data as well as an analysis of why some countries rather than others more readily imitate, buy technology, or undergo training than others. Based on the empirical data provided in Appendix A, this paper argues that regime type and the extent of interconnectedness between countries explains why information control diffusion is more likely to occur in some cases than others.

Explanatory variable 1: Regime type

When it comes to tracking diffusion indicators, regime type is a key variable for imitation – but it holds less explanatory power for technology and training. In this paper regime type is defined according to the Economist Intelligence Unit's *Democracy Index*, which distinguishes between democracies, hybrid regimes, and authoritarian regimes.[65] Data gathered in this study shows that authoritarian and hybrid regimes are more readily imitating Russia and China. Out of the 19 countries found to be imitating China or Russia (this includes Russia mimicking China and vice-versa), 58 percent are authoritarian, and 37 percent are hybrid. Just 5 percent are democratic.

Why are hybrid and authoritarian regimes more likely to imitate China and Russia? One reason might be that autocratic countries tend to be more willing to learn from each other because they face similar threats to regime survival.[66] This inclination leads to the sharing of various techniques and policies among autocracies. Already in 1848, autocrats of different polities discussed and shared techniques on how to counter revolutionary tendencies in Europe. Likewise, during and after the Arab Spring in the early 2010s, autocrats engaged in "elite learning," which allowed them to develop more informed policies. While in some cases assistance between autocrats is more subtle, such as knowledge transfer, it can be also blunt and overt. This was the case in Bahrain in 2011, where Saudi Arabia actively helped to crush dissent.[67]

Regime type provides less explanatory power with regards to the technology and training indicators. Although authoritarian or hybrid regimes make up a large number (56 percent) of the countries that have adopted information controls from China and Russia, they are not alone. Democracies are also likely to buy technology or undergo training, and comprising 37 percent of countries to which information controls diffused.[68] This may be because surveillance technology is seen as more compatible with democratic values, because it can be used for purposes that democracies consider "legitimate." Similarly, receiving training from China in digital forensics or for journalistic coverage may not be perceived as necessarily damaging to democratic values.

Furthermore, many of the technologies being imported are dual-use in nature. For example, democracies, such as Argentina, Brazil, France, Germany, Italy, and Spain, have imported surveillance technology that could be used to suppress street crime in "smart cities."[69] This technology, however, could also be misused to prevent protesters from gathering.

Despite the belief that democracies will not abuse surveillance equipment, the potential for misuse is tangible. Sophisticated surveillance technology always creates cause for concern. Authoritarian and illiberal practices are commonly employed in democracies as well.[70] Prominent examples include Donald Trump's United States, Victor Orbán's Hungary, or Rodrigo Duterte's Philippines.[71] Furthermore, accidental misuse is already present through biases in technology. Microsoft, for instance, declined a request by a Californian law enforcement authority to provide its facial recognition capabilities for officers' body and car cameras. The company feared that its technology could affect minorities unfairly, because the algorithms had been trained on predominantly male and white training sets.[72]

Citizens from democracies, such as Australia, Indonesia, the United Kingdom, and the United States, have also been involved in a variety of trainings by Chinese entities.[73] Individuals from the United Kingdom, for instance, have undergone training by Meiya Pico in digital forensics methods and journalists from the U.S. and Australia have visited China for study trips.[74]

Explanatory variable 2: Interconnectedness

Bilateral economic, political, historical, and social interconnectedness between political entities may explain why Chinese and Russian information controls are more likely to diffuse to certain countries than others. The stronger the degree of interconnectedness between Russia/China and another country, the more likely it is that information controls will spread. This finding is similar to – but distinct from – Levitsky and Way's concept of linkage, which also builds on the density of ties between countries

to build hypotheses in regards to diffusion of democratic practices.[75] In their studies, the two authors examine the concept of linkage with regards to the ties between the West and certain authoritarian-leaning regimes in the post–Cold War era. Wherever high linkage was present, they found democratization was more likely to occur.[76] Scholars such as Ambrosio and Weyland have also considered the argument of linkage and geographical closeness in the context of authoritarian diffusion.[77] The argument of this paper builds on the work of these scholars, but also substantially differs in key areas.

Levitsky and Way, for instance, claim that the most important factor for the establishing of strong bonds between countries is geographical closeness.[78] China, however, has become more interconnected further abroad – likely due in part to the country's economic rise. Overseas financing is an illustrative example. A list of official Chinese financing of different regions is topped by Africa, followed by Central and Eastern Europe (including Russia), and Latin America.[79] Only after these regions do South Asia, Southeast Asia, and Central and Northeast Asia appear on the list. The data presented in this paper on information controls diffusion depicts this trend as well. Although Russia's information controls have diffused most deeply to countries that are part of the Commonwealth of Independent States, many of the other countries to which Russian information controls have diffused are not Russia's neighbours. China's information controls have also diffused broadly and deeply across the world, weakening the hypothesis that geographical closeness is the strongest factor in the establishing of interconnectedness, which in turn propels information controls diffusion.

Levitsky and Way also note that leverage, "or the degree to which governments are vulnerable to external democratizing pressure," can explain a change in a country's policies and practices.[80] Given this, in the process of diffusion of information controls, one would imagine democratic governments pressuring countries to not import information controls. Because information control technology is dual-use in nature and propaganda trainings are being labelled as media trainings, though, it is unlikely that democracies are able to criticize such exports without sounding hypocritical. After all, democracies are major exporters of similar products themselves, and are also recipients of information control trainings from China.[81] Furthermore, one could imagine China and Russia exercising leverage over countries to import their information controls, though the use of leverage of China and Russia over countries to adopt such technology and techniques has not been observed during this paper's research process. In the end, the data presented in Appendix A indicates the major reason behind diffusion is unlikely to be leverage, i.e., external pressure, through sanctions, threat of military force, or aid withdrawal. Instead, it is more plausible to assume that there is a vivid demand for such equipment and techniques.

This paper therefore proposes the term "interconnectedness" to shed light on the causes behind the international diffusion of information controls. It examines the explanatory variable together with the regime type variable (discussed above) in order to assess the likeliness of information control diffusion (See Table 1).

Proxies for interconnectedness

In this paper, the Belt and Road Initiative (BRI) and the Commonwealth of Independent States (CIS) are considered to be alternative measures demonstrating strong interconnectedness with China and Russia. Countries that are involved with both or either organisation/initiative, are more likely to use Chinese or Russian information controls. This is so because the BRI and CIS are essentially proxies for substantial economic, diplomatic, technocratic, social, information, and civil society ties between China and Russia on the one hand and the other countries involved on the other hand. A number of factors contribute to this alignment. First, both initiatives go back to historical

Table 1: Measuring diffusion.

	Russia/China	**Russia/China**	**Russia/China**
Explanatory variable	Interconnectedness	Regime type / interconnectedness	Interconnectedness
Indicators of diffusion	Filtering or surveillance technology	Imitation of laws and techniques	Training of government/law enforcement officials / private companies, or journalists to share techniques
Breadth and depth of diffusion Country X C(1), R (2)	The breadth "Country X" and depth "C(1) R(2)" of diffusion are indicated in the left sidebar		

narratives, which presume tight interconnectedness between China/Russia and the other countries. The BRI relies on the revival of ancient silk trading roads.[82] The CIS, on the other hand, builds on the tradition of the former Soviet Union and acts as a continuation of those ties. Second, both initiatives receive active commitment from Russia and China. Russia frequently engages in Eastern Europe and Central Asia, which it sees as part of its sphere of influence, and China encourages the exchange of ideas, goods, and social interactions along the BRI (these interactions are formally enshrined in bilateral Memorandums of Understanding).[83] China also weaves journalist and media trainings into the BRI framework.[84] The selling of technology and services is also integrated into the BRI. On the one hand, Chinese companies are trying to find new export markets in search of profit. On the other hand, foreign trade is to some extent coordinated with the government. Meiya Pico, a Chinese cybersecurity company, was instructed by the Chinese Ministry of Public Security to train countries affiliated with the BRI in digital forensics (See Image 2). Meiya Pico may also be part of establishing a Safety Corridor from China to Europe, aiming to tie security and safety services and products to international development projects.[85] The Safety Corridor is currently planned to cover Kazakhstan, Russia, Belarus, Poland, Germany, and the Netherlands.[86]

Image 1: Retrieved from Meiya Pico's website on 1 May 2019. Illustrates the planned strategic Safety Corridor project.[87]

Image 2: Meiya Pico was instructed by the Chinese Ministry of Public Security to train countries of the Belt and Road Initiative in digital forensics. This image, which was retrieved on 29 April 2019, depicts nineteen countries.[88]

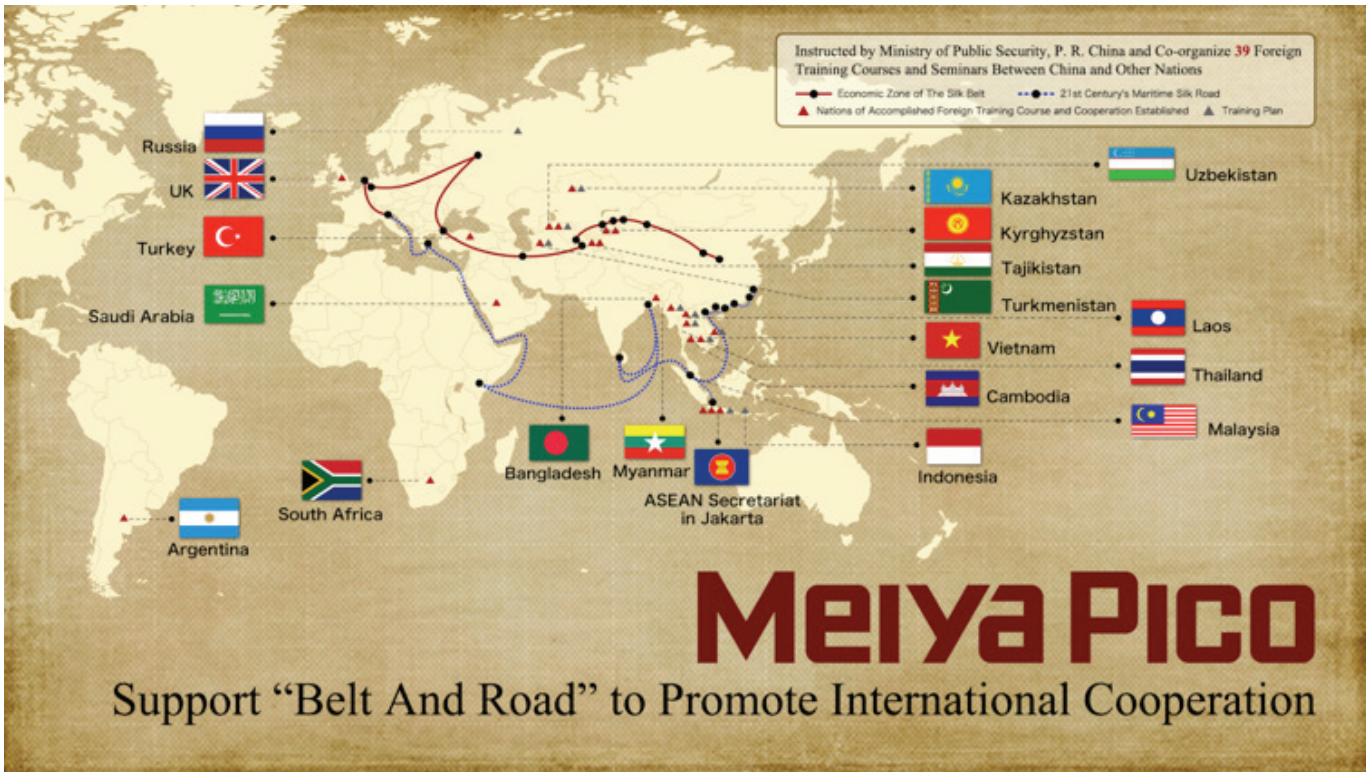


Image 3: This image, which was retrieved on 5 September 2019, shows twenty-nine countries. The reference to the Ministry of Public Security (See Image 2) on the top right-hand side of the image was removed by Meiya Pico.[89]

5. BEIJING AND MOSCOW'S CORE TECHNOSPHERES

The following section highlights how a strong degree of interconnectedness results in profound diffusion and the creation of a core technosphere. Countries that are less interconnected to Russia and China, like those that are not part of the BRI or the CIS, are less likely to experience extensive diffusion of information controls. They remain at the periphery of the Russian and Chinese technospheres.

