THE DIFFUSION OF CYBER NORMS

- Technospheres, Sovereignty, and Power -

Valentin Weber
Worcester College
University of Oxford

A thesis submitted in partial fulfilment
of the requirements for the degree
of Doctor of Philosophy
Trinity Term
2021

77,824 words



The Diffusion of Cyber Norms: Technospheres, Sovereignty, and Power

Valentin Weber
Worcester College
Doctor of Philosophy
Trinity Term 2021

Abstract

Why have the Chinese and Russian internet sovereignty norms diffused successfully to some countries – thereby undermining the previously dominant US norm of internet freedom – and what are the implications of successful international diffusion of information controls for understandings of sovereignty in International Relations?

Starting in the 1980s, internet freedom swept through the world and soon became the leading global cyber norm. This rise was propelled by US goals of increasing economic power and spreading democracy. Many countries that imported internet technologies, saw the economic benefits of the technologies, but with the import of the internet they also adopted loose market and content regulations. However, in the 2000s, the eruption of protests in the Middle East, Latin America, Africa, and across Asia, powered through internet-connected devices, increased the regime threat perception of authoritarian-leaning leaders. As a result, they started importing technology/techniques associated with internet sovereignty from China and Russia, who had, early-on, built up their information control capabilities. Beijing and Moscow, for their part, have actively promoted internet sovereignty diffusion to geographical areas that they conceived as their spheres of influence – the Commonwealth of Independent States for Russia and the Belt and Road Initiative for China.

This thesis makes several main contributions. It builds a framework to distinguish the three cyber norms it studies: internet freedom, and the Chinese and Russian variants of internet sovereignty. This thesis also devises a neoclassical realist framework of International Relations, which focusses on explanatory variables at the unit level (perception underlying export/import) to explain the international expansion of internet freedom/sovereignty. Additionally, it updates the term of sovereignty to the digital age. Namely, with the diffusion of internet freedom/sovereignty norms, technological spheres of influence emerged, in which the US, China, and Russia have weakened countries' Westphalian sovereignty and shaped their domestic and interdependence sovereignty.

Table of Contents

TABLES AND FIGURES v
ACKNOWLEDGEMENTS vii

CHAPTER 1: THE RISE AND DECLINE OF INFORMATION CONTROL NORMS 1

1.1. RESEARCH QUESTION AND ARGUMENT 1
1.2. CONTRIBUTION 12
1.2.1. Theoretical contribution 12
1.2.2. Empirical contribution 21
1.3. THESIS STRUCTURE 23

CHAPTER 2: DATA AND METHODS 26

2.1. DATA 26
2.2. METHODS 30
2.2.1. Case study research 30
2.2.2. Process tracing 35
2.2.3. Interviews 40

CHAPTER 3: LITERATURE REVIEW 45

3.1. EXPLAINING STATE BEHAVIOUR IN IR 48
3.2. NORM DIFFUSION 53
3.3. CYBER NORMS 72
3.4. CYBER NORM DIFFUSION 75

CHAPTER 4: INTERNET NORM DIFFUSION: A FRAMEWORK OF ANALYSIS 81

4.1. A TYPOLOGY OF INFORMATION CONTROL NORMS 82
4.2. INTERNATIONAL CYBER NORM DIFFUSION 89

CHAPTER 5: INTERNET FREEDOM IN A BRAVE NEW WORLD 106

5.1. THE INTERNET FREEDOM NORM 107
5.1.1. A history 107
5.1.2. Internet freedom in practice 113
5.2. THE DIFFUSION OF THE INTERNET FREEDOM NORM 118
5.2.1. Understanding the supply side of diffusion 118
5.2.2. Understanding the demand side of diffusion 125
5.3. VARIATION IN THE DEPENDENT VARIABLE 140
5.4. WHY GEOGRAPHICAL PROXIMITY AND CONSTRUCTIVIST EXPLANATIONS FAIL TO EXPLAIN INTERNET FREEDOM NORM DIFFUSION 146
5.5. THE US TECHNOSPHERE AND SOVEREIGNTY 149
5.5.1. The US introduces checks and balances to domestic and interdependence sovereignty 149
5.5.2. The US erodes Westphalian sovereignty 151
5.6. MEASURING THE RECEDING OF INTERNET FREEDOM 156
5.7. CONCLUSION 158

CHAPTER 6: THE WORLDWIDE WEB OF CHINESE INFORMATION CONTROLS 160

6.1. CHINA'S INTERNET SOVEREIGNTY NORM 162
6.2. THE DIFFUSION OF CHINA'S INTERNET SOVEREIGNTY NORM 166
6.2.1. Understanding the supply side of diffusion 166
6.2.2. Understanding the demand side of diffusion 169
6.3. VARIATION IN THE DEPENDENT VARIABLE 188
6.4. WHY GEOGRAPHICAL PROXIMITY AND CONSTRUCTIVIST CHALLENGES FAIL TO EXPLAIN CHINESE CYBER NORM DIFFUSION 194
6.5. THE CHINESE TECHNOSPHERE AND SOVEREIGNTY 197
6.5.1. China bolsters domestic and interdependence sovereignty 197

6.5.2. China erodes Westphalian sovereignty ... *202*
6.6. Conclusion ... 209

CHAPTER 7: THE REGIONAL WEB OF RUSSIAN INFORMATION CONTROLS ... 211

7.1. Russia's internet sovereignty norm ... 212
7.2. The diffusion of Russia's internet sovereignty norm ... 219
7.2.1. Understanding the supply side of diffusion ... *219*
7.2.2. Understanding the demand side of diffusion ... *229*
7.3. Variation in the dependent variable ... 247
7.4. Why geographic proximity and constructivist challenges fail to explain Russian cyber norm diffusion ... 251
7.5. The Russian technosphere and sovereignty ... 254
7.5.1. Russia bolsters domestic and interdependence sovereignty ... *256*
7.5.2. Russia erodes Westphalian sovereignty ... *258*
7.6. Conclusion ... 261

CHAPTER 8: CONCLUSION ... 262

8.1. Findings and contributions ... 262
8.1.1. Findings ... *262*
8.1.2. Contributions ... *267*
8.2. Policy recommendations ... 268
8.2.1. Those interested in defending internet freedom should focus their norm promotion efforts on the most prized technosphere: The Technological Crescent ... *268*
8.2.2. Those interested in defending internet freedom should embrace strategic thinking ... *269*
8.2.3. Winning hearts and minds through a compelling strategic narrative ... *273*
8.3. Further work on the future of surveillance, internet freedom, and technospheres ... 275
8.3.1. Technospheres, norms, and IR ... *276*
8.3.2. The changing nature of surveillance ... *277*
8.3.3. Internet freedom – an evolving concept ... *278*
8.3.4. The future of technospheres ... *279*

BIBLIOGRAPHY ... 281

Tables and figures

Table 1: Shows the impact of the independent variables on the dependent variables.... 10
Table 2: Case study ... 35
Table 3: List of interviewees ... 43
Table 4: Measuring influence ... 103

Figure 1: Emergence of US, Chinese, and Russian cyber norms ... 89
Figure 2: 2019 RightsCon Tunis participant breakdown by region, stakeholder, and gender. ... 135
Figure 3: US core technosphere ... 152
Figure 4: Illustrates the planned strategic Safety Corridor project. ... 169
Figure 5: Meiya Pico was instructed by the Chinese Ministry of Public Security to train countries of the BRI in digital forensics. ... 169
Figure 6: Egyptian information control landscape ... 172
Figure 7: Iranian information control landscape ... 174
Figure 8: Tanzanian information control landscape ... 175
Figure 9: Thai information control landscape ... 178
Figure 10: Ugandan information control landscape ... 180
Figure 11: Vietnamese information control landscape ... 182

Figure 12: Zambian information control landscape 183
Figure 13: Zimbabwean information control landscape..... 188
Figure 14: The Chinese core technosphere (primarily) extends along BRI trade routes.
..... 197
Figure 15: The impact of Chinese information control diffusion on Zimbabwe..... 199
Figure 16: A map of Crimea and the Kerch Strait (highlighted with a red pin)..... 225
Figure 17: Crimean information control landscape..... 225
Figure 18: Donetsk/Luhansk information control landscape 229
Figure 19: Belarusian information control landscape..... 233
Figure 20: Kazakh information control landscape 237
Figure 21: Kyrgyz information control landscape..... 241
Figure 22: Ukrainian information control landscape (pre-2015)..... 243
Figure 23: Uzbek information control landscape 247
Figure 24: Ukrainian information control landscape (post-2014) 251
Figure 25: The Russian core technosphere moulds to CIS frontiers 256
Figure 28: The Eurasian Technological Crescent..... 269

Acknowledgements

Writing this thesis would not have been possible without the valuable advice from friends and colleagues as well as mentors. I am heavily indebted to them for their input, feedback, and in-depth conversations.

I am deeply grateful for the guidance and support of my supervisors Lucas Kello and Joss Wright. They have always motivated me to dig deeper and improve the quality of my contribution. I would also like to thank the Centre for Doctoral Training in Cyber Security and the Department of Politics and International Relations at Oxford University for having created intellectually stimulating and social environments. In particular, I am grateful to have been able to share an office with Jamie Collier, Florian Egloff, Robert Gorwa, Monica Kaminska, Arthur Laudrain, Jantje Silomon, and Marcel Stolz, with whom I have had the chance to exchange fascinating conversations about International Relations and new technology.

I am also grateful for the generous funding of the UK Engineering and Physical Sciences Research Council, which made the writing of this thesis possible.

The Citizen Lab has profoundly impacted my thinking on information control, not only through its research output, but also through its annual Summer Institute that I was lucky to attend in 2018 and 2019.

During my 6-month research stay at Harvard University's Berkman Klein Center for Internet & Society, I had the chance to attend Jonathan Zittrain's Internet & Society course, which greatly shaped my thinking on the workings of the internet. Thank you to Jonas Kaiser and Padmashree Gehl Sampath for their friendship. I am also thankful to the Open Technology Fund, which funded my stay at Harvard University.

Moreover, this thesis particularly benefitted from conversations and feedback by: Freddie Barr-Smith, Jonathan Bright, Nicola Chelotti, Janina Dill, Jeffrey Ding, Jacqueline Eggenschwiler, Todd Hall, Dean Jackson, Max Kuhelj-Bugaric, Gabrielle Lim, Neil MacFarlane, Dahlia Peterson, Irene Poetranto, Andrea Ruggeri, James Shires, Jasmin Stadler, Vasilis Ververis, Gregory Walton, and many more. A special thanks to Johan Jeansson for designing the cover page of this thesis.

Most of all, I am thankful to my partner Isabella, for her dedication to excellence, which has left some marks on this thesis, and for her moral support, which made the writing process a much more enjoyable experience than I had expected it to be.

This thesis is dedicated to my parents Michael and Alenka, to my siblings Timna and Benjamin, and to my grandmother Marija Inzko, whose knowledge and curiosity continue to inspire me. Buh voni!

London, June 2021

Chapter 1: The rise and decline of information control norms

1.1. Research question and argument

This thesis studies the US, Chinese and Russian norms regarding the governance/control of information online.[1] The groundwork for the US-promoted norm of internet freedom was laid in the internet's inception in the late 1960s by a plethora of internet utopians based predominantly in the US who designed the dominant network communication protocols, such as the Transmission Control Protocol/Internet Protocol (TCP/IP) and architecture that underlie today's internet.[2] Although the US government did have an important part in the development of the internet, the utopian vision of an internet free from government control – that underlies the internet freedom policy of the US government – emanates from those currents of American society.[3] This stream in society was succinctly captured by John Perry Barlow's "A Declaration of Independence of Cyberspace".[4] In the late 1990s internet freedom was officially enshrined in US policy by the Bill Clinton administration.[5] Already in the 1980s and early 1990s, however, internet freedom had swept through the world. Internet protocols, internet platforms, software and hardware created primarily in the US reached every corner around the world. The internet has been a "freer" space than the offline space, because the former is more

[1] A considerable part of Chapters 1, 4, 6, and 7 is based on Valentin Weber, "The Worldwide Web of Chinese and Russian Information Controls," Working Paper No. 11, *Centre for Technology and Global Affairs, University of Oxford*, September 2019, https://ctga.web.ox.ac.uk/files/theworldwidewebofchineseandrussianinformationcontrolspdf.

[2] "TCP [Transmission Control Protocol] and IP [Internet Protocol] are two separate computer network protocols. IP is the part that obtains the address to which data is sent. TCP is responsible for data delivery once that IP address has been found… On the vast majority of [internet connected devices], TCP/IP is built-in as standard." Avast, "What Is TCP/IP? | How the Model & Protocols Work," August 2, 2020, https://www.avast.com/c-what-is-tcp-ip.
Morozov, *The Net Delusion: The Dark Side of Internet Freedom*.

[3] Morozov, *The Net Delusion: The Dark Side of Internet Freedom*.