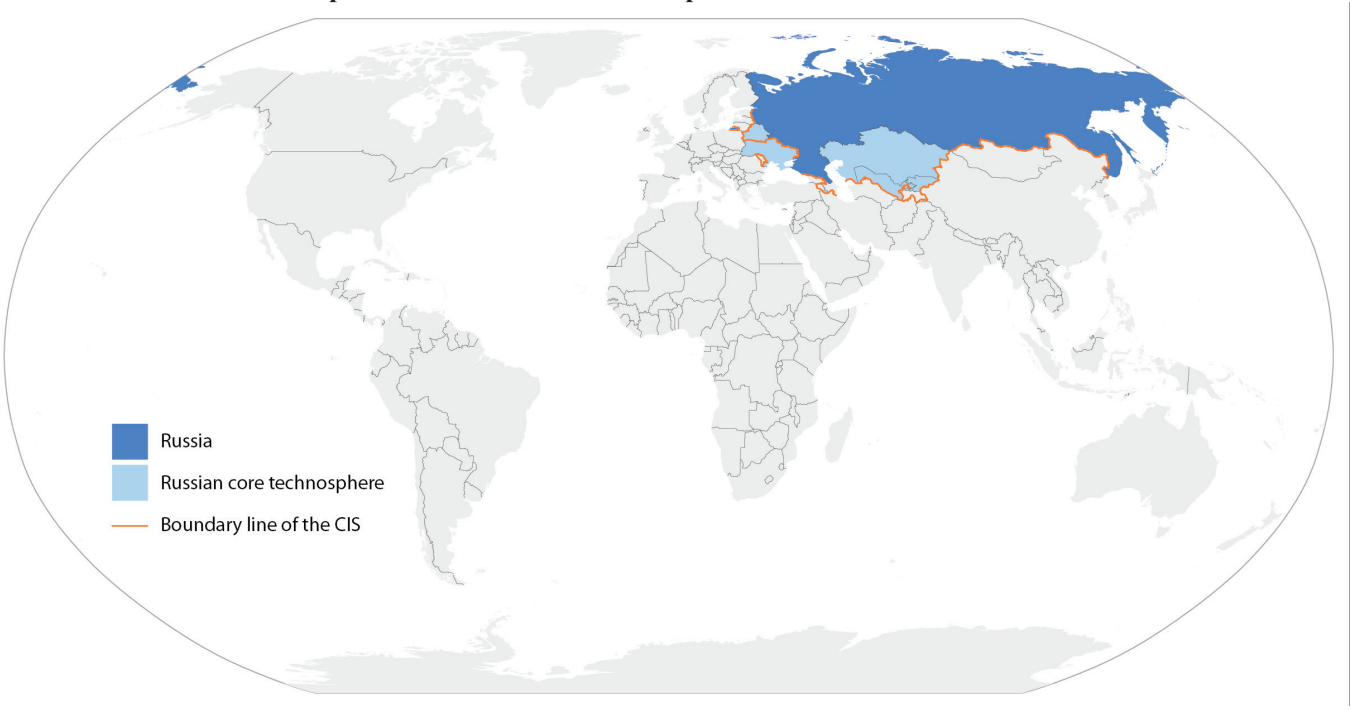
The Commonwealth of Independent States

The CIS was established after the dissolution of the Soviet Union in December 1991 and was created to encourage continuing cooperation between Russia and the newly formed countries. It involves political, economic, and cultural cooperation between the member states, which include Armenia, Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Tajikistan, and Uzbekistan. Ukraine was initially part of the CIS, but withdrew in 2018.[90]

Research for this paper found Russian information controls diffused to 28 countries that are as geographically varied as Palestine and Mexico. Countries from the CIS account for 25 percent of Russian information controls exports (7 out of 28 countries).[91] Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Ukraine, and Uzbekistan are at the core of the Russian technosphere. Each of these countries are, or have been, part of the CIS at some time and have imitated Russian laws with regards to online surveillance. Many surveillance laws in CIS countries create an atmosphere of doubt and allow room for the intimidation of dissidents, thereby replicating Russia's approach to information control. The laws and the environment of fear, however, would be less powerful without the surveillance technology provided by Russia.

In Belarus, the Ministry of Internal Affairs purchased technology from Analytical Business Solutions, a Russian firm that specialises in increasing the efficiency of online monitoring.[92] The Belarusian government has imitated Russian law and most likely purchased SORM surveillance equipment from Russia.[93] Kazakhstan bought deep packet inspection technology from VAS Experts, a company based in St. Petersburg.[94] It also acquired monitoring tools from iTeco, SORM technology from MFI-Soft, and Protei, audio forensics tools from Speech Technology Center, and mobile forensics from Oxygen Software.[95] The Kazakh Ministry of Emergency Situations also acquired Semantic Archive, an information analysis platform provided by Analytical Business Solutions.[96] Kyrgyzstan bought SORM equipment from Oniks-Line and Signatek.[97] Ukraine also acquired SORM equipment.[98] Uzbekistan imported deep packet inspection technology from VAS Experts and Protei, SORM equipment from MFI-Soft, audio forensics from Speech Technology Center, and mobile forensics from Oxygen Software.[99] The Uzbekistan government also instituted a law mimicking Russia's law on state surveillnce.[100]

Map 2: The Russian core technosphere moulds to CIS frontiers.



The Belt and Road Initiative

The Belt and Road Initiative was officially launched in 2013 and comprises 138 countries; 82 percent of Chinese information controls exports go to BRI countries (84 out of 102 countries).[101] The Initiative consists of the Silk Road Economic Belt, which connects China and Europe over land, and the 21st Century Maritime Silk Road, which aims to revive old maritime trade routes.[102] These land and maritime routes are also complemented by a Digital Silk Road, which seeks to tie other countries to China through cooperation in the digital realm.

This sub-section of the paper examines ten countries — all part of the BRI — where information controls have diffused most deeply (based on the three indicators of diffusion). These countries comprise the core of China's technosphere.

China's influence in Egypt is strong. Regarding the transfer of surveillance technology, Huawei built a safe city in the country and Hikvision supplied CCTV cameras for the Suez Governate's bus fleet.[103] Alongside these technology transfers, Egyptian journalists have visited Beijing for ten-month long media fellowships, organized by the China Public Diplomacy Association. There they were exposed to an autocratic media landscape through visits to media houses like the People's Daily.[104] Egyptian officials, for their part, visited Meiya Pico to learn about digital forensics.[105] Cooperation between Egypt and China is more profound, however. In 2014, Egypt signed a cybercrime-fighting treaty with China.[106] Four years later, Egypt passed a cybercrime law for regulating social media that mimics China's way of handling social media platforms.[107]

Iran has also been crucially influenced by China's use of information controls. One of the earliest surveillance equipment exports to Iran was Huawei's sale of gear that gives government agencies access to mobile phones.[108] ZTE, another Chinese company, also sold surveillance equipment into Iran that could be used to intercept citizens' communications.[109] This technological cooperation was complemented by a 2014 meeting between Chinese and Iranian state officials where it was agreed that China would help Iran with the implementation of Iran's National Information Network.[110] In turn, Iran has been very open about learning from China. Iran's development of the Soroush messenger app mirrors China's domestic ecosystem of apps that allows for government access.[111] And the head of Iran's Information Technology Organization lauded China for its "four decades of good experiences in the application development of services for information technology," and noted, "We hope to use these experiences."[112]

Malaysia is another country situated at the core of China's technosphere. Malaysia's journalists have received training in Beijing, which was supported by the Chinese Ministry of Foreign Affairs, the Ministry of Education, and Huaneng Industry, a state-owned company.[113] According to a professor at the Communication University of China, these experiences "can serve as a blueprint for the trainees to develop media industry in their home countries."[114] Training is not only confined to journalists. Meiya Pico, a cybersecurity company based in Xiamen, organized digital forensics trainings, which allow for the extraction of data from phones and computers, in Malaysia. In doing so, the company states that "as always, Meiya Pico has stuck to the strategy of 'Going Global' and the initiative of 'Belt and Road'."[115] In terms of technology, Malaysia has been an avid buyer of Chinese surveillance technology. It has, for instance, acquired body cameras for its security forces from Yitu, a Shanghai-based company.[116] Furthermore, it acquired an AI-enabled traffic management control system from Alibaba Group to monitor traffic in Kuala Lumpur.[117] The country appears intent on continuing this course, as Prime Minister Mahathir bin Mohamad recently announced that Malaysia will make use of Huawei equipment as much as possible.[118] Additionally, Malaysia's former Deputy Prime Minister, Ahmad Zahid Hamidi, stated that China's sophisticated use of surveillance equipment to monitor every movement is worth imitating.[119]

Russia, for its part, has been keenly imitating China's more sophisticated methods of online content filtering.[120] Filtering specific content, rather than entire websites, reduces the possibility of overblocking. To increase cooperation, the architects of the Great Firewall of China were invited to Russia to share techniques.[121] Chinese training and technology have also diffused to Russia. Russian experts have been trained in digital forensics by Meiya Pico.[122] Huawei's safe city solutions have been implemented in St. Petersburg;[123] Huawei provided a cloud storage solution that was "specially designed for massive video data storage and analysis."[124]

The case of Tanzania provides a good example of how information controls diffuse in a nearly linear way, starting first with technology transfer, followed by training, and eventually progressing to imitation. In 2014, Huawei announced that it had implemented a safe city in Tanzania.[125] The following year, Dahua Technology, a Hangzhou-based company, equipped the Zanzibar Presidential Office with smart cameras that are capable of recognising faces and audio.[126] One year later, the People's Daily reported that Tanzanian journalists participated in a media fellowship programme organized by China's Public Diplomacy Association.[127] In turn the strengthened bonds between Tanzania and China have resulted in the Tanzanian government working to imitate the Chinese concept of censorship. Tanzania's former Deputy Minister for Transport and Communication, Edwin Ngonyani, summed it up well. At a China-Tanzania New Media Roundtable, co-organized by the government of Tanzania and the Cyberspace Administration of China, he declared: "Our

Chinese friends have managed to block such media in their country and replaced them with their homegrown sites that are safe, constructive and popular. We aren't there yet, but while we are still using these platforms we should guard against their misuse."[128]

Thailand is another case where Chinese surveillance technology has been exported successfully. Hikvision took on the task of providing CCTV monitoring for the Thai Ministry of Commerce,[129] as well as supplying Thai police with portable video recorders, which help with real-time recording and remote monitoring.[130] And in cooperation with the Thai police, Huawei is implementing its eLTE Trunking Joint Innovation Project surveillance solution.[131] As is the case in many other BRI countries, Meiya Pico has trained Thai experts in mobile and computer forensics, and Thai journalists have received media trainings in China.[132] Thailand has also signalled that it intends to create its own Great Firewall in the image of China's.[133] Although the initial plans for a single internet gateway have since been scrapped, a recent law went into effect in Thailand mimicking the vague and broad nature of China's 2017 cybersecurity law, allowing for invasive government on-site inspections at companies and individuals' properties in Thailand.[134]

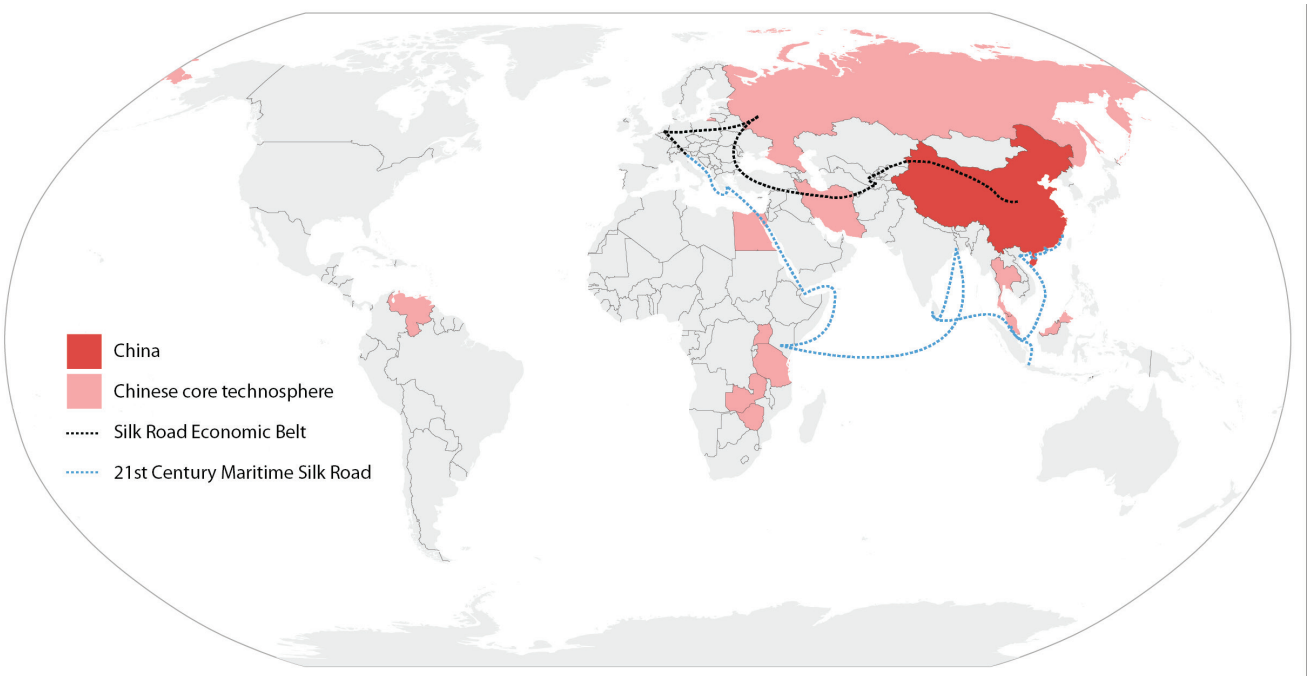
Uganda's information control collaboration with China is far-reaching and steadily progressing. In 2017, Ugandan officials travelled to Beijing and met with representatives of the China National Electronics Import & Export Corporation (CEIEC), a state-owned company. The two parties agreed that CEIEC would help Uganda to monitor social media and other "cybercrime"-related services.[135] That same year, Ugandan journalists completed a ten-month-long media training at the China Africa Press Center in Beijing, organized by the China Public Diplomacy Association.[136] The following year, Huawei delivered 900 surveillance cameras to facilitate the Ugandan government's smart policing programme.[137] The Shenzhen based company also assisted the government access of the encrypted communications of opposition figures.[138] Finally in June 2019, the Uganda Communications Commission revealed a draft internet regulation. The measure is intended to centralize control over the international information flows that enter and exit the country. The move is similar to Thailand's attempts to create a single international internet gateway. According to an insider of the Ugandan regulatory process, "it will be like turning the Internet in Uganda into something like China where it is centrally controlled and you can put one system at the centre of it all to control everything."[139]

The extensive interconnectedness between Zambia and China reveals that the African country is positioned at the core of China's technosphere. In order to control its domestic population, the government of Zambia has relied on censorship and surveillance gear supplied by Huawei and ZTE.[140] Huawei employees allegedly aided the Zambian government intercept the digital communications of journalists and opposition groups.[141] Huawei also implemented a smart city to increase Zambia's physical surveillance capabilities.[142] In addition, the media landscape of the country has been influenced by Zambian journalists who have attended media trainings in China.[143] In the words of a Zambian minister, Zambia is now following "the China way" of managing the internet.[144]

Zambia's neighbour to the south, Zimbabwe, has long collaborated with China on information control. As far back as 2005, China was reportedly discussing selling communication interception equipment to Zimbabwe, and since then it is suspected that Chinese gear has been used to jam radio broadcasts.[145] These instances were some of the first examples of China exporting censorship technology, which China has refined since then. In addition to inhibiting broadcast content, several Chinese companies have also provided surveillance gear. Hangzhou-based Hikvision partnered with Zimbabwe's Nations Hardware and Electrical to implement broader CCTV coverage in the country.[146] Similarly, Cloudwalk Technology Co., is providing facial recognition cameras, which will likely cover railways, airports, and a national facial database, among others.[147] Since at least 2011, Zimbabwean journalists have been trained in information dissemination techniques (steering conversations, managing media in an autocratic environment).[148] Zimbabwe has been imitating China and has been quite frank about it. Zimbabwe has been developing local app equivalents of social media platforms in order to enhance greater control.[149] In 2016, Supa Mandiwanzira, former Zimbabwean Minister of Information Communications Technology, said: "The President [Mugabe] is saying let us do something about it and we are doing something about it. He mentioned the example of China which has gone to great lengths to protect the integrity of the internet."[150]