[4] John Perry Barlow, "A Declaration of the Independence of Cyberspace," *Electronic Frontier Foundation*, February 8, 1996, https://www.eff.org/de/cyberspace-independence.

[5] Jack Goldsmith, "The Failure of Internet Freedom," *Knight First Amendment Institute at Columbia University*, June 2018, https://knightcolumbia.org/content/failure-internet-freedom.

difficult to regulate than the latter and hence freedoms of speech, assembly, and association can flourish even better in digital space. This was recently highlighted by Jason Pielemeier, the Policy Director of the Global Network Initiative, who compared Freedom House's Freedom on the Net index with its Freedom of the Press index. He states that no country is found to be less free in the online index, compared to the "offline" press index.[6]

However, the Freedom on the Net 2020 index shows that internet freedom – human rights online – has declined for ten consecutive years.[7] Concurrently, repressive information controls, e.g., censorship, and unchecked surveillance, have been on the rise. While Western companies have their fair share in what Ron Deibert, Director of the Citizen Lab, calls a "surveillance pandemic", a particular challenge arises through China's and Russia's models of digital authoritarianism.[8] China and Russia do not label their governance models as digital authoritarianism, but as internet sovereignty, a vision where the state is at the centre of internet governance, and where it wields the right to impose domestic internet policies without interference or criticism from abroad, even if human rights are infringed upon.[9]

[6] Jason Pielemeier, "Reports of the Death of Internet Freedom Are Greatly Exaggerated," *Council on Foreign Relations*, July 9, 2018, https://www.cfr.org/blog/reports-death-internet-freedom-are-greatly-exaggerated.

[7] Freedom House, "The Pandemic's Digital Shadow," *Freedom House*, 2020, https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow.

[8] Center for International Media Assistance - National Endowment for Democracy, "Surveillance for Sale: How China and Russia Export Repression Technology," September 17, 2019, https://www.cima.ned.org/event/surveillance-for-sale-how-china-and-russia-export-repression-technology/.

[9] Stanislav Budnitsky and Lianrui Jia, "Branding Internet Sovereignty: Digital Media and the Chinese–Russian Cyberalliance," *European Journal of Cultural Studies* 21, no. 5 (January 31, 2018): 594–613.

Like other norms, the US, Chinese, and Russian information governance norms are shared assumptions by states, international organisations, and non-state actors about "proper behavior of actors."[10]

Norms are both the drivers of actual (normal) and appropriate behaviour (normative). They are normal in the sense that they are accepted in a certain number of countries.[11] Internet freedom, for instance, is firmly accepted in the US and member countries of the Freedom Online Coalition.[12] Actions in line with allowing freedom of speech, assembly and association online are considered as normal and repetitive behaviours. The internet freedom norm is also present in many authoritarian-leaning countries. This is because a void in internet regulation still allows for free speech online, which would be stifled offline. Russia, for instance, only introduced a blacklist of prohibited websites in 2012 and in many countries, there are still no laws against hate speech online.[13]

Norms are also normative in the sense that they prescribe moral conduct.[14] In other words, the norms can be designated as "good" or "bad" according to different actors'

[10] Peter J Katzenstein, *The Culture of National Security : Norms and Identity in World Politics*, New Directions in World Politics (New York: Columbia University Press, 1996): 5.
[11] Annika Björkdahl, "Norms in International Relations: Some Conceptual and Methodological Reflections," *Cambridge Review of International Affairs* 15, no. 1 (2002): 9–23.
[12] Members of the Freedom Online Coalition are: Argentina, Australia, Austria, Canada, Costa Rica, the Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Ghana, Ireland, Japan, Kenya, Latvia, Lithuania, the Maldives, Mexico, Moldova, Mongolia, the Netherlands, New Zealand, Norway, Poland, Spain, Sweden, Switzerland, Tunisia, United Kingdom, United States.
[13] Russian Federation, "Federal Law of July 28, 2012 N 139-ФЗ (as Amended on October 14, 2014)," 2012, http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=169766&fld=134&dst=1000000001,0&rnd=0.6093347731359393#07964751504707204.
[14] Jeffrey S. Lantis, "Theories of International Norm Contestation: Structure and Outcomes," Oxford Research Encyclopedia of Politics (http://politics.oxfordre.com/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-590, June 2017).

interpretation.[15] To illustrate this point, extensive censorship is a common occurrence in China (objective assessment). At the same time, censorship is considered as being "good practice" by the Chinese Communist Party (subjective assessment), i.e., it is moral in their minds, because it preserves regime stability. The US, China, and Russia have each their own practices (norms) and in a normative sense, they each see their own internet governance behaviour as good and moral. The US, however, for instance claims a moral high ground when it calls out China for implementing censorship, because in US opinion, extensive censorship infringes on the human right of freedom of expression.[16] In other words, freedom of expression is only a norm in the US, but normative both in the US and China (seen as good by US leadership and bad by Chinese political elites). China on the other hand, maintains that the US approach of giving a lot of influence to private and civil society actors in governing the internet should cease to be a global norm. China argues that more competence should be given to multilateral institutions led by governments (at the expense of institutions that are led by a mix of governments, private companies, and civil society). In China's opinion, this is moral, since stronger government-involvement (a prominent feature of internet sovereignty) would reduce the digital divide between countries of the Global North and the Global South.[17]

Chinese and US characterisations of the norms presented above play into the contested nature of the words "freedom" and "sovereignty".[18] Firstly, freedom is, like other

[15] "Oxford English Dictionary," in *OED Online* (Oxford University Press), accessed March 11, 2021, https://www.oed.com/view/Entry/122086.
[16] Hillary Clinton, "Secretary Clinton Remarks Internet Freedom," *C-SPAN*, January 1, 2010, https://www.c-span.org/video/?291518-1/secretary-clinton-remarks-internet-freedom.
[17] The term digital divide concerns the gaps that exist in regards to access to communication and information technologies. OECD, "Bridging the Digital Divide," n.d., https://www.oecd.org/site/schoolingfortomorrowknowledgebase/themes/ict/bridgingthedigitaldivide.htm.
[18] William E Connolly, *The Terms of Political Discourse*, 3rd ed. (Princeton, N.J.: Princeton University Press, 1993).

contested words, appraisive in nature. It describes a concept, but at the same time it attributes a value to it. It is both descriptive and evaluative. Internet sovereignty is portrayed as the negative opposite of internet freedom by the US. However, in the eyes of Russia and China, internet sovereignty keeps people safe from public unrest and instability.[19] They portray internet sovereignty as if it was in the interest of their citizens. But reality shows a different picture. China used sovereignty to justify network shutdowns in Xinjiang in the late 2000s, as well as more recent human rights abuses against Uyghurs, an ethnic minority that predominantly lives in Xinjiang.[20] Nevertheless, sometimes stronger national control of information and a call for more internet sovereignty is not necessarily illegitimate. Brazil, for instance, was planning not to route internet traffic through the United States in response to the Snowden leaks, which had revealed that the US was spying on most of the world, including Brazil.[21]

All in all, this analysis acknowledges the contested nature of the internet freedom and sovereignty terms. Not doing so would impact the quality of analysis of the cyber norms.[22] However, this thesis focusses on the "normal" side of norms, i.e., the extent to which the prioritisation of sovereignty concerns is becoming ordinary across the world.

---

[19] United Nations General Assembly, "Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General" (New York, January 13, 2015), https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

[20] Qing Qiu, "India's Internet Shutdown Shows Normal Practice for Sovereign Countries," December 17, 2019, http://en.people.cn/n3/2019/1217/c90000-9641267.html; Reuters Staff, "China Tells U.N. Rights Chief to Respect Its Sovereignty After Xinjiang Comments," *Reuters*, September 11, 2018, https://in.reuters.com/article/un-rights-china-idINKCN1LR0KB.

[21] Amar Toor, "Cutting the Cord: Brazil's Bold Plan to Combat the NSA," *The Verge*, September 25, 2013, https://www.theverge.com/2013/9/25/4769534/brazil-to-build-internet-cable-to-avoid-us-nsa-spying; Bruce Douglas, "Brazil Debates Internet Law in Wake of NSA Scandal," *BBC News*, November 12, 2013, sec. Technology, https://www.bbc.com/news/technology-24899396.

[22] Connolly, *The Terms of Political Discourse*.

In recent years the US model of information governance has been receding, at the expense of the Chinese and Russian approaches to controlling information. The Freedom on the Net index is a good indicator of this trend as it shows that global internet freedom has declined since 2011, and the report accompanying the index specifically links this development to the export of Chinese information controls.[23]

Data gathered in this thesis on information controls show just how successfully Chinese and Russian technology and techniques have spread around the world, aiding governments in their regime preserving endeavours. Successful norm diffusion is measured here by the number of countries that have adopted Chinese and/or Russian technology, imitated their laws and techniques, and/or have been trained by China and Russia in information controls.

All of this leads to my research question: *Why have the Chinese and Russian internet sovereignty norms diffused successfully to some countries – thereby undermining the previously dominant US norm of internet freedom – and what are the implications of successful international diffusion of information controls for understandings of sovereignty in International Relations?*

To understand successful information governance diffusion, this thesis looks at the "supply" and "demand" side of the phenomenon. Diffusion has occurred because there has been a supply of internet sovereignty practices. China and Russia have targeted specific countries with their norm exports to gain normative influence (e.g., ability to

[23] Freedom House, "Freedom on the Net 2018: The Rise of Digital Authoritarianism," October 30, 2018, https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism.

shape norms of managing information in other countries or steering of political processes abroad by propping up incumbent elites at the expense of democratic opposition. See footnote at the end of this sentence and Chapter subheading 4.2. for a more extensive discussion of influence).[24] Concurrently there has been internet sovereignty demand. Many political elites in Africa, across Asia and Latin America were receptive to the import of Chinese or Russian norms because they had experienced large-scale protests organised through social media, which increased their regime threat perception. Following protests, they saw Chinese and Russian information control assistance as beneficial to their domestic regime survival, which in turn prompted their import of Chinese and Russian information control gear and techniques. In short, both the demand and supply side are driven by purely rational calculations (logic of expected consequences, see 3.2.) that are aimed to further, on the one hand, the influence of Beijing and Moscow and, on the other hand, secure elite regime survival in countries such as Thailand or Kazakhstan. On the flipside, diffusion is driven less by what Moscow (exporting country) or Zimbabwe (importing country) think is appropriate behaviour in the international community of 195 countries (logic of appropriateness, see 3.2.).

Information governance norms have diffused successfully to specific countries because the US, China and Russia have singled out these countries in their information control export strategies. These are countries that the US, China, and Russia want to draw into or keep in their spheres of influence (seeking of influence is the perception underlying export – independent variable 1). At the time when the internet diffused first, the US was

[24] This thesis sees influence as "deriv[ing] partially from discrepancies in access to national resources. National resources include economic, political, and security means... Such imbalances allow state A to exert influence over state B both explicitly and implicitly." Jonathan D. Moyer et al., "Power and Influence in a Globalized World" (Atlantic Council, University of Denver, The Hague Centre for Strategic Studies, January 2018), https://www.atlanticcouncil.org/in-depth-research-reports/report/power-and-influence-in-a-globalized-world/: 7.

on the verge of being the only superpower in the world and it saw the internet as a possibility to extend its influence globally.[25] Internet (freedom) technologies were encouraged to be exported through open market and non-regulation policies. Russia sees its sphere of influence (for a more in-depth discussion of the term, see footnote at the end of this sentence or 3.2.) in countries of the Commonwealth of Independent States (CIS), while China sees it in countries that are part of the Belt and Road Initiative (BRI).[26] US, Russian and Chinese strategic perceptions underlying exports are showcased in the empirical chapters with reference to policy documents, government statements, and export behaviour. This includes, for instance, China's Ministry of Public Security instructing Chinese security companies to export to countries along the Silk Road Economic Belt in order to secure the BRI trade routes for Chinese exports and to draw these countries into a "security community" with China at its core.[27] Another example is Bill Clinton's statement that the internet should diffuse to open up repressive societies across the globe.[28]

Different perceptions underlie the import of internet freedom/sovereignty norms. For countries importing internet freedom, the primary motivation was that they saw the internet as a tool to increase economic growth. Later on, authoritarian-leaning countries, such as Egypt, Iran, Kazakhstan, and Zimbabwe, became aware that the internet would

[25] Robert Farley, "America Ruled the World in the 1990s - But It Doesn't Anymore," Text, *The National Interest* (The Center for the National Interest, December 20, 2020), https://nationalinterest.org/blog/reboot/america-ruled-world-1990s-it-doesnt-anymore-174709.

[26] A sphere of influence is commonly understood as control of a geographic area by one power and at the same time the exclusion of other powers from this specific territory. Paul Keal, "Contemporary Understanding About Spheres of Influence," *Rev. Int. Stud.* 9, no. 3 (1983): 155–72; Edy Kaufman, *The Superpowers and Their Spheres of Influence: The United States and the Soviet Union in Eastern Europe and Latin America* (London: Croom Helm, 1976).

[27] Lianyungang Forum, "The 4th Lianyungang Forum Was Successfully Held," 2018, http://www.lygforum.gov.cn/index.php?m=news&a=details&content_id=294.

[28] "Clinton's Words on China: Trade Is the Smart Thing," *The New York Times*, March 9, 2000, sec. World, https://www.nytimes.com/2000/03/09/world/clinton-s-words-on-china-trade-is-the-smart-thing.html.

threaten their domestic political stability. As a result, they started adopting internet sovereignty norms.

This thesis highlights this "internet sovereignty import" phenomenon by looking at political leaders' perception that motivate imports (independent variable 2). It establishes that authoritarian-leaning countries import illiberal internet norms to ensure their regime survival in the digital age, in which flows of information via the internet can help to disseminate anti-regime views and thereby instigate public discontent towards undemocratic regimes. In 2010, for example, the Arab Spring demonstrated that internet communications can be a powerful tool for the fuelling of popular revolts. As showcased in the empirical chapters, authoritarian-leaning countries around the world, which were affected by similar revolutionary movements, realised that they had to impose restrictive information controls in order to stay in power. By interviewing government officials, and through the examination of primary and secondary sources, this thesis highlights how large-scale protests increased the perception of regime threat within hybrid/authoritarian regimes.[29] This change of perception amongst those regimes in turn has dramatically increased their demand for internet sovereignty. In other words, governments want to close the sovereignty gap that exists between the online and offline spaces.[30] In order to do so, they import Chinese and/or Russian technology, imitate their laws, and undergo

[29] The Economist Intelligence Unit's Democracy Index describes hybrid regimes as those where "elections have substantial irregularities that often prevent them from being both free and fair. Government pressure on opposition parties and candidates may be common. Serious weaknesses are … prevalent … in political culture, functioning of government and political participation. Corruption tends to be widespread, and the rule of law is weak. Civil society is weak. Typically, there is harassment of and pressure on journalists, and the judiciary is not independent." Those regimes are described as "hybrid" since they share characteristics of both democracies and authoritarian regimes. 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.

[30] Sovereignty gap describes the phenomenon that states exert sovereignty and control to a greater extent offline than they do online, this is due to many factors such as the decentralised nature of the internet's infrastructure. See Morozov, *The Net Delusion: The Dark Side of Internet Freedom*.

training in propaganda or cybersecurity. All these three elements (technology transfer, imitation, training) are manifestations of norm diffusion (dependent variable 1), however, only imitation shows advanced norm diffusion. In short, whenever demand and supply meet, internet freedom/sovereignty is likely to diffuse successfully.

Causal logic	**Supply (freedom and sovereignty)**	**Demand (freedom and sovereignty)**
Unit level factors (independent variables 1 and 2)	Perception underlying export is seeking of influence	Perception underlying import of internet freedom/sovereignty is economic growth expectations/regime survival concerns
State behaviour (dependent variable 1)	**Freedom/sovereignty norm diffusion** Import/export of internet/filtering/surveillance technology Training of government officials or journalists to share techniques Imitation of laws and techniques	
Consequence of behaviour (dependent variable 2)	Impacts on sovereignty (weakening of Westphalian and shaping of domestic and interdependence sovereignty of importing country)	



Table 1: Shows the impact of the independent variables on the dependent variables.

The principal implication of this thesis for understandings of sovereignty in International Relations (IR) is related to the discipline's debate about what constitutes a violation of sovereignty. This thesis counterargues Kenneth Waltz's vision of sovereignty (see 1.2.1. and 3.1. for a more in-depth discussion), who maintains that only a physical intervention into a country is a violation of sovereignty (e.g., US intervention of Iraq in 2003) and that

influence of a foreign country on the domestic and foreign affairs is perfectly compatible with sovereignty. In other words, no country is free from influence. This thesis argues that influence of one country onto another, falling short of a physical intervention, can also be labelled as a restriction of sovereignty of the latter country. To give an example, during the Cold War, Eastern Germany was on paper a sovereign country, but Soviet influence was so extensive (even without a physical intervention) that Eastern Germany was all but a sovereign entity. This thesis claims that, similarly to the East German case, countries where internet sovereignty diffused to are restricted in their sovereignty. They voluntarily take Chinese and Russian assistance in suppressing their populations (internet sovereignty diffusion), but this assistance very likely precludes them from taking independent decisions in the future. If China had access to, e.g., Tanzania's governmental decisions within Tanzanian borders, through backdoors, and if those decisions, for instance, affected Chinese businesses or interests, China may well use this information to change the Tanzanian government's decision-making process in its favour. In this case, Westphalian sovereignty, or the principle of non-intervention into a state's internal affairs, would be restricted.[31]

[31] See 3.2. for precise definitions of Krasner's four types of sovereignty, including Westphalian sovereignty. Backdoor "is a term that refers to the access of the software or hardware of a computer system without being detected. The backdoor can be created by the developer themselves so that they can quickly and easily make changes to the code without the need to log in to the system. However, backdoors can be used by hackers in cyberattacks to steal personal information and data." ISMS, "Backdoor (Computing)," *ISMS.Online*, December 14, 2020, https://www.isms.online/glossary/backdoor-computing/; Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* (Princeton, N.J.: Princeton University Press, 1999).

1.2. Contribution

1.2.1. Theoretical contribution

This thesis seeks to contribute to IR literature in three ways. Firstly, it highlights previously largely disregarded causes of norm diffusion. Current scholarship on norm diffusion focusses on either ideational persuasion (constructivism) or geographic proximity to explain successful diffusion.[32] These may well be the causes for some kinds of norm diffusion, but not for internet freedom/sovereignty, where material incentives (seeking of influence and economic growth expectations/regime survival) are the primary drivers of diffusion. Secondly, this thesis aims to contribute to the literature on sovereignty and the concept's relation to cyberspace.[33] The contribution lies in the empirical demonstration of how internet sovereignty diffusion limits the sovereignty of the importing country, i.e., how Zimbabwe and Kazakhstan experience a decrease in Westphalian sovereignty (principle of non-intervention into a state's internal affairs) during the process of diffusion. By propping up the incumbent elites with surveillance gear, China and Russia make it much more difficult for opposition parties to run successfully for election, thereby they meddle in the affairs of another state. To capture these impacts on sovereignty, this thesis adapts the concept of spheres of influence to the digital age. It proposes the concept of technological spheres of influence and coins the term "technospheres". Thirdly, this thesis intends to add to the IR literature by reassessing the relationship between norms and technology. It claims that states can define the norms

[32] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (1998): 887–917; Amitav Acharya, "How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism," *International Organization* 58, no. 2 (2004): 239–75; Steven Levitsky and Lucan Way, *Competitive Authoritarianism: Hybrid Regimes After the Cold War*, Problems of International Politics (New York: Cambridge University Press, 2010).

[33] David J. Betz and Tim Stevens, "Chapter Two: Cyberspace and Sovereignty," in *Cyberspace and the State: Toward a Strategy for Cyber-Power*, Adelphi Series (London, United Kingdom: International Institute of Strategic Studies, 2011): 55–74.

that are ingrained in technology, e.g., the US funds internet technologies, such as the anonymous Tor Browser, that are designed to enhance people's right to privacy. At the same time, technology can shape norms of state behaviour, i.e., the private nature of Virtual Private Networks (VPNs) prompted China and Russia to pass regulations that limit their availability in mobile app(lication) stores.[34] The ensuing chapters serve to illustrate each of the four contributions in detail.

When it comes to norm diffusion, often two major causes are named in the IR literature: persuasion and geographic proximity. As regards to the former, numerous constructivist works explain the causes of international norm diffusion.[35] One of the most prominent contributions is Finnemore and Sikkink's article "International Norm Dynamics and Political Change", which illustrates how ideational persuasion by actors can cause a change in norms in other countries.[36] Norm entrepreneurs, such as women's rights advocates, launched several campaigns in order to convince a critical amount of countries to embrace new norms that are more favourable to women's rights. They managed to convince other actors to start believing in these norms, even though it might not have been in their material interest. This view follows a "logic of appropriateness", whereby

[34] "A virtual private network (VPN) is an encrypted connection between two or more computers. VPN connections take place over public networks, but the data exchanged over the VPN is still private because it is encrypted." Cloudflare, "What Is IPsec? | How IPsec VPNs Work," 2021, https://www.cloudflare.com/learning/network-layer/what-is-ipsec/; 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.

[35] Acharya, "How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism"; Tim Maurer, "Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-Security," Explorations in Cyber International Relations Discussion Paper Series (Belfer Center for Science and International Affairs, September 2011), https://www.belfercenter.org/sites/default/files/legacy/files/maurer-cyber-norm-dp-2011-11-final.pdf; Jeffrey S Lantis and Daniel J Bloomberg, "Changing the Code? Norm Contestation and US Antipreneurism in Cyberspace," *International Relations* 32, no. 2 (March 13, 2018): 149–72, doi:10.1177/0047117818763006.

[36] Finnemore and Sikkink, "International Norm Dynamics and Political Change."

states act in accordance with their identities that are tied to behavioural rules, instead of merely following their rational calculations in pursuit of material interests.[37] This viewpoint is opposed to rationalist IR scholars (including neorealists and neoliberals), who see norms as a result of the "logic of expected consequences".[38] In this logic, actors pick from different actions by evaluating their consequences and choose the one that suits them best.[39] This thesis follows a logic of expected consequences, which is in line with neoclassical realist scholar's perception of IR (for a more in-depth discussion of the two logics, see 3.2.).

When it comes to internet freedom/sovereignty diffusion, the countries that embrace sovereignty or freedom do not need to be persuaded by appeals to behavioural appropriateness. Instead, elites in the analysed countries are driven by a logic of expected consequences. The Arab Spring and other revolutions powered by social media were shock enough to trigger Iranian and Uzbek survival instincts. There was no further persuasion needed from Russia and China. Countries that implement internet freedom today (Freedom Online Coalition +) are predominantly countries that had embraced strong democratic principles offline for decades.[40] There is no need for the US to persuade them.

[37] James G. March and Johan P. Olsen, "The Institutional Dynamics of International Political Orders," *International Organization* 52, no. 4 (1998): 943.
[38] Joseph M. Grieco, "Anarchy and the Limits of Cooperation: A Realist Critique of the Newest Liberal Institutionalism," *International Organization* 42, no. 3 (1988): 485–507; John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York, N.Y.: W. W. Norton & Company, 2001); Gideon Rose, "Neoclassical Realism and Theories of Foreign Policy," *World Politics* 51, no. 1 (1998): 144–72.
[39] Michael Hechter and Satoshi Kanazawa, "Sociological Rational Choice Theory," *Annual Review of Sociology* 23 (1997): 191.
[40] See 5.2.2. for a full list of countries that form the Freedom Online Coalition +.

However, the US, Russia, and China still make an argument for diffusion. Beijing and Moscow's goal is to challenge the status quo and replace the norm of internet freedom globally with their concept of information control. They emphasise government control of the internet and the diminution of freedom of expression and other human rights at the expense of public security. Lu Wei, the former Director of the Cyberspace Administration of China, made clear that China's vision of information control is at direct opposition to the US vision and that the Chinese approach to governing the internet should not be limited to China, but adopted around the world.[41] The US, too, makes an argument for internet freedom. Secretary of State Hillary Clinton, for instance, proclaimed that:

> "Both the American people and nations that censor the internet should understand that our government is committed to helping promote internet freedom… As I speak to you today, government censors somewhere are working furiously to erase my words from the records of history. But history itself has already condemned these tactics."[42]

Furthermore, the democratisation literature maintains that authoritarian countries that are strongly tied to democracies via geographic, political and economic links are more likely to democratise ("linkage" theory).[43] My thesis contests the democratisation literature and especially its claim that geography is the most important factor for norm diffusion.[44] My thesis shows that diffusion has occurred wherever the norm promoter fosters exports (quest for influence) and not only if a country is geographically close. The Chinese norm (which emphasises the use of extensive censorship to control information, see 6.1. for more information on how the subsidiary norm of extensive censorship defines China's

---

[41] Lu Wei et al., "Cyber Sovereignty Must Rule Global Internet," *HuffPost*, December 15, 2014, https://www.huffpost.com/entry/china-cyber-sovereignty_b_6324060.
[42] Hillary Clinton, "Remarks on Internet Freedom," *U.S. Department of State*, January 21, 2010, //2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.
[43] Steven Levitsky and Lucan Way, *Competitive Authoritarianism: Hybrid Regimes After the Cold War*, Problems of International Politics (New York: Cambridge University Press, 2010).
[44] Ibid.

model), for instance, spreads more easily to countries along the BRI trade routes, independently of whether they are located near or far the Chinese border, and the US norm diffused globally. Russia's norm (which emphasises the inducing of self-censorship in the population to control information, see 7.1. for more information) has most successfully diffused to CIS countries, which is in line with geographical proximity as the main factor of diffusion. However, geographic proximity scholars have difficulties explaining the halt and even reversal of Russian internet sovereignty diffusion to Ukraine post-2014, since Ukraine's geographical proximity to Russia did not change between 2014 and 2015.