Venezuela is both part of the BRI and at the core of China's technosphere, despite the fact that it is not situated along the BRI land or maritime routes. Deepening ties between China and Venezuela started to emerge under Presidents Hu Jintao and Hugo Chávez shortly before the global financial crisis in 2008.[151] Stronger bilateral cooperation and an increase in interconnectedness also translated into surveillance cooperation between Beijing and Caracas. In 2008, interested Venezuelan Justice Ministry officials visited Shenzhen to learn about a national ID card.[152] In the eyes of the Venezuelan government, the ID card was a project worth emulating. Roughly ten years later, Venezuela is implementing a new smart-card ID, also known as the fatherland card or *carnet de la patria*, with the help of a Shenzhen based company, ZTE. The card includes massive amounts of information including not just birthdays, and family information, but also medical history, social media

Map 3: The Chinese core technosphere extends along BRI trade routes.



activity, political party membership, and whether a person voted in elections.[153] The information included on the cards is used to encourage certain types of behaviour, such as being a good citizen. In other words, China's social credit system, which relies on "big-data collection and analysis to monitor, shape and rate behaviour via economic and social processes" is no longer confined to China.[154] Yet surveillance cooperation between China and Venezuela extends even further. In an effort to give Venezuelan officials more control over their citizens, various smart city projects and thousands of CCTV cameras have been installed across the country by Huawei, ZTE, and CEIEC.[155] As part of this process, Huawei provided training to Venezuelan technical experts on how to operate the system.[156]

Overlapping technospheres

China and Russia share overlapping technospheres in twenty countries. Interestingly, every country found to exist deep within the Russian technosphere also exists partly within China's technosphere. China is active in Belarus, Kazakhstan, Kyrgyzstan, Ukraine, and Uzbekistan. Russia, on the other hand, is present beyond its borders in only one of the countries that constitute China's core technosphere; in Thailand, a Russian company that specialises in audio forensics, Speech Technology Center, has been providing equipment.[157]

6. THE IMPACT OF DIFFUSION

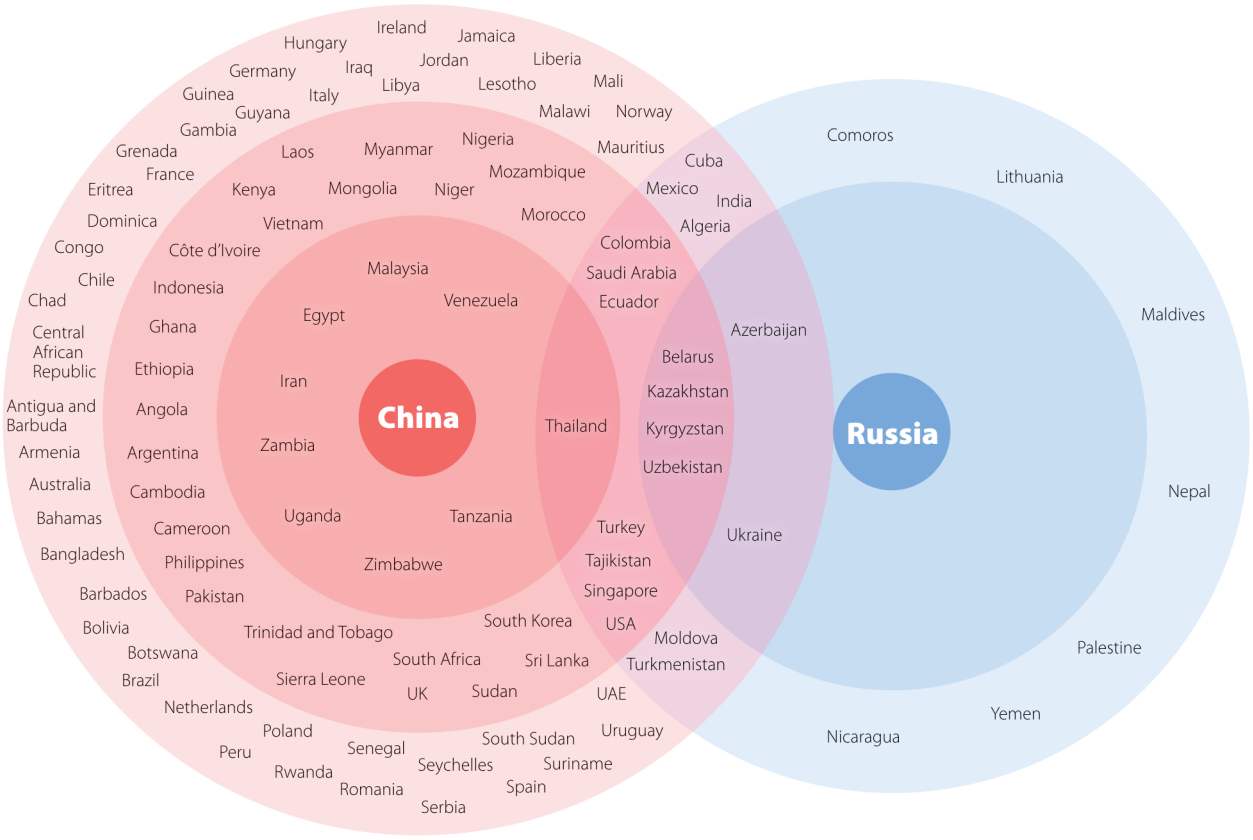
The primary result of the diffusion discussed in this paper is the creation of a technosphere — a geographical area that comes with various advantages for the information controls exporter. These advantages can be categorized as political, economic, and intelligence related. Politically, the proliferation of information controls reinforces autocratic regimes.[158] The widespread adoption of Russia's view of information security, for example, aids the Kremlin domestically in consolidating its legitimacy, because it can point to the fact that its model is being imitated abroad. It also proliferates its system of information control and hence establishes its image as a norm-setter. The training of government officials and journalists socializes leading figures in governments and media abroad into a Chinese understanding of what an authoritarian information environment looks like. One may question the impact of training a few government officials or journalists per country, but training thousands of individuals on a global level may translate into a broader structural change, making countries reliant on equipment and techniques primarily from China. Meiya Pico's Information Security Academy has already trained more than 1,000 overseas law enforcement personnel in digital forensics, and the China Public Diplomacy Association seeks to train 1,500 international journalists per year by 2020.[159]

Image 4: Baise Executive Leadership Academy, where Southeast Asian journalists and officials are trained in Chinese information control.[160]

Economically, the diffusion of information controls creates new markets for exporting nations. In China and Russia, something similar to a military-industrial complex has been created. This security-industrial complex is made up of politicians dependent on security-related industries, private security companies, and the police. Each of these entities/individuals profit from increased security spending at home and exports abroad. Information controls create revenues for Hikvision, Huawei, Protei, VAS Experts, and other surveillance and censorship equipment companies in China and Russia. The export of information control technology is a "win-win" particularly for China. Ecuador, for instance, provides oil to China and receives surveillance-related purchases in exchange. This then creates further employment and revenues in China.[161]

The diffusion of information controls into a technosphere also creates intelligence implications. China, for instance, built the African Union's headquarters in Addis Ababa, Ethiopia, and in doing so allegedly funnelled massive amounts of data from the installed computer systems back to China.[162] It might, in turn, have used this intelligence to better achieve its foreign policy goals on the continent. And in Pakistan, unknown Wi-Fi modules were discovered in CCTV cameras supplied by Huawei. These could have been a potential risk for information exfiltration, which highlights the intelligence benefits that could emerge for a country exporting surveillance products.[163] Notably, China does not appear to be alone in wanting to retain access to exported equipment. The Russian companies that provided surveillance gear to Kyrgyzstan were accused of keeping backdoors into the system, allowing them to continue to obtain information after installation.[164]

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



Increased diffusion also affects the way information controls are implemented and employed around the world. If one takes the example of Zimbabwe, this paper shows that censorship and surveillance technology as well as training in propaganda were the primary exports from China to Zimbabwe. This diffusion does increase Zimbabwe's options to induce fear through surveillance technology as well as its ability to censor and manipulate its public. In other words, the increase in Chinese exports increases the information control *options* available to Zimbabwe. At the same time, the *use* of information controls may have changed with diffusion. Zimbabwe may have chosen to rely on censorship and strategic information dissemination no matter what, but interacting with China has definitely brought the African country closer to adopting that approach in full. The convergence of the Zimbabweans to the Chinese way of managing information is visible in the former voicing that it aims to imitate the latter.

CONCLUSION

This paper covers approximately thirteen years of Chinese and Russian information controls exports. During this period, the nature of the technology that has diffused changed considerably. Initially, mostly crude censorship and surveillance technology diffused internationally. This includes Chinese gear that served to jam radio broadcasts in Zimbabwe and Russian filtering and audio forensics equipment that was provided to countries within the former Soviet Union. Increasingly, however, exports diversified and previous rudimentary tools were refined. Now we are looking at the diffusion of CCTV cameras that use facial recognition technology, a plethora of digital forensics tools, smart national identity cards, intelligent databases for governments, and smart cities.[165]

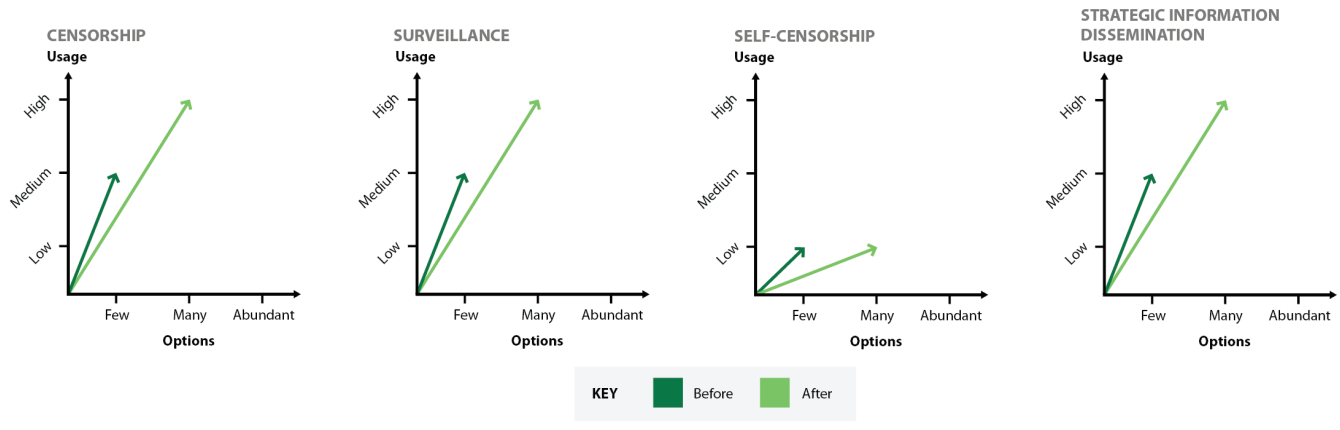
In this fast-changing environment, it is important to trace what is currently being developed and deployed in Russia and China today in order to anticipate what might occur abroad tomorrow. Of course, countries such as Iran, Thailand, and Venezuela develop their own techniques and technology, but the sheer presence of Russian and Chinese information controls in the world serve as an important starting point to identify future trends before they diffuse across the globe.

So, what should democracies do when faced with these trends? Unfortunately, there is no easy answer – in part because it is difficult to prevent the spread of dual-use information control technology and techniques (not to mention the fact that democracies are themselves avid buyers of information control equipment). And when trainings are portrayed as benign rather than conduits for sharing strategic information dissemination techniques they cannot simply be criticized out of hand.

Nonetheless, democracies can still take action. Domestically, democratic countries do not have to deploy all tools that promise more surveillance. Massachusetts is considering legislation to restrict the use of facial recognition.[166] San Francisco has already passed such measures.[167] And when it comes to their own companies that are involved in the production of censorship and surveillance technology, democracies should make sure that they do not abuse human rights or become complicit in such abuse.[168]

Democracies should also work on making individuals'

Graphs 5 – 8: The impact of diffusion on Zimbabwe. The in-depth study of Zimbabwe's information control landscape is outside the scope of this paper; therefore, the graphs depicting the country before and after the diffusion of Chinese information controls are hypothetical. The convergence towards the China model in the process of diffusion, however, is not a hypothetical and is based on the evidence gathered in this paper.



devices and channels of communication more resistant to filtering or surveillance equipment. Yet the opposite is currently the case. Recently, Australia passed a law that extends surveillance and undermines end-to-end encrypted messages, a move often implemented in authoritarian regimes.[169] Canada, New Zealand, the United Kingdom, and the United States intend to introduce similar access points for authorities.[170] Such moves are not necessary for maintaining security. Research indicates that even without access to messages, government authorities still have many avenues to combat crime.[171] End-to-end encryption does not mean "going dark." Metadata, for instance, can be used to tackle crime – and it is often more useful than the content of private messages.

Finally, it should go without saying that in democracies the use of surveillance gear by public authorities should follow a process that is transparent and accountable to the public. For instance, checks and balances should be put into place that prevent access of surveillance equipment by national intelligence agencies when it is meant to be accessed only by local police.[172]

Though none of these suggestions by themselves can stop the spread of surveillance technology around the world, together they can potentially mitigate future abuses.

The global state of freedom of expression and human rights is deteriorating. To date, over one hundred countries have bought, imitated, or been trained by Russia and China in information control. Given this trend, democracies need to serve as a bulwark against authoritarian uses of technology and show the world that it is possible for countries to combat crime and ensure national security without weakening cybersecurity — or the privacy of their citizens. This will certainly not be an easy task, but it is one worth striving towards. For if democracies do not take action, who else will?

ACKNOWLEDGMENTS

I am indebted to Lucas Kello and Joss Wright for their insightful advice and guidance during the various stages of this project. I profited from comments by Irene Poetranto, Gabrielle Lim, Max Kuhelj-Bugaric, Jonas Kaiser, and Dean Jackson. I am also very grateful to the Berkman Klein Center for Internet and Society at Harvard University for having provided me with a vibrant space to think and to the Open Technology Fund and the UK Engineering and Physical Sciences Research Council for generously supporting my research.

APPENDIX A: DIFFUSION TABLE

	Regime type	Filtering or surveillance technology		Imitation		Training	
Countries		**China**	**Russia**	**China**	**Russia**	**China**	**Russia**
Algeria C(1) R(1)	A[173]	X[174]	X[175]				
Angola C(2)	A	X[176]				X[177]	
Antigua and Barbuda C(1)	/					X[178]	
Argentina C(2)	D	X[179]				X[180]	
Armenia C(1)	H					X[181]	
Australia C(1)	D					X[182]	
Azerbaijan C(1) R(2)	A	X[183]	X[184]		X[185]		
Bahamas C(1)	/					X[186]	
Bangladesh C(1)	H					X[187]	
Barbados C(1)	/					X[188]	
Belarus C(2) R(2)	A	X[189]	X[190]		X[191]	X[192]	
Bolivia C(1)	H	X[193]					
Botswana C(1)	D					X[194]	
Brazil C(1)	D	X[195]					
Cambodia C(2)	A	X[196]				X[197]	
Cameroon C(2)	A	X[198]				X[199]	
Chad C(1)	A					X[200]	

	Regime type	Filtering or surveillance technology		Imitation		Training	
Countries		**China**	**Russia**	**China**	**Russia**	**China**	**Russia**
Central African Republic C(1)	A					X[201]	
Chile C(1)	D	X[202]					
China R(1)	A	N/A		N/A	X[203]	N/A	
Colombia C(2) R(1)	D	X[204]	X[205]			X[206]	
Comoros R(1)	A		X[207]				
Congo C(1)	A					X[208]	
Côte d'Ivoire C(2)	H	X[209]				X[210]	
Cuba C(1) R(1)	A	X[211]	X[212]				
Dominica C(1)	/					X[213]	
Ecuador C(2) R(1)	D	X[214]	X[215]			X[216]	
Egypt C(3)	A	X[217]		X[218]		X[219]	
Eritrea C(1)	A					X[220]	
Ethiopia C(2)	A	X[221]				X[222]	
France C(1)	D	X[223]					
Gambia C(1)	H					X[224]	
Germany C(1)	D	X[225]					
Ghana C(2)	D	X[226]				X[227]	
Grenada C(1)	/					X[228]	

	Regime type	Filtering or surveillance technology		Imitation		Training	
Countries		**China**	**Russia**	**China**	**Russia**	**China**	**Russia**
Guinea C(1)	A					X[229]	
Guyana C(1)	D					X[230]	
Hungary C(1)	D	X[231]					
India C(1) R(1)	D		X[232]			X[233]	
Indonesia C(2)	D	X[234]				X[235]	
Iran C(3)	A	X[236]		X[237]		X[238]	
Iraq C(1)	H	X[239]					
Ireland C(1)	D	X[240]					
Jordan C(1)	A	X[241]					
Italy C(1)	D	X[242]					
Jamaica C(1)	D					X[243]	
Kazakhstan C(2) R(2)	A	X[244]	X[245]		X[246]	X[247]	
Kenya C(2)	H	X[248]				X[249]	
Kyrgyzstan C(2) R(2)	H	X[250]	X[251]		X[252]	X[253]	
Laos C(2)	A	X[254]				X[255]	
Lesotho C(1)	D					X[256]	
Liberia C(1)	H					X[257]	
Libya C(1)	A	X[258]					
Lithuania R(1)	D		X[259]				

	Regime type	Filtering or surveillance technology		Imitation		Training	
Countries		**China**	**Russia**	**China**	**Russia**	**China**	**Russia**
Malawi C(1)	H					X[260]	
Malaysia C(3)	D	X[261]		X[262]		X[263]	
Maldives R(1)	/		X[264]				
Mali C(1)	H					X[265]	
Mauritius C(1)	D	X[266]					
Mexico C(1) R(1)	D	X[267]	X[268]				
Moldova C(1) R(1)	H	X[269]			X[270]		
Mongolia C(2)	D	X[271]				X[272]	
Morocco C(2)	H	X[273]				X[274]	
Mozambique C(2)	A	X[275]				X[276]	
Myanmar C(2)	A	X[277]				X[278]	
Nepal R(1)	H		X[279]				
Netherlands C(1)	D	X[280]					
Nicaragua R(1)	A		X[281]				
Niger C(2)	A	X[282]				X[283]	
Nigeria C(2)	H	X[284]				X[285]	
Norway C(1)	D	X[286]					
Pakistan C(2)	H	X[287]				X[288]	
Palestine R(1)	H		X[289]				

	Regime type	Filtering or surveillance technology		Imitation		Training	
Countries		**China**	**Russia**	**China**	**Russia**	**China**	**Russia**
Peru C(1)	D					X[290]	
Philippines C(2)	D	X[291]				X[292]	
Poland C(1)	D	X[293]					
Romania C(1)	D	X[294]					
Russia C(3)	A	X[295]	N/A	X[296]	N/A	X[297]	N/A
Rwanda C(1)	A					X[298]	
Saudi Arabia C(2) R(1)	A	X[299]	X[300]			X[301]	
Senegal C(1)	D	X[302]					
Serbia C(1)	D	X[303]					
Seychelles C(1)	/					X[304]	
Sierra Leone C(2)	H	X[305]				X[306]	
Singapore C(2) R(1)	D	X[307]	X[308]			X[309]	
South Africa C(2)	D	X[310]				X[311]	
South Korea C(2)	D	X[312]				X[313]	
South Sudan C(1)	/					X[314]	
Spain C(1)	D	X[315]					
Sri Lanka C(2)	D	X[316]				X[317]	
Sudan C(2)	A	X[318]				X[319]	
Suriname C(1)	D					X[320]	

	Regime type	Filtering or surveillance technology		Imitation		Training	
Countries		**China**	**Russia**	**China**	**Russia**	**China**	**Russia**
Tajikistan C(2) R(1)	A	X[321]	X[322]			X[323]	
Tanzania C(3)	H	X[324]		X[325]		X[326]	
Thailand C(3) R(1)	H	X[327]	X[328]	X[329]		X[330]	
Trinidad and Tobago C(2)	D	X[331]				X[332]	
Turkey C(2), R(1)	H	X[333]	X[334]			X[335]	
Turkmenistan C(1), R(1)	A		X[336]			X[337]	
Uganda C(3)	H	X[338]		X[339]		X[340]	
Ukraine C(1), R(2)	H	X[341]	X[342]		X[343]		
United Arab Emirates C(1)	A	X[344]					
United Kingdom C(2)	D	X[345]				X[346]	
United States of America C(2), R(1)	D	X[347]	X[348]			X[349]	
Uruguay C(1)	D	X[350]					
Uzbekistan C(2) R(2)	A	X[351]	X[352]		X[353]	X[354]	
Venezuela C(3)	A	X[355]		X[356]		X[357]	
Vietnam C(2)	A			X[358]		X[359]	
Yemen R(1)	A		X[360]				
Zambia C(3)	H	X[361]		X[362]		X[363]	
Zimbabwe C(3)	A	X[364]		X[365]		X[366]	

	Regime type	Filtering or surveillance technology		Imitation		Training	
Countries		**China**	**Russia**	**China**	**Russia**	**China**	**Russia**
Total (out of 110)		73	26	11	8	75	0
Russian diffusion		Russian information controls diffused to 28 countries					
Chinese diffusion		Chinese information controls diffused to 102 countries					
Combined diffusion		Russian and Chinese information controls diffused to 110 countries (this includes the Russian model diffusing to China and vice versa). Information controls were exported to 41 democracies, 24 hybrid regimes, 37 authoritarian regimes. The Economist's regime type database does not provide the regime type of 8 studied countries. Those are Antigua and Barbuda, Bahamas, Barbados, Dominica, Grenada, Maldives, Seychelles, and South Sudan.					

APPENDIX B: LIST OF CHINESE COMPANIES

Company	Type of technology/ involvement	Based in	Reaches
Alcatel-Lucent Shanghai Bell Co.	SORM compatible equipment	Shanghai	Kazakhstan
Alibaba Group	AI-enabled traffic management control system	Hangzhou	Malaysia
Baifendian / Percent Corporation	Big database managing systems powered by AI	Beijing	Angola
CEIEC (China National Electronics Import & Export Corporation	Safe cities	Beijing	Ecuador, Trinidad and Tobago, Uganda, Venezuela
CloudWalk Technology	Facial recognition cameras	Beijing	Zimbabwe
Dahua Technology Co.	Facial recognition cameras	Hangzhou	Tanzania
Hikvision	Facial recognition cameras	Hangzhou	Argentina, Brazil, Egypt, Ireland, Jordan, Myanmar, South Africa, South Korea, Thailand, Ukraine, United Kingdom, Zimbabwe
Huaneng Industry	Supports media trainings	Beijing	Bangladesh, Malaysia
Huawei	Censorship technology, facial recognition cameras, safe cities, helps governments access encrypted communications	Shenzhen	Algeria, Azerbaijan, Belarus, Bolivia, Cameroon, Chile, Colombia, Côte d'Ivoire, Cuba, Ecuador, Egypt, France, Germany, Ghana, Hungary, Indonesia, Iran, Iraq, Italy, Kenya, Laos, Mexico, Moldova, Morocco, Mozambique, Niger, Nigeria, Netherlands, Norway, Pakistan, Philippines, Poland, Russia, Saudi Arabia, Serbia, Singapore, Spain, Tajikistan, Tanzania, Thailand, Trinidad and Tobago, Turkey, Uganda, Ukraine, United Arab Emirates, United States, Venezuela, Zambia
Meiya Pico	Digital forensics and cybersecurity training	Xiamen	Argentina, Armenia, Bangladesh, Belarus, Cambodia, Colombia, Ecuador, Egypt, India, Indonesia, Kazakhstan, Kyrgyzstan, Laos, Malaysia, Mongolia, Morocco, Myanmar, Pakistan, Philippines, Russia, Saudi Arabia, Singapore, South Africa, Thailand, Tajikistan, Turkmenistan, Turkey, Uzbekistan, United Kingdom, Vietnam
SenseTime	Dynamic face recognition people control system	Beijing	Mongolia
Yitu	Facial recognition cameras	Shanghai	Malaysia
ZTE	Censorship technology, safe cities	Shenzhen	Belarus, Ethiopia, Libya, Romania, Senegal, Sierra Leone, Sri Lanka, Sudan, Uruguay, Venezuela, Zambia

APPENDIX C: LIST OF CHINA-RELATED ENTITIES

Entity	Role	Based in	Reaches
Australia – China Relations Institute	Organized journalist study tours to China	Sydney, Australia	Australia
China's Embassy in the Philippines	Media trainings of journalists and officials	Beijing	Philippines
China International Publishing Group	Media trainings of journalists and officials	Beijing	Philippines
China Public Diplomacy Association	Coordinates media trainings	Beijing	Angola, Antigua and Barbuda, Bahamas, Barbados, Botswana, Cameroon, Chad, Central African Republic, Congo, Côte d'Ivoire, Dominica, Egypt, Eritrea, Gambia, Ghana, Grenada, Guinea, Guyana, Jamaica, Kenya, Lesotho, Liberia, Malawi, Mali, Mozambique, Niger, Nigeria, Pakistan, Rwanda, Seychelles, Sierra Leone, South Africa, South Sudan, Sudan, Suriname, Uganda
China – United States Exchange Foundation	Organized journalist tours to China	Hong Kong	United States
Communication University of China	Conducts media trainings	Beijing	Bangladesh, Malaysia
Information Council / State Council Information Office	Sharing of information control techniques with officials and journalists	Beijing	Iran, Philippines
Guangxi Communist Party's Personnel Unit	Operates the Baise Executive Leadership Academy	Guangxi region	Laos, Myanmar, Vietnam
Ministry of Commerce	Media trainings of journalists and officials	Beijing	Philippines
Ministry of Education	Supports media trainings	Beijing	Bangladesh, Malaysia
Ministry of Foreign Affairs	Supports media trainings	Beijing	Bangladesh, Malaysia
Ministry of Public Security	Cooperation on surveillance equipment with Cambodian law enforcement	Beijing	Cambodia
People's Liberation Army Intelligence Division	Training of officials in information controls	Beijing	Sri Lanka
Tsinghua University	Global business journalism programme	Beijing	South Korea

APPENDIX D: LIST OF RUSSIAN COMPANIES

Company	Type of technology/ involvement	Based in	Reaches
Analytical Business Solutions	Tools to analyse open source data in forums and social media platforms	Moscow	Belarus, Kazakhstan
iTeco	Tools to analyse open source data in forums and social media platforms	Moscow	Kazakhstan
MFI - Soft	SORM equipment	Nizhny Novgorod and Moscow	Kazakhstan, Tajikistan, Uzbekistan
Oniks – Line	SORM equipment	Moscow	Kyrgyzstan
Oxygen Software	Mobile forensics	Moscow	Kazakhstan, Uzbekistan
Protei	SORM equipment	St. Petersburg	Comoros, Cuba, Kazakhstan, Palestine, Tajikistan, Uzbekistan
Signatek	SORM equipment	Novosibirsk	Kyrgyzstan
Speech Technology Center (STC) / SpeechPro	Audio forensics / facial recognition	St. Petersburg	Algeria, Colombia, Ecuador, India, Kazakhstan, Maldives, Mexico, Nepal, Saudi Arabia, Singapore, Turkmenistan, Turkey, United States, Uzbekistan, Yemen
VAS Experts	SORM equipment	St. Petersburg	Azerbaijan, Kazakhstan, Lithuania, Nicaragua, Uzbekistan

ENDNOTES

1 Joe Parkinson, Nicholas Bariyo, and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," *Wall Street Journal*, August 15, 2019, sec. Tech, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017; Sheridan Prasso, "China's Digital Silk Road Is Looking More Like an Iron Curtain," January 10, 2019, https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain; Paul Mozur, Jonah M. Kessel, and Melissa Chan, "Made in China, Exported to the World: The Surveillance State," *The New York Times*, April 24, 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html; Andrei Soldatov and Irina Borogan, "Putin Brings China's Great Firewall to Russia in Cybersecurity Pact," *The Guardian*, November 29, 2016, sec. World news, https://www.theguardian.com/world/2016/nov/29/putin-china-internet-great-firewall-russia-cybersecurity-pact.