This thesis maintains that neither persuasion nor geographic proximity are useful mechanisms to explain internet sovereignty norm diffusion. It is rather material incentives – the quest for normative influence, as well as regime survival – which drive the export/import of this type of norms.

The second theoretical contribution of this thesis pertains to the notion of restriction of sovereignty in cyberspace. Susanna Hast writes that this is still a much-discussed issue in IR, as the following views, of David A. Lake, on the one hand, and Steven Krasner, on the other hand, illustrate.[45] Restriction of sovereignty is more difficult if academics see sovereignty as absolute and indivisible.[46] In this vision, influence from another state may, for instance, not constitute a restriction of sovereignty but is rather a state of dependence of one state on another. Waltz, for example, wrote that "[s]overeign states may be hardpressed all around, constrained to act in ways they would like to avoid, and able to

[45] Ibid: 58.
[46] David A. Lake, "The New Sovereignty in International Relations," *International Studies Review* 5, no. 3 (2003): 303–23.

do hardly anything just as they would like to … To say that a state is sovereign means that it decides for itself how it will cope with its internal and external problems, including whether or not to seek assistance from others and in doing so to limit its freedom by making commitments to them."[47] Similarly, David A. Lake claims that "the observation that states might choose policies or adopt institutions that would tie their hands became, not an infringement on sovereignty, but rather its manifestation."[48] Based on this understanding of sovereignty, only an intervention (e.g. US invasion of Iraq) would signify a restriction of sovereignty.[49]

If sovereignty is divisible into different parts, then it is easier to violate one part, while not violating another part. As we will discuss in Chapter 3, Krasner, for instance, sees sovereignty as constituted by different parts.[50] All these parts can be restricted. In his vision, most states, except great powers, live with a restricted sovereignty.[51] Historically, states have accepted foreign military forces on their territory in order to maintain stability, e.g., Bosnia and Herzegovina after the Yugoslav wars.

This thesis taps into this debate and explores whether and how sovereignty is restricted in cyberspace. This thesis argues that when it comes to cyberspace, similarly as the "offline world", states engage in trading their sovereignty when it comes to their regime survival.[52] They sacrifice part of their sovereignty to another state that can help them establish sovereignty at home. This thesis claims that countries import Chinese and

[47] Kenneth Waltz N., *Theory of International Politics* (Reading, MA: Addison-Wesley, 1979): 95-96.
[48] Lake, "The New Sovereignty in International Relations."
[49] Hast, *Spheres of Influence in International Relations: History, Theory and Politics*.
[50] Lake, "The New Sovereignty in International Relations"; Krasner, *Sovereignty: Organized Hypocrisy*.
[51] Lake, "The New Sovereignty in International Relations."
[52] Burak Kadercan, "Making Sense of Survival: Refining the Treatment of State Preferences in Neorealist Theory," *Review of International Studies* 39, no. 4 (2013): 1015–37.

Russian information control technology and techniques to gain more control over their domestic population (that is, to increase domestic and interdependence sovereignty).[53] At the same time, the import of technology, and its installation into critical infrastructure, means that China and Russia have many more options to meddle in the internal affairs of importing countries, e.g., Zimbabwe or Kazakhstan (decrease in Westphalian sovereignty). It is help in a self-help world.

These impacts on sovereignty are captured in the concept of spheres of influence (SOI). Van Jackson defines a sphere of influence as:

> "… [A] hierarchical structure, the construction and maintenance of which results from a practice involving two specific features: some amount of control over a given territory or polity by a foreign/outside actor, especially as regards third-party relations, and exclusion of other external actors from exercising that same kind of control over the same space."[54]

Consequently, a sphere of influence is a hierarchical structure that exists within an anarchical system.[55] Jack Donnelly illustrates this by highlighting the hierarchical relations between the German Democratic Republic (East Germany) and the Soviet Union.[56] East Germany had legal sovereignty, but practically it was only allowed to act according to the constraints imposed by the Soviet Union.

According to Jackson's quote above, besides being hierarchical, SOIs are also defined by exclusion (of a rival power from the sphere's territory) and control (of the SOIs territory).

---

[53] See 3.2. for precise definitions of Krasner's four types of sovereignty, including domestic and interdependence sovereignty.
[54] Van Jackson, "Understanding Spheres of Influence in International Politics," *European Journal of International Security*, n.d.: 1–19.
[55] Jack Donnelly, ed., "Anarchy, Hierarchy, and Order," in *Realism and International Relations*, Themes in International Relations (Cambridge: Cambridge University Press, 2000): 81–106.
[56] Ibid.

It also entails various circles of influence, ranging from strong influence to weaker influence over other areas.[57] The task undertaken in 4.2. is to precisely define the terms of exclusion and control in the context of internet freedom/sovereignty as well as to show how norm diffusion (dependent variable 1 [DV1]) impacts the sovereignty of importing countries (dependent variable 2 [DV2]). This thesis argues that the import of surveillance technology from China and Russia (DV1) gives the exporting countries technological influence, i.e., privileged capability to control that technology (compared to other countries that would want to exploit that equipment) to further their interests. At the same time, the import of techniques and technology gives China and Russia the ability to bolster regimes that they favour (normative influence) and weaken political entities or individuals that might be more favourable towards the US.

The third contribution of this thesis is that it addresses a longstanding debate among scholars about the relationship between technology and norms. This thesis reinforces the point that norms and technology are inseparable. Finnemore and Hollis, for example, mention the arrival of Simple Network Management Protocol to administer devices on a network.[58] Once adopted, the protocol had to be executed by the thousands of users of the Management Protocol. The protocol became the new normal. While it is unclear what values this protocol embodies, technology can entail the spirit of internet freedom or internet sovereignty.

[57] James Burnham, *The Struggle for the World* (London: Jonathan Cape, 1947).
[58] Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *American Journal of International Law* 110, no. 3 (2016): 445.

States can shape technology and define the norms that are ingrained in it.[59] Madeline Carr calls this the "political construction of technology."[60] "They [US policy makers] enact policies which they believe will promote these elements [freedom] and this becomes an example of the way that technology can be understood as an "expression" of norms and values."[61] While applications, such as the Tor Browser (developed with US government funds) provide high security from the prying eyes of government, messenger applications such as VK, Soroush and WeChat (supported and influenced by the Russian, Iranian, and Chinese governments) provide easy preying ground for Moscow, Tehran, and Beijing to respectively surveil their citizens and enforce information controls.

In turn, technology can shape norms of state behaviour, i.e., how states behave. For instance, because of the private nature of VPNs, both China and Russia banned non-state-approved VPNs.[62] In other words, the arrival of a new technology prompted a response from states. What is more, the availability of technology can also influence state behaviour. Partly, due to different availability of technology, China and Russia have developed different kinds of sovereignty norms. China has many more options to impose information controls than Russia does (e.g., large-scale deployment of facial recognition, and biometric identification systems, and intrusive apps that monitor citizens, to name just a few). Because it has a self-sufficient technology ecosystem at home (Alibaba, WeChat, …) it can impose strict censorship. Russia does not have such an ecosystem and has to rely partly on Google and Facebook, who refuse to impose strict censorship. Due to the multinational companies' market size, they have leverage vis-à-vis Russia.

[59] Ibid.: 446.
[60] Carr, *US Power and the Internet in International Relations - The Irony of the Information Age*: 184.
[61] Carr: 147.
[62] Ververis et al., "Shedding Light on Mobile App Store Censorship."

1.2.2. Empirical contribution

The thesis aims to make two empirical contributions. First, it proposes one of the first conceptual frameworks to account for the different kinds of information governance systems and their associated norms. This framework helps to acquire new empirical understandings of the Chinese, Russian, and US information governance norms. The new empirical understandings are that China emphasises censorship to control information, whereas Russia relies on inducing self-censorship. By contrast, the US predominantly relies on propaganda to control information domestically. All three countries have strong domestic surveillance capabilities. While China and Russia deploy those capabilities excessively with no checks and balances, the US has safeguards in place that limit the conduct of mass surveillance of internet content amongst US persons.[63] At the same time, it is worth noting that the US has conducted extensive surveillance on practically everyone else.[64]

Second, the thesis presents data that has yet largely been unexamined by academics. It provides evidence that US, Chinese, and Russian cyber norms have spread to over 100 countries. This thesis traces diffusion by looking at a wide array of norm diffusion indicators. It traces the diffusion of Russian surveillance equipment, US training of journalists, Chinese CCTV cameras, safe cities, the Chinese training of law enforcement

[63] Jaclyn Kerr, "The Russian Model of Internet Control and Its Significance," LLNL-TR-764577 (Lawrence Livermore National Laboratory, December 21, 2018); Valentin Weber, "How China's Control of Information Is a Cyber Weakness," *The Lawfare Institute*, November 12, 2020, https://www.lawfareblog.com/how-chinas-control-information-cyber-weakness; For a more critical account of US check and balances concerning surveillance on US citizens See American Civil Liberties Union, "Checks, Balances, and the National Security Agency," June 10, 2013, https://www.aclu.org/blog/national-security/secrecy/checks-balances-and-national-security-agency;.

[64] Ewen MacAskill et al., "NSA Files Decoded: Edward Snowden's Surveillance Revelations Explained," *The Guardian*, November 1, 2013, http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded.

officials abroad, amongst others.[65] All these are examples of norm diffusion. Whenever Zimbabwe strikes a surveillance deal with China, it is to bolster Zimbabwean internal sovereignty (better monitoring of its population). Whenever journalists visit the People's Daily (China Communist Party's mouthpiece), they learn how to manage online content in an authoritarian media landscape.

This dataset also includes a mapping of the internet freedom community. This mapping includes listing governments that have a free internet environment according to Freedom House's Freedom on the Net index, or those that are part of the Freedom Online Coalition, as well as the identification of civil society organisations that are committed to ensuring internet freedom and human rights online within these countries.[66] These are the countries where internet freedom is strongly engrained today. Many studies have already devoted time to study the US government's internet freedom policy, but only few have studied the norms' diffusion by adding the many civil society organisations and internet freedom events across the world that strive towards ensuring digital human rights.[67] Examples of internet freedom entities include Access Now (civil society organisation), the Global Network Initiative (civil society organisation) and Citizen Lab (academia). The mapping conducted in this thesis provides in-depth analysis of the major governmental and non-governmental internet freedom entities and contributes through the adding of primary

[65] Safe cities are cities that reduce crime, antisocial behaviour through a mix of advanced technology and policing. Adam Bannister, "What Exactly Is a 'Safe City'?," *IFSEC Global | Security and Fire News and Resources*, September 5, 2014, https://www.ifsecglobal.com/security/exactly-safe-cities-mean/.

[66] Freedom House, "Freedom on the Net 2018."

[67] Shawn M Powers and Michael Jablonski, *The Real Cyber War: The Political Economy of Internet Freedom* (Urbana, Chicago, and Springfield: University of Illinois Press, 2015); James Griffiths, *The Great Firewall of China : How to Build and Control an Alternative Version of the Internet* (London: Zed Books, 2019); Goldsmith, "The Failure of Internet Freedom"; Richard Fontaine and Will Rogers, "Internet Freedom: A Foreign Policy Imperative in the Digital Age" (Center for New American Security, June 2011), https://www.cnas.org/publications/reports/internet-freedom-a-foreign-policy-imperative-in-the-digital-age.

sources (US laws and interviews with members of the internet freedom community) that give profound insight into the examined internet freedom organisations. This mapping also provides a more impartial view of what internet freedom is today. Rather than being portrayed as an exclusively US-led project, this thesis highlights how internet freedom is increasingly becoming a global movement that is spearheaded by individuals and civil society organisations around the world, that is still very loosely organised via mailing lists, a few annual conferences and festivals, as well as many interpersonal contacts.[68]

1.3. Thesis structure

Chapter 2 lays out the data and methods that are used in this thesis and discusses their limitations. Data is drawn from secondary (e.g., newspaper articles) and primary sources, such as government documents (e.g., 2019 Thai cybersecurity law), as well as interviews – that I conducted with current and former government officials – that help explain the perception underlying the import of the Chinese cyber norm, amongst, for instance, Zimbabwean elites. This thesis uses case study analysis, process tracing, and interviews, to gather and subsequently analyse the data. The major limitation of case study analysis is that the findings cannot be generalised, which this thesis does not do. Regarding interviews, the researcher may be biased, but measures to reduce bias, such as avoiding asking leading questions, have been introduced in the interview design process.

Chapter 3 of the thesis begins with an overview of the current state of the IR and Internet Governance literature that pertains to change in state behaviour, (cyber) norms and their diffusion, and highlights the theoretical (e.g., what does a sphere of influence look like in

[68] Nani Jansen Reventlow and Jonathan McCully, "Internet Freedom Without Imperialism," *Knight First Amendment Institute*, June 13, 2018, https://knightcolumbia.org/content/internet-freedom-without-imperialism.

the digital space?) and empirical (e.g., mapping the diffusion of internet freedom, Chinese and Russian internet sovereignty norms) void that needs to be filled by current research.