2 Stabroek News, "China Launches Press Programme to Improve Ties with Caribbean," *Stabroek News*, April 8, 2018, https://www.stabroeknews.com/2018/news/guyana/04/08/china-launches-press-programme-to-improve-ties-with-caribbean/; Irina Borogan and Andrei Soldatov, "Just Business: How Russian Technology Provides the Eyes and Ears for the World's Big Brothers," *OpenDemocracy*, January 25, 2012, http://www.opendemocracy.net/od-russia/andrei-soldatov-irina-borogan/just-business-how-russian-technology-provides-eyes-and-ears-.

3 Jianfeng Zhang, "China-Caribbean Press Center Launched," April 19, 2018, http://english.cctv.com/2018/04/19/ARTIBzkdnQ3Ld2GWuohcBiSd180419.shtml; Fredrick P. W. Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China," *People's Daily Online*, December 2, 2016, http://en.people.cn/n3/2016/1202/c90000-9150101.html; Juan Pablo Cardenal, "China in Latin America: Understanding the Inventory of Influence," in *Sharp Power: Rising Authoritarian Influence* (National Endowment for Democracy, 2017), https://www.ned.org/wp-content/uploads/2017/12/Chapter1-Sharp-Power-Rising-Authoritarian-Influence-China-Latin-America.pdf; Hikvision, "Hikvision's Products Deployed in Military Command of the East in Brazil," April 21, 2010, https://www.hikvision.com/en/Press/Success-Stories/Government/305528967821644; Hikvision, "Total Control for Jordan's House of Parliament," March 31, 2016, https://www.hikvision.com/en/Press/Success-Stories/Government/305528977464530.

4 VAS Experts, "About Us," *VAS Experts*, 2019, https://vasexpertsdpi.com/about-us/; Borogan and Soldatov, "Just Business"; Protei, "Past Events," accessed January 18, 2019, http://www.protei.com/events/past/; Protei, "News and Events - Protei MENA," accessed January 18, 2019, http://protei.me/News-and-Events.

5 Ronald J. Deibert and Masashi Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls," *Global Governance* 18 (2012). p. 339.

6 Margaret E. Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall* (Princeton N.J.: Princeton University Press, 2018).

7 Bruce Schneier, "Click Here to Kill Everyone," 2017, https://nymag.com/intelligencer/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html.

8 Erika Kinetz, "In China, Your Car Could Be Talking to the Government," *AP NEWS*, November 29, 2018, https://apnews.com/c6e610eb8f4645b4806bc16479b64809.

9 Frederick Schauer, "Fear, Risk and the First Amendment: Unraveling the Chilling Effect" (College of William & Mary Law School, 1978), https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=2010&context=facpubs; Marilyn Clark and Anna Grech, "Journalists Under Pressure - Unwarranted Interference, Fear and Self-Censorship in Europe" (Council of Europe, 2017), https://rm.coe.int/168070ad5d; Daniel J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review* 154, no. 3 (January 1, 2006): 477, doi:10.2307/40041279.

10 Andrew F. Hayes, Carroll J. Glynn, and James Shanahan, "Willingness to Self-Censor: A Construct and Measurement Tool for Public Opinion Research," *International Journal of Public Opinion Research* 17, no. 3 (2005): 298–323, doi:10.1093/ijpor/edh073.

11 Ibid.

12 Ibid.

13 Tor is a software that allows for anonymous communication and thereby shields users from surveillance.

14 Jan Rydzak, "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, February 7, 2019), https://papers.ssrn.com/abstract=3330413.

15 Jonathan Auerbach and Russ Castronovo, "Introduction: Thirteen Propositions About Propaganda," in *The Oxford Handbook of Propaganda Studies*, 2013, https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199764419.001.0001/oxfordhb-9780199764419-e-023; Gabrielle Lim, "Disinformation Annotated Bibliography" (Citizen Lab, May 2019), https://citizenlab.ca/wp-content/uploads/2019/05/Disinformation-Bibliography.pdf.

16 Adam B. Ellick and Adam Westbrook, "Operation Infektion: A Three-Part Video Series on Russian Disinformation," *The New York Times*, November 1, 2018, https://www.nytimes.com/2018/11/12/opinion/russia-meddling-disinformation-fake-news-elections.html.

17 Jesper Schlæger and Min Jiang, "Official Microblogging and Social Management by Local Governments in China," 2014, https://journals.sagepub.com/doi/full/10.1177/0920203X14533901.

18 Sina Weibo, "微博–随时随地发现新鲜事," n.d., https://www.weibo.com/login.php.

19 Max Seddon and Henry Foy, "Russian Technology: Can the Kremlin Control the Internet?," *Financial Times*, June 5, 2019, https://www.ft.com/content/93be9242-85e0-11e9-a028-86cea8523dc2.

20 Cyberspace Administration of China, "Internet Forum Community Service Management Regulations," August 25, 2017, http://www.cac.gov.cn/2017-08/25/c_1121541921.htm; Benjamin Haas, "Man in China Sentenced to Five Years' Jail for Running VPN," *The Guardian*, December 22, 2017, sec. World news, http://www.theguardian.com/world/2017/dec/22/man-in-china-sentenced-to-five-years-jail-for-running-vpn.

21 Jakub Dałek, *Russian Blacklist*, Python, (2014; repr., 2018), https://github.com/jakubd/russian-blacklist.

22 This paper examines Russian and Chinese approaches to information control, but there may be also countries that take similar approaches to controlling information without having been directly exposed to Russian/Chinese technology, techniques, or training. These are cases of independent emergence of information control models. For instance, a small island country in the Pacific Ocean may have created a sophisticated legal and extra-legal framework to induce self-censorship within its population, while at the same time, it overwhelms social media fora with pro-regime messages. This does not mean that the country is implementing Russian information controls, but rather that it independently developed to handle information in this way. Other countries, in turn, have found alternative approaches to censoring online space. While India has been exposed to Chinese and Russian information controls, it has notoriously relied on network shutdowns to keep dissent at bay, a move that China and Russia do not implement to such an extent.

23 Jaclyn Kerr, "The Russian Model of Internet Control and Its Significance," LLNL-TR-764577 (Lawrence Livermore National Laboratory, December 21, 2018).

24 Privacy International, "Lawful Interception: The Russian Approach," March 4, 2013, https://privacyinternational.org/blog/1296/lawful-interception-russian-approach.

25 Russian Federation, "Information Security Doctrine of the Russian Federation" (2000), https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf.

26 Kerr, "The Russian Model of Internet Control and Its Significance."

27 Masha Gessen, "Reporting Within the Lines in Putin's Russia," *The New York Times*, July 15, 2016, sec. Opinion, https://www.nytimes.com/2016/07/15/opinion/reporting-within-the-lines-in-putins-russia.html.

28 Radio Free Europe / Radio Liberty, "U.S. Lawmakers Overwhelmingly Condemn Kremlin For Nemtsov Killing," *RadioFreeEurope/RadioLiberty*, March 13, 2019, https://www.rferl.org/a/russia-nemtsov-putin-killing/29818275.html; Marc Bennetts, "Russian Opposition Leader Alexei Navalny Jailed for 30 Days," *The Guardian*, August 27, 2018, sec. World news, https://www.theguardian.com/world/2018/aug/27/russian-opposition-leader-alexei-navalny-jailed-for-30-days; Danny Hakim, "Once Celebrated in Russia, the Programmer Pavel Durov Chooses Exile," *The New York Times*, December 21, 2017, sec. Technology, https://www.nytimes.com/2014/12/03/technology/once-celebrated-in-russia-programmer-pavel-durov-chooses-exile.html.

29 Erik C. Nisbet, Olga Kamenchuk, and Aysenur Dal, "A Psychological Firewall? Risk Perceptions and Public Support for Online Censorship in Russia," *Social Science Quarterly* 98, no. 3 (2017): 958–75.

30 John D. Gallacher and Rolf E. Fredheim, "Division Abroad, Cohesion at Home: How the Russian Troll Factory Works to Divide Societies Overseas but Spread Pro-Regime Messages at Home," in *Responding to Cognitive Security Challenges* (Latvia: NATO STRATCOM Centre of Excellence, 2019).

31 Ibid.; BBC, "Russia Profile - Media," April 25, 2017, sec. Europe, https://www.bbc.com/news/world-europe-17840134.

32 Miriam Elder, "Hacked Emails Allege Russian Youth Group Nashi Paying Bloggers," *The Guardian*, February 7, 2012, sec. World news, https://www.theguardian.com/world/2012/feb/07/hacked-emails-nashi-putin-bloggers; Shaun Walker, "The Russian Troll Factory at the Heart of the Meddling Allegations," *The Guardian*, April 2, 2015, sec. World news, https://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house.

33 Walker, "The Russian Troll Factory at the Heart of the Meddling Allegations."

34 Federal Antimonopoly Service of the Russian Federation, "Yandex vs. Google," June 27, 2016, http://en.fas.gov.ru/documents/documentdetails.html?id=14677; Brendan McGonigle, "Yandex Catches Google on Android in Russia," *Russian Search Marketing*, August 28, 2018, https://russiansearchmarketing.com/yandex-catches-google-on-android-in-russia/; Statcounter, "Social Media Stats Russian Federation," *StatCounter Global Stats*, accessed April 30, 2019, http://gs.statcounter.com/social-media-stats/all/russian-federation.

35 Dałek, *Gets a Simple Dump of the Russian Federal Black List of Blocked Sites from the Excellent Antizapret.Info in a Few Formats*; Seddon and Foy, "Russian Technology."

36 Алексей Навальный, "Алексей Навальный," *YouTube*, accessed March 19, 2019, https://www.youtube.com/channel/UCsAw3WynQJMm7tMy093y37A.

37 Matt Burgess, "This Is Why Russia's Attempts to Block Telegram Have Failed," *Wired UK*, April 28, 2018, https://www.wired.co.uk/article/telegram-in-russia-blocked-web-app-ban-facebook-twitter-google.

38 Ryan Browne, "Russia Follows China in VPN Clampdown, Raising Fresh Censorship Concerns," *CNBC*, July 31, 2017, https://www.cnbc.com/2017/07/31/russia-follows-china-in-vpn-clampdown-raising-censorship-concerns.html; Vasilis Ververis et al., "Shedding Light on Mobile App Store Censorship," in *UMAP'19 Adjunct Adjunct Publication of the 27th Conference on Modeling, Adaptation and Personalization* (Larnaca, Cyprus and New York NY: ACM, 2019), https://dl.acm.org/citation.cfm?id=3324965.

39 Joseph Cox and Emanuel Maiberg, "Chinese Government Forces Residents To Install Surveillance App With Awful Security," *Vice*, April 9, 2018, https://www.vice.com/en_us/article/ne94dg/jingwang-app-no-encryption-china-force-install-urumqi-xinjiang; Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority," April 14, 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.

40 Yujie Xue, "Camera Above the Classroom," *Sixth Tone*, March 26, 2019, https://www.sixthtone.com/news/1003759/camera-above-the-classroom; Karen Hao, "China's Government Has Given Location-Tracking Watches to 17,000 Children," *MIT Technology Review*, July 18, 2019, https://www.technologyreview.com/f/613978/china-gps-beidou-gives-location-tracking-watches-to-17-000-children-privacy/.

41 Jonathon W. Penney, "Chilling Effects: Online Surveillance and Wikipedia Use," *Berkeley Technology Law Journal* 31, no. 1 (2016): 118–82.

42 Josh Chin, "New Target for China's Censors: Content Driven by Artificial Intelligence," *Wall Street Journal*, April 11, 2018, sec. Tech, https://www.wsj.com/articles/new-target-for-chinas-censors-content-driven-by-artificial-intelligence-1523446234.

43 Tao Zhu et al., "The Velocity of Censorship: High-Fidelity Detection of Microblog Post Deletions" (USENIX Security Symposium, Washington, D.C., 2013), https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/zhu.

44 Ray Bradbury, *Fahrenheit 451*, Reissue edition (New York; Toronto: Simon & Schuster, 2012).

45 Ververis et al., "Shedding Light on Mobile App Store Censorship."

46 Gary King, Jennifer Pan, and Margaret E. Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument," *American Political Science Review* 111, no. 03 (August 2017): 484–501, doi:10.1017/S0003055417000144.

47 Rongbin Han, "Manufacturing Consent in Cyberspace: China's 'Fifty-Cent Army,'" *Journal of Current Chinese Affairs* 2 (2015): 105–34.

48 They have reportedly been paid 50 renminbi cents per post, hence the name 50 Cent Party. Lei Zhang, "Invisible Footprints of Online Commentators," *Global Times*, February 5, 2010, http://www.globaltimes.cn/special/2010-02/503820.html.

49 King, Pan, and Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument."

50 Ibid.; Yuan Yang, "China's Communist Party Raises Army of Nationalist Trolls," *Financial Times*, December 30, 2017, https://www.ft.com/content/9ef9f592-e2bd-11e7-97e2-916d4fbac0da.

51 Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall*, p. 94.

52 Ibid, pp. 13–14.

53 Haas, "Man in China Sentenced to Five Years' Jail for Running VPN"; Cyberspace Administration of China, "Internet Forum Community Service Management Regulations."

54 Mindy K. Longanecker, "No Room for Dissent: China's Laws Against Disturbing Social Order Undermine Its Commitments to Free Speech and Hamper the Rule of Law," *Pacific Rim Law & Policy Journal* 18, no. 2 (April 2009): 373–403.

55 Substantial evidence of Russian training abroad was not found – consequently only two indicators for Russia.

56 Hikvision, "Hikvision Gives Japan a Culturally and Technically Relevant Solution," December 1, 2011, https://www.hikvision.com/en/Press/Success-Stories/Education/305528882360250.

57 For more information on surveillance middleboxes See Jakub Dałek et al., "Planet Netsweeper: Executive Summary," *The Citizen Lab*, April 25, 2018, https://citizenlab.ca/2018/04/planet-netsweeper/.

58 Maria Xynou, Arturo Filastò, and Simone Basso, "Measuring Internet Censorship in Cuba's ParkNets," *OONI - Open Observatory of Network Interference*, August 28, 2017, https://ooni.torproject.org/post/cuba-internet-censorship-2017/; Huawei, "HUAWEI ESight Network Full Product Datasheet," *Huawei Enterprise*, 2017, https://e.huawei.com/uk/material/esight/e60e006763444062a048bc83f1965ebf.

59 "Colombia," OONI Explorer, accessed June 17, 2019, http://tiny.cc/Colombia_AS262928; Xynou, Filastò, and Basso, "Measuring Internet Censorship in Cuba's ParkNets"; "Italy," OONI Explorer, accessed June 17, 2019, http://tiny.cc/Italy_AS203469; "Mexico," OONI Explorer, accessed June 17, 2019, http://tiny.cc/Mexico_AS22908; Censys, "V2R2C00-IAE/1.0," Censys, accessed July 9, 2019, http://tiny.cc/Nigeria_AS; "Pakistan," OONI Explorer, accessed June 17, 2019, http://tiny.cc/Pakistan_AS45773; "Spain," OONI Explorer, accessed June 17, 2019, http://tiny.cc/Spain_AS12430 "Turkey," OONI Explorer, accessed June 17, 2019, http://tiny.cc/Turkey_AS201411.

60 Borogan and Soldatov, "Just Business."
61 Asterius Banzi, "Tanzania: Govt Seeks Chinese Help in Social Media," *The East African (Nairobi)*, August 1, 2017, https://allafrica.com/stories/201708020658.html; Lincoln Towindo, "Government to Regulate Social Media," April 10, 2016, http://www.sundaymail.co.zw/social-media-regulation-is-nigh/.
62 Louisa Lim and Julia Bergin, "Inside China's Audacious Plan for Global Media Dominance," *The Guardian*, December 7, 2018, https://www.theguardian.com/news/2018/dec/07/china-plan-for-global-media-dominance-propaganda-xi-jinping.
63 Cardenal, "China in Latin America: Understanding the Inventory of Influence."
64 Huifeng He, "In a Remote Corner of China, Beijing Is Trying to Export Its Model by Training Foreign Officials the Chinese Way," *South China Morning Post*, July 14, 2018, https://www.scmp.com/news/china/economy/article/2155203/remote-corner-china-beijing-trying-export-its-model-training.
65 The Economist Intelligence Unit also distinguished between full democracy and flawed democracy, a distinction which is not made explicitly in this paper. The Economist, "The Retreat of Global Democracy Stopped in 2018," *The Economist*, January 8, 2019, https://www.economist.com/graphic-detail/2019/01/08/the-retreat-of-global-democracy-stopped-in-2018.
66 Kurt Weyland, "Crafting Counterrevolution: How Reactionaries Learned to Combat Change in 1848" 110, no. 2 (2016): 215–31, doi:10.1017/S0003055416000174.
67 Ibid.
68 The remaining 7 percent of countries do not have a defined regime type in the Economist's *Democracy Index 2018* (See Appendix A for a list of those countries).
69 Hikvision, "Hikvision and Argentina: Working Together for a Safer Tomorrow," August 4, 2011, https://www.hikvision.com/en/Press/Success-Stories/City-Surveillance/305528874961488; Huawei, "Huawei Smart City Solution," 2013, https://www.iotone.com/files/pdf/vendor/Huawei_Smart_City_Solution_2013.pdf; Xinhua, "华为助力法国打造'平安城市'–新华网," February 10, 2017, http://www.xinhuanet.com/world/2017-02/10/c_1120445581.htm; Huawei, "Gelsenkirchen: A Small, Smart City with Big Plans," *Huawei Enterprise*, 2017, https://e.huawei.com/us/case-studies/global/2017/201709071445; Huawei Enterprise, "Smart City: Sardinia Italy," *Huawei Enterprise*, accessed January 20, 2019, https://e.huawei.com/en/videos/global/2018/201804101040; Huawei Enterprise, "Spain Enhances Smart City with ELTE Solution," *Huawei Enterprise*, 2018, https://e.huawei.com/us/case-studies/global/2018/201807041019.
70 Glasius defines "authoritarian practices as patterns of action that sabotage accountability to people over whom a political actor exerts control or their representatives, by means of secrecy, disinformation and disabling voice. These are distinct from illiberal practices, which refer to patterned and organized infringements of individual autonomy and dignity." Marlies Glasius, "What Authoritarianism Is … and Is Not: A Practice Perspective," *International Affairs* 94, no. 3 (2018): 515–33, doi:10.1093/ia/iiy060.
71 Ibid.
72 Joseph Menn, "Microsoft Turned down Facial-Recognition Sales on Human Rights Concerns," April 16, 2019, https://www.reuters.com/article/us-microsoft-ai/microsoft-turned-down-facial-recognition-sales-on-human-rights-concerns-idUSKCN1RS2FV.
73 Lim and Bergin, "Inside China's Audacious Plan for Global Media Dominance"; Meiya Pico, "Training," 2019, https://meiyapico.com/training/index.html.
74 Lim and Bergin, "Inside China's Audacious Plan for Global Media Dominance"; Meiya Pico, "Training."
75 Steven Levitsky and Lucan Way, "Linkage Versus Leverage: Rethinking the International Dimension of Regime Change," *Comparative Politics* 38, no. 4 (2006): 379, doi:10.2307/20434008.
76 Ibid.
77 Thomas Ambrosio, "Catching the 'Shanghai Spirit': How the Shanghai Cooperation Organization Promotes Authoritarian Norms in Central Asia," *Europe-Asia Studies* 60, no. 8 (2008): 1321–44, doi:10.1080/09668130802292143; Thomas Ambrosio, "Constructing a Framework of Authoritarian Diffusion: Concepts, Dynamics, and Future Research," *International Studies Perspectives* 11, no. 4 (2010): 375–92, doi:10.1111/j.1528-3585.2010.00411.x; Weyland, "Crafting Counterrevolution: How Reactionaries Learned to Combat Change in 1848."
78 Steven Levitsky and Lucan Way, "International Linkage and Democratization," *Journal of Democracy* 16, no. 3 (2005): 20–34.
79 Axel Dreher et al., "Aid, China, and Growth: Evidence from a New Global Development Finance Dataset," *SSRN Electronic Journal*, 2017, doi:10.2139/ssrn.3051044.
80 Levitsky and Way, "Linkage Versus Leverage: Rethinking the International Dimension of Regime Change," p. 379.
81 Bill Marczak et al., "HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," *The Citizen Lab*, September 18, 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/; Meiya Pico, "Training."
82 Crispian Balmer, "China's Xi Looks to Strengthen Italian Ties, Evokes Ancient Trade Routes," *Reuters*, March 22, 2019, https://uk.reuters.com/article/uk-italy-china-president-idUKKCN1R318O.
83 Reuters, "Factbox: Draft Italy Belt and Road MOU Has Broad Outlines, Few Specifics," *Reuters*, March 15, 2019, https://www.reuters.com/article/us-italy-china-mou-factbox-idUSKCN1QW1EB.
84 State Council Information Office - The People's Republic of China, "Journalists from Belt and Road Countries Learn About China," July 13, 2018, http://english.scio.gov.cn/aboutscio/2018-07/13/content_56606453.htm; iiMedia, "'一带一路'沿线国家政府网络监管部门官员代表团到访艾媒," November 14, 2017, https://www.iimedia.cn/c886/59716.html.
85 Meiya Pico, "Meiya Pico Joined the NELB-ILEC Forum at Lianyungang from Sep 26 to 30," September 21, 2016, https://web.archive.org/web/20170217164635/https://meiyapico.com/news/detail-551.html.
86 "Meiya Pico Joined the NELB-ILEC Forum at Lianyungang from Sep 26 to 30," accessed May 1, 2019, http://web.archive.org/web/20171113105154/https://meiyapico.com/news/detail-551.html.
87 Ibid.
88 Meiya Pico, "Training."
89 Ibid.
90 Ministry of Foreign Affairs of the Republic of Belarus, "Commonwealth of Independent States," 2019, http://mfa.gov.by/en/organizations/membership/list/c2bd4cebdf6bd9f9.html; Radio Free Europe / Radio Liberty, "Ukraine Shuts Down Offices In CIS Member States," *RadioFreeEurope/RadioLiberty*, August 28, 2018, https://www.rferl.org/a/ukraine-shuts-down-offices-in-cis-member-states/29457859.html.
91 This number represents the breadth of diffusion (number of countries exported to) and not the depth (how much was exported to a given country).
92 Analytical Business Solutions, "Semantic Archive," n.d., http://www.rustrade.hu/07_Kommercheskie_predlojenia_i_zaprosi/07_01_Predlojenia_ross_export/07_01_01_Tovar/07_01_01_16_Tovari/Semantic%20Archive%20presentation.compressed.pdf.
93 Andreĭ Soldatov and Irina Borogan, *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*, First (New York: PublicAffairs, 2015).
94 VAS Experts, "About Us."
95 Peter Bourgelais, "Commonwealth of Surveillance States: On the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia" (Access Now, 2013), https://web.archive.org/web/20160419101818/https://s3.amazonaws.com/access.3cdn.net/279b95d57718f05046_8sm6ivg69.pdf; Privacy International, "Private Interests: Monitoring Central Asia," November 2014, https://privacyinternational.org/report/837/private-interests-monitoring-central-asia.
96 Analytical Business Solutions, "Semantic Archive."
97 Andrei Soldatov 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/.

98 Soldatov and Borogan, *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*.

99 VAS Experts, "About Us"; Bourgelais, "Commonwealth of Surveillance States: On the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia."

100 Borogan and Soldatov, "Just Business."

101 State Information Center, "Profiles - Belt and Road Portal," accessed July 12, 2019, https://eng.yidaiyilu.gov.cn/info/iList.jsp?cat_id=10076&cur_page=1.

102 Mercator Institute for China Studies, "Mapping the Belt and Road Initiative: This Is Where We Stand," June 7, 2018, https://www.merics.org/en/bri-tracker/mapping-the-belt-and-road-initiative.

103 Alessandro Cozzi, "Smart Cities: Envisioning a Sustainable Future," *International Telecommunications Union*, June 18, 2014, https://www.itu.int/en/ITU-T/Workshops-and-Seminars/Documents/SSC-Genoa-Italy-17-20-jun-2014/PPT/Pres3_Cozzi_Alessandro-18June2014_Smart_City(Huawei).pdf; Hikvision, "Hikvision Enhances Suez Governorate's Bus Fleet Operation," April 17, 2018, https://www.hikvision.com/en/Press/Success-Stories/Transportation/Hikvision-enhances-Suez-Governorates-bus-fleet-operation.

104 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."

105 Meiya Pico, "The Assistant Minister of Interior and the Director of Information and Communication Bureau of Egypt, Mr. Ahmed·Mostafa Visited Meiya Pico," March 12, 2019, https://web.archive.org/web/20190625190652/https://www.meiyapico.com/the-assistant-minister-of-interior-and-the-director-of-information-and-communication-bureau-of-egypt-mr-ahmed-mostafa-visited-meiya-pico_n11.

106 The Economic Times, "China, Egypt Sign Strategic Partnership Agreement," *The Economic Times*, December 24, 2014, https://economictimes.indiatimes.com/news/international/business/china-egypt-sign-strategic-partnership-agreement/articleshow/45629765.cms?.

107 Al-Masry Al-Youm, "Egyptian Parliament Approves Law to Combat Cybercrime," *Egypt Independent*, May 15, 2018, https://ww.egyptindependent.com/egyptian-parliament-approves-law-to-combat-cybercrime/.

108 Steve Stecklow, Farnaz Fassihi, and Loretta Chao, "Chinese Tech Giant Aids Iran," *Wall Street Journal, Eastern Edition; New York, N.Y.*, October 27, 2011, https://www.wsj.com/articles/SB10001424052970204644504576651503577823210.

109 Steve Stecklow, "Special Report: Chinese Firm Helps Iran Spy on Citizens," *Reuters*, March 22, 2012, https://www.reuters.com/article/us-iran-telecoms-idUSBRE82L0B820120322.

110 Center for Human Rights in Iran, "China to Help Iran Implement Its Closed National Internet," *Center for Human Rights in Iran*, January 21, 2014, http://www.iranhumanrights.org/2014/01/china-iran-internet/.

111 Al Jazeera, "Iran Releases Messaging App Soroush to Replace Telegram," April 26, 2018, https://www.aljazeera.com/news/2018/04/iran-releases-messaging-app-soroush-replace-telegram-180426112935318.html.

112 Center for Human Rights in Iran, "China to Help Iran Implement Its Closed National Internet."

113 Zhou Yuan and Zhihao Zhang, "China Boosts Soft Power by Training Foreign Journalists," *Chinadaily*, October 17, 2016, http://www.chinadaily.com.cn/china/2016-10/17/content_27077588.htm.

114 Ibid.

115 Meiya Pico, "Training."

116 BOTS team, "AFSB First in Malaysia to Integrate Body-Worn Cameras with Facial Recognition Technology," *New Straits Times*, April 16, 2018, https://www.nst.com.my/lifestyle/bots/2018/04/358122/afsb-first-malaysia-integrate-body-worn-cameras-facial-recognition.

117 Liz Lee, "Alibaba to Take on Kuala Lumpur's Traffic in First Foreign Project," *Reuters*, January 29, 2018, https://www.reuters.com/article/us-alibaba-malaysia-idUSKBN1FI0QV.

118 Yiswaree Palansamy, "Dr M: Taking China's Side? It's Free Speech," *Malay Mail*, June 24, 2019, https://www.malaymail.com/news/malaysia/2019/06/24/dr-m-taking-chinas-side-its-free-speech/1765086.

119 Abdul Aziz Harun Bernama, "DPM: Chinese Crime-Fighting Methods Worth Emulating," January 15, 2017, https://www.malaysiakini.com/news/369309.

120 Radio Free Europe / Radio Liberty, "Q&A: Russia, China Swapping Cybersecurity, Censorship Tips," *RadioFreeEurope/RadioLiberty*, accessed April 30, 2019, https://www.rferl.org/a/russia-china-swapping-cybersecurity-censorship-tips-internet/28155171.html.

121 Seddon and Foy, "Russian Technology."

122 Meiya Pico, "Training."

123 Huawei Enterprise, "Huawei Helps Saint Petersburg Become a Safe City," *Facebook*, July 29, 2014, https://www.facebook.com/huaweiit/photos/a.1433359283549278/1521750881376784/?type=3.