Chapter 4 discusses the theoretical scheme for the analysis of internet freedom/sovereignty diffusion. It first proposes a typology of information governance, which helps to differentiate the US, Chinese, and Russian cyber norms. The theoretical framework then examines the causes of US, Chinese and Russian cyber norm diffusion. Those are the seeking of influence, which is the perception underlying export. The perception driving the import of internet sovereignty is regime survival concerns and the one driving import of internet freedom is the expectation that internet freedom will propel economic growth. The framework further lays out three indicators to measure norm diffusion (DV1): technology transfer, imitation, and training. Finally, the theoretical framework introduces the concept of technological spheres of influence.

Chapter 5 focusses on the US-promoted internet freedom norm. It documents how this norm has diffused to most parts of the world, even to authoritarian regimes, such as Iran, in the 1980s and 1990s, but not to China or North Korea, since those two countries had considered the internet from the outset as a challenge to the survival of their regime. The internet freedom chapter serves as a baseline for the ensuing chapters which analyse the Chinese and Russian internet sovereignty norms that are challenging the internet freedom norm.

Chapter 6 reviews China's information control norm and analyses why it diffused to countries such as Zimbabwe or Thailand, but not to Nicaragua or Bahrain. It also illustrates that Chinese information controls proliferated more readily than Russian

controls due to China's greater strategic ambitions reflected in the BRI framework. It also illustrates what impact Chinese exports have on importing countries' sovereignty.

Chapter 7 examines Russia. Russia does not have the technological prowess of China. It does not rely primarily on high-technology measures to curb domestic dissent but on a variety of means. Those are laws, regulations, intimidation, and internet infrastructure surveillance through its SORM (System of Operative Investigative Activities) system. The chapter looks at countries where the Russian norm diffused, with a meticulous examination of countries such as Uzbekistan as well as Ukraine where the norm diffused to at first but then stopped diffusing in 2015.

Chapter 8 summarises this thesis' arguments and explores its broader implications for IR theory and research. Having discussed the findings and implications of this thesis, the potential avenues for further research and policy recommendations are laid out. One such avenue could be to study not only the impact of the technological sphere of influence ("technosphere") on the relationship between the hegemon and subject of the sphere, but also what technospheres mean for great power conflict. Do technological spheres of influence foster conflict or propel a peaceful regional and international order?

This chapter introduced the research question of this thesis, its major contributions and gave an outline of the chapters to come. The next chapter lays out how research in this thesis was conducted. This is especially pertinent to understand how data in the empirical Chapters 5, 6, and 7 was gathered and analysed.

Chapter 2: Data and methods

The following chapter lays out the data and methods that this thesis uses to answer its research question.

2.1. Data

A major drawback of cyber studies is the perceived lack of reliable or complete data.[69] This is because many governments prefer their restrictive actions to remain in the dark or in twilight. Few countries publish precisely how or what information they deny, disrupt, or monitor; or else this information is purposefully misleading. To illustrate this with the US case, until the Snowden revelations, few knew how extensive the US's domestic online monitoring programme was. It included breaking into Google's internal networks, and mass surveillance through the co-opting of companies into sharing information with the National Security Agency.[70] When it comes to censorship (denying/disrupting information), some countries are quite transparent about some categories of content that is blocked, such as gambling. However, they are less vocal about other content denied, such as voices from the political opposition.[71] The US for its part would also prefer not to be too vocal of where and how it promotes internet freedom, since the action of promoting democracy is seen in other countries as an attempt to subvert regimes.[72] During the 2009 Iranian presidential elections, for instance, the US government instructed

[69] Valentin Weber, "States and Their Proxies in Cyber Operations," *Lawfare*, May 15, 2018, https://www.lawfareblog.com/states-proxies-cyber-operations.
[70] BBC, "Google Outrage at 'NSA Hacking,'" *BBC News*, October 31, 2013, sec. US & Canada, https://www.bbc.com/news/world-us-canada-24751821; T. C. Sottek, "Everything You Need to Know About PRISM," *The Verge*, July 17, 2013, https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet.
[71] Masashi Crete-Nishihata, Ronald J. Deibert, and Adam Senft, "Not by Technical Means Alone: The Multidisciplinary Challenge of Studying Information Controls," *IEEE Internet Computing* 17, no. 3 (May 2013): 34–41.
[72] Morozov, *The Net Delusion: The Dark Side of Internet Freedom*.

Twitter to postpone an update to its services, in order to not disrupt social media services during Iranian protests, since protesters were partly reliant on the same social media platform for organisational purposes.[73] The US government confirmed the request to Twitter to keep its services running, but it said that it was not meddling in Iranian internal affairs.[74]

Does this secrecy in the cyber domain prevent scholars from researching it? James de Waal, a Senior Fellow at Chatham House draws an analogy with the study of Special Operations Forces. Even though their precise actions are not reflected in official policy documents and evidence of their actions is scant, Special Operations Forces are an integral part of US strategy and behaviour.[75] De Waal continues by saying that scarce evidence of Special Operations Forces activities has not precluded a prolific research community from emerging.[76] Similarly, it may be argued that greater secrecy does not rule out academic writing on the diffusion of norms in the cyber domain.

This study relies on data gathered from secondary and primary sources. Valuable sources that help to address the obstacles of governmental secrecy in cyberspace are: reports by independent research organisations (Citizen Lab, Berkman Klein Center for Internet and Society) and think tanks (Brookings Institution), articles in traditional media (e.g. The New York Times, The Guardian), and journal articles. Primary sources in this thesis include interviews with government officials; government websites; as well as company

[73] Mark Landler and Brian Stelter, "Washington Taps Into a Potent New Force in Diplomacy," *The New York Times*, June 16, 2009, sec. Middle East, https://www.nytimes.com/2009/06/17/world/middleeast/17media.html.
[74] Ibid.
[75] Valentin Weber, "Linking Cyber Strategy with Grand Strategy: The Case of the United States," *Journal of Cyber Policy*, August 17, 2018.
[76] Ibid.

websites and marketing material (all of which are used to measure technology diffusion); government documents, and laws. Some examples of documents that this thesis analyses are: Russia's information security doctrine from 2000, the 2019 Thai cybersecurity law, the 2017 Vietnamese cybersecurity law, the 2018 Egyptian cybersecurity law, Russia's 2012 law to establish a blacklist, and a Thai government document that directs government entities to model its internet infrastructure in the image of China's. While government documents may be unreliable and not show the true intentions of public authorities, I cross-reference government documents and interviews with expert interviews, journal and newspaper articles as well as reports by independent research organisations that analyse government policy documents and laws. Such documents reflect the policies of states over years and therefore serve researchers who analyse evolving policies.

This thesis uses primary sources to study the perception of political elites. Ripsman et al. mention that in order to study perception researchers need to study primary sources:

"The best way for a neoclassical realist researcher to be certain that he/she understands the reasons why state decision makers took the policies that they did, therefore, would be to consult primary sources—such as government documents, memoirs, speeches, decision-maker interviews, and oral histories— in addition to secondary sources. "[77]

Once collected, those primary sources need to be examined for the logic of elite reasoning based on the neoclassical realist framework.[78]

[77] Steven E Lobell, Jeffrey W Taliaferro, and Norrin M Ripsman, "A Methodology of Neoclassical Realism," in *Neoclassical Realist Theory of International Politics*, vol. Oxford University Press (New York: New York: Oxford University Press, 2016).
[78] Sachio Nakato, "North Korea's Second Nuclear Test: Neoclassical Realism Perspectives: North Korea's Second Nuclear Test," *Pacific Focus* 27, no. 1 (2012): 10–35, doi:10.1111/j.1976-5118.2012.01074.x.

In order to study perceptions, this thesis examines speeches of politicians, conducts interviews with the political elites in the examined countries. This may be government ministers who were in power during the studied time period, opposition politicians, or members of parliament who are in charge of media and broadcasting committees in parliament. Similarly to other neoclassical realist analyses, empirical evidence gathered is then mustered for practical reasoning, which is driven by concerns of survival and the quest for influence.[79]

This thesis conceives leader perceptions as following a rational logic, but this does not prevent them from sometimes misperceiving the situation and taking irrational decisions.[80] Holsti mentions that these challenges could be due to cognitive limits on the capacity of human beings to examine information, particularly in times of upheaval, when every decision could have major impacts.[81]

Other valuable data to trace the export of censorship and surveillance technology, for instance, comes from private companies, such as Huawei, ZTE, or Protei. The difficulty with this kind of data is that it is often deleted after a few months. There is no proper archiving occurring on these websites. In order to mitigate the disappearance of vital evidence, this thesis maintains a Zotero repository with snapshots of the websites and marketing material of companies. This thesis also uses the "Wayback Machine", a service which archives the internet.[82] This helps with uncovering marketing material from

[79] Giorgi Gvalia, Bidzina Lebanidze, and David S. Siroky, "Neoclassical Realism and Small States: Systemic Constraints and Domestic Filters in Georgia's Foreign Policy," *East European Politics* 35, no. 1 (January 2, 2019): 21–51, doi:10.1080/21599165.2019.1581066.
[80] Olavi Rudolf Holsti, "Theories of Crisis Decision-Making," in *Diplomacy: New Approaches in History, Theory, and Policy* (New York: Free Press, n.d.), 99–136.
[81] Olavi Rudolf Holsti, "Theories of Crisis Decision-Making," in *Diplomacy: New Approaches in History, Theory, and Policy* (New York: Free Press, n.d.), 99–136.
[82] "Wayback Machine," accessed April 15, 2021, https://web.archive.org/.

company websites that may have already been deleted and hence allows for additional data to be uncovered.

2.2. Methods

This section highlights the methods used in this thesis: case study analysis, process tracing, and interviews.

2.2.1. Case study research

The thesis uses case study analysis as its main research method. Case study research as a social science method is widely recognised as a vigorous research method, including in the subfield of IR.[83] John Gerring defined case study research as "an intensive study of a single unit with an aim to generalize across a larger set of units."[84] The set of units is eventually integrated in a single study.[85]

The chosen method has its limitations. Robert K. Yin criticises the limited number of cases that are chosen to draw larger conclusions of a phenomenon.[86] However, the focus of this thesis is to explain why internet freedom/sovereignty has diffused from the US, Russia and China. The aim of this thesis is not to generalise its findings to other cases.

[83] Andrew Bennett and Colin Elman, "Case Study Methods in the International Relations Subfield," *Comparative Political Studies* 40, no. 2 (February 1, 2007): 170–95.
[84] John Gerring, 'What Is a Case Study and What Is It Good For?', *The American Political Science Review* 98, no. 2 (2004): 341.
[85] Ibid.
[86] Robert K. Yin, *Case Study Research: Design and Methods* (Sage Publications, 1984).

Cases

This thesis chose to study the US (internet freedom), Chinese and Russian (internet sovereignty) norms, because they represent the cyber norms that have – so far – diffused most broadly and deeply across the world.[87] As Stephen M. Walt notes, IR scholars prefer to study more important phenomena rather than trivial ones.[88]

This thesis focusses on the US, as opposed to on the EU, because the two visions of the internet are broadly aligned. For instance, the discourse on multistakeholderism and internet freedom efforts (defending an open and interoperable internet) voiced by European countries is largely aligned with how the internet was envisioned by the US.[89]

At the same time, while individual member states of the EU have international influence on digital affairs, the EU is still not an actor with a coherent foreign policy. There is too much of a diversity of actors for it to be likened to the US, China or Russia. Carrapico and Barrinha highlighted in their studies that:

> "both the architecture put in place under the EU [Cyber Security Strategy] and the resistance from Member States to allow the EU to have a more stringent control over their cyber activities, limit the EU's coherence in the field."[90]

---

[87] Other norms have diffused too. To give an example, the Iranian norm, the "Halal internet" is diffusing to other Muslim countries, such as Pakistan. The goal is to establish an intranet that is entirely in line with religious practices of a country. Neal Ungerleider, "Iran Cracking Down Online With 'Halal Internet,'" *Fast Company*, April 18, 2011, https://www.fastcompany.com/1748123/iran-cracking-down-online-halal-internet.

[88] Stephen M. Walt, *Revolution and War* (Ithaca and London: Cornell University Press, 1997).

[89] Freedom Online Coalition, "FOC Issues Joint Statement on Freedom of Expression Online at the 47th Session of the United Nations Human Rights Council," *Freedom Online Coalition*, July 4, 2021, https://freedomonlinecoalition.com/foc-issues-joint-statement-on-freedom-of-expression-online-at-the-47th-session-of-the-united-nations-human-rights-council/; Sozialdemokratischen Partei Deutschlands (SPD), BÜNDNIS 90 / DIE GRÜNEN, and Freien Demokraten (FDP), "Koalitionsvertrag 2021 – 2025 Zwischen Der Sozialdemokratischen Partei Deutschlands (SPD), BÜNDNIS 90 / DIE GRÜNEN Und Den Freien Demokraten (FDP)," 2021; Vincent Manancourt, "The Demise of Privacy Shield May Be the End of US-Europe Data Transfers," *POLITICO*, August 3, 2020, https://www.politico.eu/article/privacy-shield-is-dead-long-live-data-localization/.