124 Ibid.

125 Cozzi, "Smart Cities: Envisioning a Sustainable Future."

126 Dahua Technology, "Dahua IP Megapixel Solution Secures Government Office in Tanzania," April 3, 2015, https://www.dahuasecurity.com/newsEvents/successStories/51/30.

127 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."

128 Banzi, "Tanzania."

129 Hikvision, "Hikvision Protects Ministry of Commerce (MOC) Thailand," June 24, 2010, https://www.hikvision.com/en/Press/Success-Stories/Government/305528969213861.

130 Hikvision, "Hikvision Helping Bangkok's Police Force Stay Ahead of the Curve-Hikvision," July 11, 2012, https://www.hikvision.com/en/Press/Success-Stories/Government/305528970582113.

131 SmartCitiesWorld, "Huawei Helps to Realise 'Thailand 4.0,'" *Smart Cities World*, June 5, 2017, https://www.smartcitiesworld.net/connectivity/connectivity/huawei-helps-to-realise-thailand-40.

132 Meiya Pico, "Training"; Yuan and Zhang, "China Boosts Soft Power by Training Foreign Journalists."

133 Doug Bernard, "Thailand Set to Build China-like Internet Firewall," *VOA*, September 28, 2015, https://www.voanews.com/a/thailand-set-to-build-china-like-internet-firewall/2982650.html.

134 Reuters, "Thailand Scraps Unpopular Internet 'Great Firewall' Plan," *Reuters*, October 15, 2015, https://www.reuters.com/article/us-thailand-internet-idUSKCN0S916I20151015; Scott Ikeda, "Does the New Thailand Cybersecurity Law Go Too Far?," *CPO Magazine*, March 10, 2019, https://www.cpomagazine.com/data-privacy/does-the-new-thailand-cybersecurity-law-go-too-far/; Nithin Coca, "Tourism from China Provokes an Internet Crackdown in Thailand," *Coda Story*, March 12, 2019, https://codastory.com/authoritarian-tech/tourism-from-china-provokes-an-internet-crackdown-in-thailand/.

135 Yasiin Mugerwa, "China to Help Uganda Fight Internet Abuse," *Daily Monitor*, July 26, 2017, https://www.monitor.co.ug/News/National/China-Uganda-Internet-Evelyn-Anite-Africa-Internet-Users/688334-4032626-u1l61r/index.html.

136 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."

137 Unwanted Witness, "Chinese Firm Supplies 900 Surveillance Cameras to Uganda," August 3, 2018, https://www.unwantedwitness.org/chinese-firm-supplies-900-surveillance-cameras-to-uganda/.

138 Parkinson, Bariyo, and Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents."

139 Stephen Kafeero, "Government in New Move to Control Internet," *Daily Monitor*, June 29, 2019, https://web.archive.org/web/20190710074146/https://www.monitor.co.ug/News/National/Government-new-move-control-Internet/688334-5175382-vbwvsj/index.html/.

140 Zambian Watchdog, "Huawei Completes Installing Hacking Devices on All Internet Service Providers in Zambia," *Zambian Watchdog*, September 2, 2013, https://www.zambiawatchdog.com/huawei-completes-installing-hacking-devices-on-all-internet-service-providers-in-zambia/.

141 Parkinson, Bariyo, and Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents."

142 Huawei, "Huawei Smart City Overview Presentation," *Huawei Enterprise*, 2018, https://e.huawei.com/en/material/onLineView?MaterialID=02ad4d5ab608492ea24659ec667f04bd.
143 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
144 Prasso, "China's Digital Silk Road Is Looking More Like an Iron Curtain."
145 Reporters Without Borders, "All Communications Can Now Be Intercepted under New Law Signed by Mugabe," August 6, 2007, https://rsf.org/en/news/all-communications-can-now-be-intercepted-under-new-law-signed-mugabe.
146 Hongpei Zhang, "Chinese Facial ID Tech to Land in Africa," *Global Times*, May 17, 2018, http://www.globaltimes.cn/content/1102797.shtml.
147 Amy Hawkins, "Beijing's Big Brother Tech Needs African Faces," *Foreign Policy*, July 24, 2018, https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/.
148 Xiaoling Zhang, Herman Wasserman, and Winston Mano, "China's Expansion of Influence in Africa: Projection, Perception and Prospects in Southern African Countries," *South African Journal for Communication Theory and Research* 42, no. 1 (March 17, 2016): 1–22.
149 Towindo, "Government to Regulate Social Media."
150 Ibid.
151 Stephen B Kaplan and Michael Penfold, "China-Venezuela Economic Relations: Hedging Venezuelan Bets with Chinese Characteristics," 2019, https://www.wilsoncenter.org/sites/default/files/china-venezuela_relations_final.pdf.
152 Angus Berwick, "A New Venezuelan ID, Created with China's ZTE, Tracks Citizen Behavior," *Reuters*, November 14, 2018, https://www.reuters.com/investigates/special-report/venezuela-zte/.
153 Ibid.
154 Samantha Hoffman, "Social Credit," *Australian Strategic Policy Institute*, June 28, 2018, https://www.aspi.org.au/report/social-credit.
155 Huawei, "Huawei Smart City Solution"; Álvaro Artigas, "Surveillance, Smart Technologies and the Development of Safe City Solutions: The Case of Chinese ICT Firms and Their International Expansion to Emerging Markets" (Institut Barcelona d'Estudis Internacionals (IBEI), 2017), https://www.ibei.org/surveillance-smart-technologies-and-the-development-of-safe-city-solutions-the-case-of-chinese-ict-firms-and-their-international-expansion-to-emerging-markets_112561.pdf; Ryan Mallett-Outtrim, "30,000 More Security Cameras and 17,000 Less Guns on Venezuelan Streets," *Venezuelanalysis.Com*, November 27, 2013, https://venezuelanalysis.com/news/10198.
156 VEN 911, "#Ahora | Personal De Huawei Refuerza Conocimientos Al Personal De Tecnología Del #VEN911 Barinas Para El Mantenimiento De Data Center #Dialogoproductivoenmarcha," June 4, 2018, 911, https://twitter.com/VEN911Oficial/status/1003657444264996864.
157 Borogan and Soldatov, "Just Business."
158 Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (1998): 887–917.
159 Meiya Pico, "Training"; Lim and Bergin, "Inside China's Audacious Plan for Global Media Dominance."
160 Gooood, "Baise Executive Leadership Academy, China By ECADI," September 13, 2017, https://www.gooood.cn/baise-executive-leadership-academy-by-ecadi.htm.
161 Mozur, Kessel, and Chan, "Made in China, Exported to the World: The Surveillance State."
162 Joan Tilouine and Ghalia Kadiri, "A Addis-Abeba, le Siège de l'Union Africaine Espionné par Pékin," *Le Monde*, January 26, 2018, http://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html.
163 Leo Kelion and Sajid Iqbal, "Huawei Kit Pulled from Pakistan CCTV System," April 8, 2019, sec. Technology, https://www.bbc.com/news/technology-47856098.
164 Soldatov and Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You."
165 People's Daily, "China-Designed Big Data System Aids Angola's Intelligent Governance," August 23, 2018, https://web.archive.org/web/20190202234913/http://www.eurasiainfo.ch/en/china-designed-big-data-system-aids-angolas-intelligent-governance/.
166 Christian M. Wade, "Massachusetts Considers Bill to Limit Facial Recognition," February 11, 2019, https://www.govtech.com/policy/Massachusetts-Considers-Bill-to-Limit-Facial-Recognition.html.
167 Kate Conger, Richard Fausset, and Serge F. Kovaleski, "San Francisco Bans Facial Recognition Technology," *The New York Times*, May 16, 2019, sec. U.S., https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.
168 Marczak et al., "HIDE AND SEEK"; Dalek et al., "Planet Netsweeper."
169 BBC, "Australia Data Encryption Laws Explained," December 7, 2018, sec. Australia, https://www.bbc.com/news/world-australia-46463029.
170 Zack Whittaker, "'Five Eyes' Governments Call on Tech Giants to Build Encryption Backdoors — or Else," *TechCrunch*, September 3, 2018, http://social.techcrunch.com/2018/09/03/five-eyes-governments-call-on-tech-giants-to-build-encryption-backdoors-or-else/.
171 Urs Gasser et al., "Don't Panic: Making Progress on the 'Going Dark' Debate," February 1, 2016, https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.
172 Mozur, Kessel, and Chan, "Made in China, Exported to the World: The Surveillance State."
173 D" refers to democracy, "H" to hybrid regime, and "A" to authoritarian regime.
174 Huawei, "Huawei Smart City Solution."
175 Borogan and Soldatov, "Just Business."
176 People's Daily, "China-Designed Big Data System Aids Angola's Intelligent Governance," *EurAsia Info*, August 23, 2018, http://www.eurasiainfo.ch/en/china-designed-big-data-system-aids-angolas-intelligent-governance/.
177 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
178 Stabroek News, "China Launches Press Programme to Improve Ties with Caribbean."
179 Hikvision, "Hikvision and Argentina."
180 Meiya Pico, "Training."
181 Ibid.
182 Lim and Bergin, "Inside China's Audacious Plan for Global Media Dominance."
183 Trend News Agency, "Китайская Huawei построит 'Умный город' в Баку," *Trend.Az*, March 18, 2017, https://www.trend.az/business/it/2733661.html.
184 VAS Experts, "About Us."
185 Rafal Rohozinski and Vesselina Haralampieva, "Internet Filtering in the Commonwealth of Independent States 2006-2007," *OpenNet Initiative*, 2007, https://opennet.net/studies/cis2007.
186 Zhang, "China-Caribbean Press Center Launched."
187 Yuan and Zhang, "China Boosts Soft Power by Training Foreign Journalists."
188 Zhang, "China-Caribbean Press Center Launched."
189 Freedom House, "Belarus Country Report | Freedom on the Net 2017," November 14, 2017, https://freedomhouse.org/report/freedom-net/2017/belarus.
190 Soldatov and Borogan, *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*.
191 Ibid.
192 Meiya Pico, "Training."
193 Artigas, "Surveillance, Smart Technologies and the Development of Safe City Solutions: The Case of Chinese ICT Firms and Their International Expansion to Emerging Markets."
194 Frederick P. W. Gaye, "33 African Journalists Arrive China for Training," *People's Daily*, August 9, 2016, http://en.people.cn/n3/2016/0809/c90000-9097628.html.
195 Hikvision, "World Cup Inspired Security and Hikvision Protect Brazil," January 17, 2012, https://www.hikvision.com/en/Press/Success-Stories/City-Surveillance/305528876368336.
196 Xinhua, "China Donates Traffic Cameras, Anti-Cybercrime Equipment to Cambodia - People's Daily Online," *Xinhua*, December 22, 2015, http://en.people.cn/n/2015/1222/c90000-8994022.html.

197 Meiya Pico, "Training."
198 Huawei, "Huawei Tetra over eLTE," 2014, http://btg.org/wp-content/uploads/2014/11/Huawei-Tertra-over-eLTE_BTG.pdf.
199 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
200 Ibid.
201 Ibid.
202 Huawei, "Huawei Announces Safe City Compact Solution to Protect Citizens in Small and Medium Cities," *Huawei Enterprise*, August 29, 2018, https://e.huawei.com/en/news/global/2018/201808391810.
203 Alexander Gabuev, "How China and Russia See the Internet," *World Economic Forum*, December 16, 2015, https://www.weforum.org/agenda/2015/12/how-china-and-russia-see-the-internet/.
204 Huawei, "Huawei Announces Safe City Compact Solution to Protect Citizens in Small and Medium Cities."
205 Borogan and Soldatov, "Just Business."
206 Meiya Pico, "Training."
207 Protei, "NEWS - Telecommunication Solutions," 2015, http://www.protei.com/news/.
208 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
209 Huawei, "Safe City: Abidjan, Côte D'Ivoire," *Huawei Enterprise*, accessed May 1, 2019, https://e.huawei.com/en/videos/global/2018/201809121118.
210 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
211 Xynou, Filastò, and Basso, "Measuring Internet Censorship in Cuba's ParkNets."
212 Protei, "Past Events."
213 Stabroek News, "China Launches Press Programme to Improve Ties with Caribbean."
214 Jun Mai, "Ecuador Is Fighting Crime Using Chinese Surveillance Technology," *South China Morning Post*, January 22, 2018, https://www.scmp.com/news/china/diplomacy-defence/article/2129912/ecuador-fighting-crime-using-chinese-surveillance.
215 SpeechPro, "SpeechPro Deploys the World's First Voice and Face Biometrics System in Ecuador," December 17, 2012, https://speechpro-usa.com/media/news/2012-12-17.
216 VEN 911, "#Ahora | Personal De Huawei Refuerza Conocimientos Al Personal De Tecnología Del #VEN911 Barinas Para El Mantenimiento De Data Center #Dialogoproductivoenmarcha," 91.
217 Cozzi, "Smart Cities: Envisioning a Sustainable Future."
218 Al-Youm, "Egyptian Parliament Approves Law to Combat Cybercrime."
219 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
220 Ibid.
221 Human Rights Watch, "Ethiopia: Telecom Surveillance Chills Rights," *Human Rights Watch*, March 25, 2014, https://www.hrw.org/news/2014/03/25/ethiopia-telecom-surveillance-chills-rights.
222 Sanja Kelly, Sarah Cook, and Mai Truong, "Freedom on the Net 2012: A Global Assessment of Internet and Digital Media" (Freedom House, September 24, 2012), https://freedomhouse.org/sites/default/files/FOTN%202012%20summary%20of%20findings.pdf.
223 Xinhua, "Huawei Helps France Create 'Safe City' -," 2017, http://www.xinhuanet.com/world/2017-02/10/c_1120445581.htm.
224 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
225 Huawei Enterprise, "Gelsenkirchen: A Small, Smart City with Big Plans," *Huawei Enterprise*, 2017, https://e.huawei.com/us/case-studies/global/2017/201709071445.
226 Huawei, "Huawei Tetra over ELTE."
227 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
228 Zhang, "China-Caribbean Press Center Launched."
229 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
230 Zhang, "China-Caribbean Press Center Launched."
231 Huawei, "Huawei Smart City Overview Presentation."
232 Borogan and Soldatov, "Just Business."
233 Meiya Pico, "Training."
234 Huawei Enterprise, "Safe City: Bandung Indonesia," *Huawei Enterprise*, accessed January 20, 2019, https://e.huawei.com/en/videos/global/2018/201804101042.
235 Meiya Pico, "Training."
236 Stecklow, Fassihi, and Chao, "Chinese Tech Giant Aids Iran."
237 Al Jazeera, "Iran Releases Messaging App Soroush to Replace Telegram."
238 Center for Human Rights in Iran, "China to Help Iran Implement Its Closed National Internet."
239 Xinhua, "China's Huawei Helps Promote Security in Iraq's Capital via 'Safe City Solution' Project," July 15, 2019, http://www.xinhuanet.com/english/2019-03/08/c_137876838.htm.
240 Hikvision, "Hikvision Provides a Safe and Secure Harbour for Dun Laoghaire," April 8, 2015, https://www.hikvision.com/en/Press/Success-Stories/Transportation/305529081472324.
241 Hikvision, "Total Control for Jordan's House of Parliament."
242 Huawei Enterprise, "Smart City."
243 Zhang, "China-Caribbean Press Center Launched."
244 Privacy International, "Private Interests: Monitoring Central Asia."
245 Soldatov and Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You."
246 Soldatov and Borogan, *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*.
247 Meiya Pico, "Training."
248 Edith Muthethya, "New Vision for Big Data: Safe Cities," *China Daily Europe*, November 4, 2016, http://europe.chinadaily.com.cn/epaper/2016-11/04/content_27269942.htm.
249 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
250 Caravanserai, "Bishkek to Install Facial Recognition System as Part of Smart City Project," *Caravanserai*, February 9, 2018, http://central.asia-news.com/en_GB/articles/cnmi_ca/newsbriefs/2018/02/09/newsbrief-02.
251 Soldatov and Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You."
252 Soldatov and Borogan, *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*.
253 Meiya Pico, "Training."
254 Huawei Enterprise, "Safe City Service Brings the Future to Laos," *Huawei Enterprise*, April 3, 2015, https://e.huawei.com/au/case-studies/global/2015/201504030937.
255 He, "In a Remote Corner of China, Beijing Is Trying to Export Its Model by Training Foreign Officials the Chinese Way."
256 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
257 Ibid.
258 Paul Sonne and Margaret Coker, "Firms Aided Libyan Spies," *Wall Street Journal*, August 30, 2011, sec. World News, https://www.wsj.com/articles/SB10001424053111904199404576538721260166388.
259 VAS Experts, "About Us."
260 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
261 BOTS team, "AFSB First in Malaysia to Integrate Body-Worn Cameras with Facial Recognition Technology."
262 Bernama, "DPM: Chinese Crime-Fighting Methods Worth Emulating."
263 Meiya Pico, "Training."
264 SpeechPro, "Maldives Police Chose the Expert Suite IKAR Lab by Speech Technology Center," September 26, 2016, https://speechpro-usa.com/media/news/2016-09-26.
265 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
266 Republic of Mauritius, "Sixth National Assembly - Parliamentary Debates," 2018, http://mauritiusassembly.govmu.org/English/hansard/Documents/2018/hansard0718.pdf.
267 Bai Jianhua, "ICT Builds Safe Cities," *Huawei Enterprise*, accessed January 20, 2019, https://e.huawei.com/us/publications/global/ict_insights/201701051027/special-report/201701051524.