[90] Helena Carrapico and André Barrinha, "The EU as a Coherent (Cyber)Security Actor?," *Journal of Common Market Studies* 55, no. 6 (2017): 1254–72, doi:10.1111/jcms.12575.

Meta-cases

The US, China, and Russia are the meta cases – they are the origins of the three cyber norms.

Observations

Then, when it comes to diffusion there are many potential sub-cases or so-called observations.[91] The thesis selects a few observations for each meta-case and examines them over a longer period of time.[92]

Observations are chosen for each meta-case combining the most similar and least-similar case comparison methods.[93] The idea behind most similar case comparison is to identify cases that are as alike as possible and differ only in one independent variable (either in IV1 or IV2 in this thesis) and the dependent variable (DV1). In that way it is possible to single out the root cause of a certain phenomenon. This thesis examines observation A at T-0 (time 0) and compares it to observation A at T-1 (time 1). It seeks to demonstrate that observation A is the same at T-0 and at T-1 except for the independent variable that has changed. This change in the independent variable had a change in the dependent variable as an outcome. To illustrate this, Thailand started to import Chinese technology after serious domestic protests that changed leaders' perception of the internet as a tool that can threaten their regime (IV2). Thailand in March (T-0) was the same country in terms of geography, population, and size as it was in June of 2010 (T-1). The only factor that

[91] Gary King, Robert O Keohane, and Sidney Verba, *Designing Social Inquiry : Scientific Inference in Qualitative Research*, Scientific Inference in Qualitative Research (Princeton, New Jersey: Princeton University Press, 1994).
[92] Audie Klotz and Cecelia Lynch, *Strategies for Research in Constructivist International Relations*, International Relations in a Constructed World (Armonk, N.Y.: M.E. Sharpe, 2007).
[93] Bennett and Elman, "Case Study Methods in the International Relations Subfield."

changed is the increased regime threat perception (IV2) in June 2010 which resulted from the massive protests that occurred in the country from March-May of that year and that eventually led to the import of Chinese surveillance technology (DV1). The least-similar case comparison method is used to compare observation A (Thailand) to observation B (Nicaragua) during both time periods (T-0 and T-1).[94] Observations A and B are very different, they have a different population, size, and geography, but they share one independent variable, namely China's seeking of influence (IV1). In Thailand, Chinese technology diffused because China expected to gain influence through the export of surveillance technology. In Nicaragua it did not diffuse because China likely wanted to withhold exports until Nicaragua ceased its diplomatic relations with Taiwan.

US internet freedom observations

With regards to the internet freedom norm, I chose the observations depending on where the US "sought influence" (IV1). Since the US was already a global superpower in the 1980s/1990s and sought to "export" internet technologies (and with it, freedom) everywhere, every country was a potential observation. The potential universe of cases is also large, when choosing based on countries that perceived the internet as a tool that propels economic growth (IV2). In the 1980s and 1990s, countries had no reason yet to perceive the internet as threatening to their regime, since it was not yet available to the broad public at that time. The internet was primarily seen as a means to achieve economic growth. Based on IV1 and IV2, this thesis decided to study China, countries that form the "Freedom Online Coalition +", and North Korea. These are countries where the US sought influence (IV1) and where the internet was seen as a tool to propel economic growth (IV2).

[94] Ibid.

Chinese internet sovereignty observations

For the Chinese internet sovereignty norm case study, I selected observations based on which countries China is expected to "seek influence" over. Those are two groups of countries. On the one hand, those are countries located along the BRI trade routes, and on the other hand, Taiwan allies. An additional requirement for countries to be considered as observations is that they all have to have a "high threat perception" (likely induced through domestic protests). Observations selected on the basis of these criteria are: Bahrain, Egypt, Iran, Nicaragua, Syria, Tanzania, Thailand, Uganda, Vietnam, Zambia, and Zimbabwe.

Russian internet sovereignty observations

I selected observations based on whether they share both IV1 and IV2, which could have had an effect on norm diffusion. The universe of observations hence includes member countries of the CIS (Russian seeking of influence) and countries which had a high regime threat perception (e.g., induced through recent protests powered by internet technologies) that may have propelled imports. Based on these criteria the observations chosen are: Belarus, Kazakhstan, Kyrgyzstan, Ukraine, and Uzbekistan.

Time period

The period of Chinese and Russian case studies is fixed to around 2010 – when Chinese and Russian information control norms started to gain traction around the globe – until today. The internet freedom case study tracks diffusion from the 1980s, through 2011 (when diffusion slowed down) and until today when only few countries still hold onto internet freedom.

Cases studies	Internet freedom	Chinese internet sovereignty	Russian internet sovereignty
Meta-cases	US	China	Russia
observations	China, Freedom Online Coalition +, North Korea	Bahrain, Egypt, Iran, Nicaragua, Syria, Tanzania, Thailand, Uganda, Vietnam, Zambia, Zimbabwe	Belarus, Kazakhstan, Kyrgyzstan, Ukraine, Uzbekistan
Time period	1980s – today	Around 2010 – today	Around 2010 – today

Table 2: Case study

2.2.2. Process tracing

I have chosen case study analysis and process tracing methodologies, because they help me with answering the *why question* that this thesis is seeking to answer. Why have Chinese and Russia norms diffused so successfully? Why have elites across the world embraced Chinese technologies and techniques? Case study analysis and process tracing are very fitting methodologies in this respect. They allow me to study a particular case in detail, across a longer period of time and establish an argument as to why China and Russia export and importing countries acquire technology and techniques from China and

Russia.[95] Establishing a timeline of critical events, for example is crucial, since it helps me to test my argument, which posits that authoritarian elites are more likely to acquire information control technologies and techniques after major protests or coup d'états.[96]

By using those two methodologies this thesis follows in the footsteps of many norm diffusion studies that have found those methodologies useful, too, to test the arguments they made.[97]

There are some drawbacks however with process tracing. Checkel mentions that it requires a lot of time to collect relevant information, to schedule and conduct in-depth interviews.[98] This needs to be taken into account when conducting research. Another limitation is how "micro" one is willing to go. In my study I traced the export of technology. I could have interviewed officials in cities where technology was deployed in order to study when a set of surveillance cameras became operational as well as if the technology that was acquired became operational at all. Due to temporal and travel constraints such research was not conducted during this project.

For the purpose of studying internet freedom/sovereignty diffusion in a neoclassical realist tradition of thinking, this method is superior to purely quantitative methods, which

---

[95] James Mahoney, "Process Tracing and Historical Explanation," *Security Studies* 24, no. 2 (2015): 200–218.
[96] Andrew Bennett, "The Oxford Handbook of Political Methodology," 2008.
[97] Katja Bender, Sonja Keller, and Holger Willing, "The Role of International Policy Transfer and Diffusion for Policy Change in Social Protection – A Review of the State of the Art," *IZNE Social Protection Working Paper*, 2014, https://www.h-brs.de/files/izne/policy_diffusion_1.pdf; Sunayana Ganguly, "A Constructivist Analysis Linking Norm Diffusion to Policy" (Berlin, 2010), https://refubium.fu-berlin.de/bitstream/handle/fub188/18589/Ganguly-A_constructivist_analysis_linking_norm_diffusion-269.pdf?sequence=1&isAllowed=y; Susan Park, "Norm Diffusion Within International Organizations: A Case Study of the World Bank," *Journal of International Relations and Development Volume*, 2005, 111–41; Elvira Rosert, "Norm Emergence as Agenda Diffusion: Failure and Success in the Regulation of Cluster Munitions," *European Journal of International Relations* 25, no. 4 (2019): 1103–31, doi:10.1177/1354066119842644.
[98] Jeffrey T. Checkel, "Process Tracing," in *Qualitative Methods in International Relations : A Pluralist Guide*, ed. Audie Klotz and Deepa Prakash, Research Methods Series (Basingstoke: Palgrave Macmillan, 2008).

could highlight successful diffusion, but not answer "why" internet freedom/sovereignty diffused successfully.[99]

In order to get to the "why" I use process tracing. I study diffusion by measuring the impact of independent variables that explain the supply (perception underlying export is seeking of influence) and demand side of internet sovereignty diffusion (regime threat concerns) as well as internet freedom diffusion (expectation that internet will propel economic growth) on the dependent variable (norm diffusion). When supply and demand meet internet freedom/sovereignty norm diffusion is likely to occur. The independent variables explain why the US, Chinese and Russian norms have been so successful, at various points in time, while the dependent variable shows that Washington's, Beijing's, and Moscow's norms actually diffused successfully across the globe. The two alternative independent variables are ideational persuasion and geographical closeness.

While states like the US, Russia, and China export technology and techniques in order to gain influence, states like Zimbabwe or Tanzania import the cyber norms because they were keen on boosting their economic growth with the arrival of the internet (internet freedom) or because now that they have realised its revolutionary potential, they want to ensure their regime survival (internet sovereignty).

The supply side independent variable of information control diffusion is Washington's, Moscow's, and Beijing's seeking of influence across the globe, within the BRI, and CIS, respectively. Initiatives such as the BRI show, for instance, Beijing's strong commitment to involved countries and its ambition to obtain some influence over the targeted

[99] Gerring, "What Is a Case Study and What Is It Good For?"

countries. The central argument of this thesis is that precisely because Beijing considers some geographical areas to be strategic, it fosters exports to these areas, which increase the likelihood of diffusion.

The initial excitement about the potential of the internet to propel economic growth provides an insight into why so many countries imported internet technologies in the 1980s and 1990s. Later on, the perceived pressure of regime survival (resulting from the same technology) explains why countries began to imitate China and Russia. Imitation of Chinese and Russian norms, by countries, such as Zimbabwe and Kazakhstan, is a strategy to ensure their internal domestic hierarchy.[100] Imitation of the Chinese and Russian norms is a strategy that is almost exclusively deployed by hybrid/authoritarian regimes after large-scale protests or a coup d'état – both events increase the perception of regime threat within ruling elites. In this thesis, regime type (democratic/hybrid/authoritarian regime) is defined according to the Economist Intelligence Unit's Democracy Index.[101]

One could argue against perception underlying export (seeking of influence)/import (regime survival concerns and economic growth expectations) as explanatory variables by saying that actually it is the density of ties between countries (linkage) to build hypotheses in regards to the diffusion of norms.[102] In their studies, Levitsky and Way, examine the concept of linkage with regards to the ties between the West and certain

[100] Kadercan, "Making Sense of Survival: Refining the Treatment of State Preferences in Neorealist Theory."
[101] The Economist also distinguishes between full democracy and flawed democracy, a distinction which is not made explicitly in this thesis. The Economist, "The Retreat of Global Democracy Stopped in 2018."
[102] 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.

authoritarian-leaning regimes in the post–Cold War era. Wherever high linkage was present, they found democratisation was more likely to occur.[103] The best proxy for linkage is geographical closeness. In other words, the closer two countries are, the higher the bilateral linkage, the more likely norms/practices are likely to diffuse. Scholars such as Ambrosio and Weyland have also considered the argument of geographical closeness in the context of authoritarian diffusion and come to a similar conclusion as Levitsky and Way.[104]

The second alternative variable that may explain internet freedom/sovereignty diffusion is ideational persuasion. The US, China, and Russia persuade countries to adopt internet freedom/sovereignty. Constructivism would purport that countries import the internet sovereignty norm because China convinced them to do so, just like Gorbachev ordered glasnost and perestroika due to persuasion from the West.[105]

The effect of the independent variables on diffusion is measured by changes in the dependent variable 1. DV1 measures norm diffusion and is comprised by three indicators (technology transfer, imitation, training). This thesis uses two indicators to measure the supply side (technology transfer, training) and one indicator (imitation) to measure the demand side of diffusion. Tracing the diffusion of technology and training is important, since imitation rarely occurs without them. Technology transfer and training often enable imitation (advanced norm diffusion). The purpose of using these three indicators is to

[103] Ibid.

[104] 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; Thomas Ambrosio, "Constructing a Framework of Authoritarian Diffusion: Concepts, Dynamics, and Future Research," *International Studies Perspectives* 11, no. 4 (2010): 375–92; Weyland, "Crafting Counterrevolution: How Reactionaries Learned to Combat Change in 1848."

[105] William Wohlforth, "Realism and the End of the Cold War," *International Security* 19, no. 3 (1994): 91–129.

measure the breadth and depth of the spread of American, Chinese and Russian tactics and technologies to other states. 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 or two indicators of diffusion, it is deemed to be located at the periphery of a technosphere. If a country checks all three indicators, the diffusion is deemed to be more profound. It might be also that parts of the US, Russian and Chinese technospheres overlap in some geographical areas.