268 SpeechPro, "World's First Nationwide Voice Identification System Deployed in Mexico by Speech Technology Center (Russia)," March 6, 2010, https://speechpro-usa.com/media/news/2010-06-03.
269 Huawei, "Huawei Smart City Overview Presentation."
270 Rohozinski and Haralampieva, "Internet Filtering in the Commonwealth of Independent States 2006-2007."
271 Xu Li, "Making Sense of Sensetime," *Jumpstart*, April 6, 2018, https://jumpstartmag.com/making-sense-of-sensetime/.
272 Meiya Pico, "Forensic MagiCube Got High Comments in Mongolia - Web.Archive," November 13, 2017, https://web.archive.org/web/20171113141645/https://meiyapico.com/news/detail-533.html.
273 Huawei, "Marrakesh: Safe City," *Huawei Enterprise*, 2018, https://e.huawei.com/en/videos/industries/2018/201812060902.
274 Meiya Pico, "Training."
275 Cozzi, "Smart Cities: Envisioning a Sustainable Future."
276 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
277 Asmag, "Yangon Goes Live with Hikvision Traffic Management Solution," *Asmag*, September 27, 2017, https://www.asmag.com/showpost/23776.aspx.
278 He, "In a Remote Corner of China, Beijing Is Trying to Export Its Model by Training Foreign Officials the Chinese Way."
279 SpeechPro, "Nepalese Law Enforcement Chooses SpeechPro for Audio Forensics and Voice Identification," August 11, 2013, https://speechpro-usa.com/media/news/2013-11-08.
280 Huawei, "Huawei Tetra over ELTE."
281 VAS Experts, "About Us."
282 Cozzi, "Smart Cities: Envisioning a Sustainable Future."
283 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
284 Cozzi, "Smart Cities: Envisioning a Sustainable Future."
285 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
286 Huawei, "Huawei Tetra over ELTE."
287 Xdyanmix, "Huawei Safe City," *Xdynamix Media Communications*, 2018, http://xdynamix.com/portfolio/huawei-safe-city/.
288 The International News, "Pakistani Journalists Complete Ten Month Training Programme in China," December 13, 2018, https://www.thenews.com.pk/latest/405387-pakistani-journalists-complete-ten-month-training-programme-in-china.
289 Protei, "News and Events - Protei MENA."
290 Cardenal, "China in Latin America: Understanding the Inventory of Influence."
291 Huawei Enterprise, "Making Manila's 'Crown Jewel' a Safe City — Huawei Case Studies," *Huawei Enterprise*, 2017, https://e.huawei.com/en/case-studies/global/2017/201704261658.
292 Lilian Mellejor, "Andanar Sends off 21 Journalists, Info Officers to China," May 16, 2018, http://www.pna.gov.ph/articles/1035427.
293 Huawei, "Huawei Tetra over ELTE."
294 Artigas, "Surveillance, Smart Technologies and the Development of Safe City Solutions: The Case of Chinese ICT Firms and Their International Expansion to Emerging Markets."
295 Huawei Enterprise, "Huawei Helps Saint Petersburg Become a Safe City."
296 Soldatov and Borogan, "Putin Brings China's Great Firewall to Russia in Cybersecurity Pact."
297 Meiya Pico, "Training."
298 Gaye, "33 African Journalists Arrive China for Training."
299 Huawei Enterprise, "Yanbu: A Smart Industrial Oil Kingdom City," *Huawei Enterprise*, accessed January 20, 2019, https://e.huawei.com/us/publications/global/ict_insights/201708310903/manufacturing/201712061133.
300 Borogan and Soldatov, "Just Business."
301 Meiya Pico, "Training."
302 Artigas, "Surveillance, Smart Technologies and the Development of Safe City Solutions: The Case of Chinese ICT Firms and Their International Expansion to Emerging Markets."
303 Huawei Enterprise, "Huawei Safe City Solution: Safeguards Serbia," Huawei Enterprise, accessed September 12, 2019, https://web.archive.org/web/20190329132454/https://e.huawei.com/en/case-studies/global/2018/201808231012.
304 Gaye, "33 African Journalists Arrive China for Training."
305 Artigas, "Surveillance, Smart Technologies and the Development of Safe City Solutions: The Case of Chinese ICT Firms and Their International Expansion to Emerging Markets."
306 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
307 Jianhua, "ICT Builds Safe Cities."
308 Borogan and Soldatov, "Just Business."
309 Meiya Pico, "Training."
310 Hikvision, "Sea Point Sees Two-Thirds Crime Drop After Hikvision Cameras Deployed," May 8, 2015, https://www.hikvision.com/en/Press/Success-Stories/Transportation/305529081636891.
311 Meiya Pico, "Training."
312 Hikvision, "Company Profile-Hikvision," accessed January 21, 2019, https://www.hikvision.com/en/Corporate/Company-Profile.
313 Yuan and Zhang, "China Boosts Soft Power by Training Foreign Journalists."
314 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
315 Huawei Enterprise, "Spain Enhances Smart City with ELTE Solution."
316 Artigas, "Surveillance, Smart Technologies and the Development of Safe City Solutions: The Case of Chinese ICT Firms and Their International Expansion to Emerging Markets."
317 Bandula Sirimanna, "Chinese Here for Cyber Censorship," *The Sunday Times*, February 14, 2010, https://web.archive.org/web/20100215081800/www.sundaytimes.lk/100214/News/nws_02.html.
318 Artigas, "Surveillance, Smart Technologies and the Development of Safe City Solutions: The Case of Chinese ICT Firms and Their International Expansion to Emerging Markets."
319 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
320 Zhang, "China-Caribbean Press Center Launched."
321 Huawei Enterprise, "Safe City Improves Traffic, Cuts Crime," *Huawei Enterprise*, April 3, 2015, https://e.huawei.com/sg/case-studies/global/2015/201504031050.
322 Bourgelais, "Commonwealth of Surveillance States: On the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia."
323 Meiya Pico, "Training."
324 Cozzi, "Smart Cities: Envisioning a Sustainable Future."
325 Banzi, "Tanzania."
326 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
327 SmartCitiesWorld, "Huawei Helps to Realise 'Thailand 4.0.'"
328 Borogan and Soldatov, "Just Business."
329 Bernard, "Thailand Set to Build China-like Internet Firewall."
330 Yuan and Zhang, "China Boosts Soft Power by Training Foreign Journalists."
331 Sohu, "中国电子进出口：扎根拉美，推动信息化能力"走出去,"October 9, 2017, www.sohu.com/a/197072125_444154.
332 Zhang, "China-Caribbean Press Center Launched."
333 Cozzi, "Smart Cities: Envisioning a Sustainable Future."
334 Borogan and Soldatov, "Just Business."
335 Meiya Pico, "Training."
336 Bourgelais, "Commonwealth of Surveillance States: On the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia."
337 Meiya Pico, "Training."
338 Unwanted Witness, "Chinese Firm Supplies 900 Surveillance Cameras to Uganda."
339 Kafeero, "Government in New Move to Control Internet."
340 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
341 Liga.net, "Smart City - Города с Разумом," accessed May 1, 2019, http://www.liga.net/projects/smart_city/.

342 Soldatov and Borogan, *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*.
343 Ibid.
344 Huawei Enterprise, "Huawei Partners with Dubai Airports to Build a Smart Airport," *Huawei Enterprise*, accessed January 20, 2019, https://e.huawei.com/us/publications/global/ict_insights/201708310903/transportation-logistics/201708311040.
345 Hikvision, "Hikvision Helps London Borough Build Extensive CCTV Solution," December 11, 2013, https://www.hikvision.com/en/Press/Success-Stories/City-Surveillance/305528877699609.
346 Meiya Pico, "Training."
347 Huawei, "Huawei Tetra over ELTE."
348 Ryan Gallagher, "Watch Your Tongue: Law Enforcement Speech Recognition System Stores Millions of Voices," *Slate Magazine*, September 20, 2012, https://slate.com/technology/2012/09/speechpro-voicegrid-nation-voice-recognition-software-for-use-by-law-enforcement.html.
349 Lim and Bergin, "Inside China's Audacious Plan for Global Media Dominance."
350 Artigas, "Surveillance, Smart Technologies and the Development of Safe City Solutions: The Case of Chinese ICT Firms and Their International Expansion to Emerging Markets."
351 Privacy International, "Private Interests: Monitoring Central Asia."
352 Soldatov and Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You."
353 Borogan and Soldatov, "Just Business."
354 Meiya Pico, "Training."
355 Mallett-Outtrim, "30,000 More Security Cameras and 17,000 Less Guns on Venezuelan Streets."
356 Berwick, "A New Venezuelan ID, Created with China's ZTE, Tracks Citizen Behavior."
357 VEN 911, "#Ahora | Personal De Huawei Refuerza Conocimientos Al Personal De Tecnología Del #VEN911 Barinas Para El Mantenimiento De Data Center #Dialogoproductivoenmarcha."
358 Trinh Huu Long, "Vietnam's Cybersecurity Draft Law: Made in China?," November 8, 2017, https://www.thevietnamese.org/2017/11/vietnams-cyber-security-draft-law-made-in-china/.
359 He, "In a Remote Corner of China, Beijing Is Trying to Export Its Model by Training Foreign Officials the Chinese Way."
360 Borogan and Soldatov, "Just Business."
361 Huawei, "Huawei Smart City Overview Presentation."
362 Prasso, "China's Digital Silk Road Is Looking More Like an Iron Curtain."
363 Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
364 Zhang, "Chinese Facial ID Tech to Land in Africa."
365 Towindo, "Government to Regulate Social Media."
366 Zhang, Wasserman, and Mano, "China's Expansion of Influence in Africa: Projection, Perception and Prospects in Southern African Countries."

CENTRE FOR
TECHNOLOGY &
GLOBAL AFFAIRS

UNIVERSITY OF
OXFORD

ABOUT THE CENTRE FOR TECHNOLOGY AND GLOBAL AFFAIRS

The Centre for Technology and Global Affairs at Oxford University is a global research and policy-building initiative focusing on the impact of technology on international relations, government, and society. The Centre's experts use their research findings to develop policy and regulatory recommendations addressing the transformative power of technological change.

The Centre serves as a bridge between researchers and the worlds of technology and policymaking to impact policy in the resolution of pressing problems across six technological dimensions: Artificial Intelligence, Robotics, Cyber Issues, Blockchain, Outer Space, and Nuclear Issues.

The Centre's mission is (a) to provide leadership in creating new knowledge on practical problems affecting the security and welfare of governments, citizens, and private enterprises; (b) to influence major policy decisions and opinions in these arenas; and (c) to guide the work of leading technology developers and policymakers.

The Centre is based in the Department of Politics and International Relations at Oxford University. It is supported by core funding from Kluz Ventures.

Kluz Ventures

Centre for Technology and Global Affairs
Department of Politics and International Relations
University of Oxford
Manor Road
Oxford OX1 3UQ
United Kingdom

UNIVERSITY OF
OXFORD

DPIR
DEPARTMENT OF POLITICS & INTERNATIONAL RELATIONS