The second dependent variable (DV2) of this thesis sheds light on the diffusion's impacts on the sovereignty of importing countries. It is the direct consequence of DV1, which highlights norm diffusion. Once diffusion has occurred (DV1), the consequence is a weakening of the importing country's Westphalian sovereignty and shaping of its domestic and interdependence sovereignty (DV2). In short DV1 is about behaviour, while DV2 is about the consequence of behaviour.

2.2.3. Interviews

Twenty-one semi-structured interviews were held with current and former government officials, opposition politicians, as well as US, China, and Russia experts working in the internet freedom/sovereignty realms. This should allow the thesis to get a clearer view on the diffusion of cyber norms, as well as inform, confirm, or debunk the findings of case study, and process tracing. Semi-structured interviews have the benefit of allowing a flexible and fluid structure. "Meanings and understandings are created in an interaction, which is effectively a co-production, involving the construction or reconstruction of knowledge."[106] In contrast, they potentially involve a researcher bias. Interviewers may

[106] Jennifer Mason, *Qualitative Researching*, 2nd ed. (Sage Publications, 2002).

use the interviews to confirm their preconceived ideas and arguments. They may misperceive what the interviewee is trying to express. On the interviewee's side, they may misunderstand the question.[107] I have mitigated those potential biases by following the approach suggested by Alshenqueeti, namely "avoiding asking leading questions, taking notes not just depending on (tape) recorders, conducting a pilot interview; and giving the interviewee a chance to sum up and clarify the points that they have made."[108]

A limitation of this thesis is that the interviewees are exclusively based in North America, Europe, Africa, and Southeast Asia. The reason for this geographical imbalance is that I fear that experts based in China and Russia may be unwilling or unable to share their views, since their personal safety may be endangered if they do so.

Interviewee	Identifier	Affiliation	Sector	Case study	Date
1	Christopher Painter	First Coordinator for Cyber Issues in the US Department of State and President of Global Forum on Cyber Expertise	Government and not-for-profit	Internet freedom	2 May 2019
2	Chinmayi Arun	Resident Fellow at Yale Law School	Academia	Internet freedom	27 May 2019
3	David Kaye	UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression and Professor at University of California Irvine	International organisation, academia	Internet freedom	20 May 2019
4	David Sullivan	Program Director at the Global Network Initiative	Not-for-profit	Internet freedom	23 April 2019
5	Jason Pielemeier	Policy Director at the Global Network Initiative and	Government and not-for-profit	Internet freedom	20 May 2019

[107] Louis Cohen, Lawrence Manion, and Keith Morrison, *Research Methods in Education*, 6th ed. (London: Routledge, 2007).
[108] Hamza Alshenqueeti, 'Interviewing as a Data Collection Method: A Critical Review', *English Linguistics Research* 3, no. 1 (31 March 2014): 44.

		previously a Special Advisor at the US Department of State, where he led the Internet Freedom, Business and Human Rights section in the Bureau of Democracy, Human Rights and Labor			
6	Rebecca MacKinnon	Founding Director of Ranking Digital Rights	Not-for-profit	Internet freedom	14 June 2019
7	Sandy Ordonez	Head of Communications and Outreach at the Open Internet Tools Project and driving force behind the Internet Freedom Festival	Not-for-profit	Internet freedom	5 August 2020
8	Nani Jansen Reventlow	Director of Digital Freedom Fund	Not-for-profit	Internet freedom	4 June 2019
9	Joey Shea	Internet researcher and Egypt expert	Not-for-profit	Chinese internet sovereignty	26 March 2020
10	Allison McManus	Non-Resident Fellow at the Tahrir Institute for Middle East Policy	Not-for-profit	Chinese internet sovereignty	8 April 2020
11	Daniel Mwesigwa	Ugandan internet researcher	Not-for-profit	Chinese internet sovereignty	20 March 2020
12	Kasit Piromya	Thai Minister of Foreign Affairs from 2008-11; Member of the House of Representatives until the coup d'état of 2014	Government	Chinese internet sovereignty	25 June 2020
13	Ida[109]	Former Thai parliamentarian	Government	Chinese internet sovereignty	29 June 2020
14	Neil Blazevic	Technology Advisor at DefendDefenders, a Ugandan human rights organisation	Not-for-profit	Chinese internet sovereignty	8 April 2020
15	Kuda Hove	Zimbabwean internet researcher at Privacy International focussing on Sub-Saharan Africa	Not-for-profit	Chinese internet sovereignty	10 April 2020
16	Senator David Coltart	Member of Parliament in Zimbabwe's National Assembly from 2000-2008; since	Government	Chinese internet sovereignty	22 May 2020

[109] This is a pseudonym chosen by the interviewee to protect their identity.

		2008 a Member of the Senate; Minister of Education, Sport, and Culture from February 2009 – August 2013			
17	Arthur Gwagwa	Zimbabwean internet researcher	Academia	Chinese internet sovereignty	28 March 2020
18	Prince Sibanda	Member of Parliament since 2013. He is the Chairperson of the Parliamentary Portfolio Committee on Information Media and Broadcasting Service in the Zimbabwean National Assembly. In this role he oversees, monitors, and scrutinises Zimbabwe's Ministry of Information, Media and Publicity. He is a member of the largest opposition party, the Movement for Democratic Change Alliance	Government	Chinese internet sovereignty	17 June 2020
19	Christopher Schwartz	Journalist based in Bishkek, Kyrgyzstan	Journalism	Russian internet sovereignty	20 May 2020
20	Rebekah Overdorf	Internet researcher focussed on Central Asia	Academia	Russian internet sovereignty	20 May 2020
21	Etienne[110]	Threat Intelligence Analyst	Private sector	Russian internet sovereignty	10 April 2020

Table 3: List of interviewees

As part of laying out case study analysis, this thesis explains why it decided to study China, Russia, and the US, as well as specific countries that the respective norms diffused to, and the time frame of analysis for each case study. Process tracing was used to

[110] Ibid.

illuminate the impact of major events, such as protests on elites' regime threat perception, which aids to understand why internet sovereignty diffused. Furthermore, this chapter meticulously laid out with whom and how the semi-structured interviews were conducted.

Chapter 3: Literature review

This chapter provides an overview of the literature relevant to the study of internet freedom/sovereignty diffusion. It most importantly delves into the constructivist norm life cycle and shows how a gap exists in applying the life cycle to realist thinking. Furthermore, this part of the thesis lays out the neoclassical realist literature and the value of applying it to the study of norm diffusion – which this thesis does in Chapters 5, 6, and 7.

This chapter has four goals. First, it aims to show the significance of the existing literature on change in state behaviour for understanding internet freedom/sovereignty norm diffusion. It does so by laying out a major debate in IR between constructivists and realists as to why the Soviet Union ceased its confrontational approach with the US towards the end of the 20th century. This debate touches both on structural change in the international system (decline in relative power of the Soviet Union vis-à-vis the US) and change in the unit-level of analysis (perception change within Soviet leaders which prompted a change in Soviet state behaviour). This thesis examines the debate both on a structural and unit level. It emphasises the value of explaining change on a unit-level of analysis, which examines the effect of elite perception on change in state behaviour (neoclassical realism). This thesis uses a unit-level analysis to demonstrate how a change in perception within, e.g., Thai, and Ugandan elites, after major protests, results in a change in state behaviour (import of Chinese information control tools and techniques).

Second, this chapter seeks to identify useful bits within major IR theories and beyond (constructivism, realism, democratisation literature) that can inform the analysis of internet freedom/sovereignty diffusion. Particular attention is given to the constructivist

life cycle framework. This thesis argues that the elements of the life cycle that quantify diffusion (measuring the depth and breadth of international diffusion) are useful for the study of internet freedom/sovereignty diffusion. However, when it comes to studying the causes of diffusion, the life cycle needs a realist interpretation to account for the regime survival and sovereignty concerns of states. As a result, this thesis presents a life cycle, which places itself within the neoclassical realist school of thought. In this vein, Chapter 4 proposes a theoretical framework that identifies material interests of seeking of influence (supply side internet freedom/sovereignty) and regime survival concerns (demand side internet sovereignty) as well as the perception of the internet as an economic growth tool (demand side internet freedom), as the leading explanatory variables driving US, Chinese and Russian internet freedom/sovereignty diffusion. Many of these elite perceptions in the US, China, Russia and importing states such as Zimbabwe, Thailand, or Japan are driven by external pressures of survival, both domestic (street protests) and international in nature (economic/intelligence/military competition amongst states), that incentivise elites into amassing economic, security, and scientific assets. The elite thinking in Washington, D.C., Beijing, and Moscow is that promoting their cyber norms will bring them more normative and economic power, thereby increasing their share of relative power in the international system (coping with pressure from above). On the other hand, in norm adopting countries, authoritarian elites perceive the adoption of cyber norms as increasing their chances of regime survival (coping with pressure from below).

In the empirical chapters, the thesis tests the neoclassical realist (materialistic) argument against constructivist and geographical proximity explanations. In this way, this thesis is one of the first academic works to lay out the causes of internet freedom/sovereignty diffusion within a realist life cycle framework and thereby seeks to fill a considerable gap

in IR literature.

Third, the chapter seeks to place discussion surrounding the concept of sovereignty in IR into the context of this thesis. It does so by using Stephen Krasner's sovereignty framework (four types of sovereignty) to study internet sovereignty. This thesis maintains that Krasner's argument – that sovereignty is a norm upheld by states, but which is at the same time frequently violated by powerful states – is also applicable in cyberspace. China and Russia, in particular, have maintained that adopting internet sovereignty is beneficial to the importing state, but as the empirical chapters demonstrate, by importing the Chinese or Russian norms, importing countries become part of the Chinese, and Russian technological spheres of influence, in which these countries' sovereignty – based on their Westphalian understanding of it – can be violated more easily by the two hegemons (see Chapter sections 6.5.2. and 7.5.2.). The empirical chapters thereby show that sovereignty in cyberspace, is also, in the words of Krasner, "organised hypocrisy". This thesis contends further that there is a direct relationship between the degree of state sovereignty and the survival of the state, such that the total loss of sovereignty represents the state's non-existence. This thesis, therefore, sees regime survival concerns as a central feature of state survival, at least in relation to autocratic regimes; as we will see in the empirical chapters, it is what motivates states to act in the adoption of information controls. The import of information controls is perceived to increase authoritarian elites' sovereignty against their own citizens, while diminishing it vis-à-vis China and Russia (see chapter sections 6.5, 7.5.).

Fourth, this chapter lays out the significance of Internet Governance literature, and particularly of scholars Milton Mueller and Laura DeNardis, for the analysis of internet

freedom diffusion. Taking this baseline of literature, this thesis examines how internet (freedom) technologies were exported from the US to the rest of the world (Chapter 5).

3.1. Explaining state behaviour in IR

If one wishes to understand why internet freedom/sovereignty norms diffuse, then one needs to first ask a larger question: do material (distribution of capabilities and relative power) or ideational factors (social interaction between states) drive state behaviour (e.g., norm adoption)? This question produced a plethora of IR literature at the end of the Cold War, when scholars tried to explain the dissolution of the Soviet Union.[1] Many arguments were put forward, including that the Reagan administration's defence build-up (material factors) prompted a belief within Soviet elites that they could not compete anymore with the United States, or that both the personality (ideational factor) of Gorbachev (diverging from usual Soviet apparatchiks) and Reagan (an ideologue trying to win over Gorbachev) was crucial to bring about the fall of the Soviet Union.[2]

While the above arguments and the broader debate is important to acknowledge in explaining the downfall of the Soviet Union, this section of the chapter focusses on reviewing a particular debate between realists and constructivists, because the

[1] Concerning the discussion of the collapse of the Soviet Union that goes beyond the debate explored in this thesis see Nick Bisley, *The End of the Cold War and the Causes of Soviet Collapse* (Basingstoke: Palgrave Macmillan, 2004); Leon Aron, "Everything You Think You Know About the Collapse of the Soviet Union Is Wrong," *Foreign Policy*, June 20, 2011, https://foreignpolicy.com/2011/06/20/everything-you-think-you-know-about-the-collapse-of-the-soviet-union-is-wrong/; Knorr Mackensie, "Why Did Russia Let the Republics Go? Revisiting the Fall of the USSR | Wilson Center," 2017, https://www.wilsoncenter.org/publication/why-did-russia-let-the-republics-go-revisiting-the-fall-the-ussr; Diana Villiers Negroponte, "Would the Soviet Union Have Collapsed Without Mikhail Gorbachev?," *Brookings Institution*, October 17, 2019, https://www.brookings.edu/blog/order-from-chaos/2019/10/17/would-the-soviet-union-have-collapsed-without-mikhail-gorbachev/.

[2] Robert G. Patman, "Reagan, Gorbachev and the Emergence of New Political Thinking," *Review of International Studies* 25, no. 4 (1999): 577–601; Fred I. Greenstein, "The Impact of Personality on the End of the Cold War: A Counterfactual Analysis," *Political Psychology* 19, no. 1 (1998): 1–16.

fundamental debate between these two schools of IR in explaining the collapse of the Soviet Union is most relevant for the analysis of why US, Chinese, and Russian cyber norms diffuse (see Chapters 5, 6, and 7).

As mentioned above, the debate about change in IR was revived with the end of the Cold War. Why did the Soviet Union give up its power and stop confronting the United States? As Alexander Wendt wrote, "[m]ainstream IR theory simply had difficulty explaining the end of the Cold War, or systematic change more generally. It seemed to many that these difficulties stemmed from IR's materialist and individualist orientation, such that a more ideational and holistic view of international politics might do better."[3] This purported failure of realism contributed to the establishment of constructivism as a theory of IR and the literature surrounding ideational factors as an explanation of international politics rose significantly.[4] Many scholars, for instance, claimed that Gorbachev ordered perestroika because he wanted to join the West and give up socialism.[5]

Kratochwil, for his part, claims that Waltz's structural realism cannot explain the shifts that occurred in 1989/90, since the changes were not a consequence of redistribution or

[3] Alexander Wendt refers to systemic change by alluding to neorealist thinking. "Neorealism is a systemic theory in this … sense because it locates the key causes of international life in the system-level properties of anarchy and the distribution of capabilities." Alexander Wendt, *Social Theory of International Politics*, Cambridge Studies in International Relations (Cambridge, U.K.: Cambridge University Press, 1999: 12). Neoclassical realists integrate these claims from neorealism (structural analysis) but introduce the unit level analysis (elite perception) to explain change in state behaviour. See Wohlforth, "Realism and the End of the Cold War."

[4] Katzenstein, *The Culture of National Security : Norms and Identity in World Politics*; Wendt, *Social Theory of International Politics*; Rey Koslowski and Friedrich V Kratochwil, "Understanding Change in International Politics: The Soviet Empire's Demise and the International System," *International Organization* 48, no. 2 (1994): 215–47; Jeffrey T. Checkel, *Ideas and International Political Change : Soviet/Russian Behavior and the End of the Cold War* (New Haven: Yale University Press, 1997).

[5] Janice Gross Stein, "Political Learning by Doing: Gorbachev as Uncommitted Thinker and Motivated Learner," *Int Org* 48, no. 2 (1994): 155–83 John Mueller, "The Impact of Ideas on Grand Strategy," in *Domestic Bases of Grand Strategy*, ed. Richard Rosecrance and Arthur A. Stein (Ithaca: Cornell University Press, 1993); Friedrich Kratochwil, "The Embarrassment of Changes: Neo-Realism as the Science of Realpolitik Without Politics," *Review of International Studies* 19, no. 1 (1993): 63–80.

systemic factors, but rather domestic factors such as an emergence of civil society in Eastern Europe and the recognition of leading figures' powerlessness vis-à-vis domestic factors explain the changes.[6] However, Waltz never claimed that structural realism could explain the behaviour of states in all cases or in great detail.[7] Some realist scholars were not satisfied with this answer and they intended to add variables that could explain more specific cases of change. Neoclassical realism was thus born.

Wohlforth, a neoclassical realist, agrees with the post-cold-war criticism of neorealism and states that one needs to introduce the intervening variable of leaders' "perception" at the domestic level to explain the changes of 1989/90.[8] In other words, neoclassical realists add the unit level of analysis in addition to the systemic level of neorealist analyses.[9] This level of analysis to explain change in political elite perception, and consequently behaviour, is important, since this thesis' analysis aims to explain the export and import of internet freedom/sovereignty through a neoclassical realist framework of IR, which means that this thesis focusses on explanatory variables at the unit level (perception underlying export/import).[10]

The intervening variable at the unit level defines how the dependent variable is executed. Wohlforth, for example, introduces the "perception of power" intervening variable.[11] But how does perception change occur? Zakaria speaks of perceptual "shocks", where a

[6] Kratochwil, "The Embarrassment of Changes: Neo-Realism as the Science of Realpolitik Without Politics."
[7] Waltz, *Theory of International Politics*.
[8] Wohlforth, "Realism and the End of the Cold War."
[9] Adam Quinn, "Kenneth Waltz, Adam Smith and the Limits of Science: Hard Choices for Neoclassical Realism," *International Politics* 50, no. 2 (2013): 159–82.
[10] Rose, "Neoclassical Realism and Theories of Foreign Policy."
[11] Wohlforth, "Realism and the End of the Cold War."

sudden event or crisis makes policy makers aware of changes in relative power.[12] Policy makers then engage in intellectual learning. They change their beliefs and strategies of how to ensure survival.[13] In that process, leaders sometimes misperceive the situation. Schweller, for instance, makes the argument that the Soviet Union misperceived the distribution of power within Europe.[14] Stalin "expected a war of attrition in the West. The fall of France abruptly ended Stalin's dream of easy conquest in a postwar period when the rest of Europe would be exhausted."[15]

Whether it is perception or misperception, this intervening variable is essential to explain change on a unit level of analysis. Wohlforth claims that in the years before glasnost and perestroika, the Soviet Union was in economic decline.[16] This material factor (economic decline) precipitated a change in ideas of the leaders of the Soviet Union about relative Soviet power. Because Gorbachev recognised that the Soviet Union had no more the capabilities to compete, he stopped the Soviet Union's confrontational approach vis-à-vis the US.[17] In 2001, Brooks and Wohlforth added previously untouched data of global production and thereby reinforced their argument of just how strongly material incentives shaped Soviet leaders' ideas about relative decline compared to the US, which in turn prompted them to give up great power competition.[18] In the words of William C. Wohlforth:

---

[12] Fareed Zakaria, *From Wealth to Power : The Unusual Origins of America's World Role*, Princeton Studies in International History and Politics (Princeton, N.J.: Princeton University Press, 1998).
[13] Stephen G. Brooks and William C. Wohlforth, "Power, Globalization, and the End of the Cold War: Reevaluating a Landmark Case for Ideas," *International Security* 25, no. 3 (2001): 5–53.
[14] Randall L Schweller, *Deadly Imbalances: Tripolarity and Hitler's Strategy of World Conquest* (New York: Columbia University Press, 1998).
[15] Randall L Schweller, *Deadly Imbalances: Tripolarity and Hitler's Strategy of World Conquest* (New York: Columbia University Press, 1998): 168.
[16] Wohlforth, "Realism and the End of the Cold War."
[17] Ibid: 96.
[18] Stephen G. Brooks and William C. Wohlforth, "Power, Globalization, and the End of the Cold War: Reevaluating a Landmark Case for Ideas," *International Security* 25, no. 3 (2001): 5–53.

"Stalin, Khrushchev, and Brezhnev may have had many reasons for competing with the United States, but a necessary condition for competition was their perception that they had the capability to do so … Gorbachev may have had numerous reasons for seeking to withdraw from the rivalry with the United States, but a necessary precondition was the perception of reduced capability to continue competing."[19]

In other words, a major reason for the Soviet Union reducing its confrontational approach towards the US is because Soviet elites, and principally amongst them Gorbachev, stopped believing that they had the economic means to compete with the US and spend vast resources on defence capabilities.

Several scholars are critical of treating perception as an intervening variable. Margarita H. Petrova claims that "the most problematic point of the realist analyses deals with the relationship between material factors and new thinking ideas."[20] She refers to a passage in Schweller and Wohlforth's article which stipulates that "change in ideas… tended to move in tandem with changes in policy that were necessitated by material pressure."[21] She states that by doing so, Schweller and Wohlforth reduce ideational factors to material factors.

Other scholars' criticism arose because realists provided little evidence as to the causality of change in the Soviet Union. The evidence provided by neoclassical realists was countered by authors such as English or Kontorovich.[22] English suggests that new

[19] Wohlforth, "Realism and the End of the Cold War,": 96.
[20] Margarita H. Petrova, "The End of the Cold War: A Battle or Bridging Ground Between Rationalist and Ideational Approaches in International Relations?," *European Journal of International Relations* 9, no. 1 (2003): 115–63., 128.
[21] Randall L Schweller and William C Wohlforth, "Power Test: Evaluating Realism in Response to the End of the Cold War," *Security Studies* 9, no. 3 (2000): 91.
[22] Robert English, *Russia and the Idea of the West : Gorbachev, Intellectuals, and the End of the Cold War* (New York: Columbia University Press, 2000); Vladimir Kontorovich, "The Economic Fallacy," *The National Interest*, no. 31 (1993): 35–45.

thinking has occurred already before economic decline.[23] He claims that the crackdown on the Prague Spring had lasting impacts on Soviet thinking. Hence ideational factors matter according to English. Kontorovich argues in a similar vein that Gorbachev's reforms came before the Soviet economic decline.[24] In order to avoid such criticism relating to causality, this thesis engages in meticulous process tracing research to show, for instance, the effect of the independent variable 2 (regime threat perception) on the dependent variable 1 (internet sovereignty diffusion).

3.2. Norm diffusion

The importance of material factors in producing state behaviour (norms) applies to the literature surrounding the international diffusion of state behaviour (norm diffusion) too. Why do norms diffuse? Why do some countries imitate the governmental policies of other countries? This question has been mostly treated by the three broad schools of IR (realism, neoliberalism, and constructivism), which place norms within the larger concept of "regimes".

Regimes are understood as "sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given area of international relations."[25] Principles are beliefs of causation or fact. Whereas norms are prescriptions for behaviour, rules prescribe or proscribe action. After having agreed on principles, norms, and rules, states define the decision-making procedures, which

[23] English, *Russia and the Idea of the West : Gorbachev, Intellectuals, and the End of the Cold War*.
[24] Kontorovich, "The Economic Fallacy."
[25] Stephen D. Krasner, "Structural Causes and Regime Consequences: Regimes as Intervening Variables," *International Organization* 36, no. 2 (1982): 185–205.

usually involves setting up organisations to implement international cooperation/ regimes/institutions.[26]

Mueller et al. illustrate how regimes, and with them norms, could emerge when it comes to internet governance.[27] They present a set of principles and norms that states should agree upon. They maintain that one commonly accepted principle is that the internet is largely composed of private networks. As a consequence, they propose a norm that "multistakeholder governance [involving the state, private companies and individuals] should be legitimized and maintained."[28] They do not go further into rules and decision-making procedures, but one could add to their account that a rule of the regime could be that states should not nationalise their domestic internet infrastructure and a decision-making procedure could entail further enshrining the role of private companies in major internet governance organisations such as ICANN (Internet Corporation for Assigned Names and Numbers) or the ITU (International Telecommunication Union).

According to rationalist IR scholars (including neorealists and neoliberals), norms are a result of the "logic of expected consequences".[29] In this logic, actors pick from different actions by evaluating their consequences and choose the one that suits them best.[30] In this calculation they assume that other actors follow the same logic.[31] Rational actors are set within an anarchical structure, which makes cooperation difficult (since no international

[26] Ibid.
[27] Milton Mueller, John Mathiason, and Hans Klein, "The Internet and Global Governance: Principles and Norms for a New Regime," *Global Governance: A Review of Multilateralism and International Organizations* 13, no. 2 (2007): 237–54.
[28] Ibid: 250.
[29] Grieco, "Anarchy and the Limits of Cooperation: A Realist Critique of the Newest Liberal Institutionalism"; Mearsheimer, *The Tragedy of Great Power Politics*; Rose, "Neoclassical Realism and Theories of Foreign Policy."
[30] Hechter and Kanazawa, "Sociological Rational Choice Theory."
[31] Ibid.

authority exists to enforce promises states make to each other), but not impossible.[32] Both the neoliberal and realist schools expect limited cooperation to emerge from this anarchical environment.

Realists maintain that cooperation is, just like conflict, a derivative of the distribution of power.[33] For instance, the international security regime amongst states, is enshrined in Chapter VII of the UN Charter, which states that "[t]he Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression" and may take any military or non-military action "to restore international peace and security."[34] At the same time, the international security regime rests on a constant balancing and armament between the major powers themselves and vis-à-vis the rest of the world, i.e., the regime is a reflection of the distribution of power.[35] Realists contend that regimes only emerge when they are most beneficial to a hegemonic power or a coalition of hegemonic powers (in the case of the UN Security Council).[36] Hegemonic powers are careful that weaker states do not gain a free ride or are cheating. The regime exists mainly because of the hegemonic power's choice and the relative power it may gain because of it.[37] Grieco puts forward another hypothesis of regime emergence. He posits that regimes generally emerge as a consequence of weaker states' insecurity.[38] By entering a regime, weaker

[32] Grieco, "Anarchy and the Limits of Cooperation: A Realist Critique of the Newest Liberal Institutionalism."
[33] Krasner, "Structural Causes and Regime Consequences: Regimes as Intervening Variables."
[34] United Nations, "Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression (Articles 39-51)," *United Nations* (United Nations), accessed April 5, 2021, https://www.un.org/en/about-us/un-charter/chapter-7.
[35] Susan Strange, "Cave! Hic Dragones: A Critique of Regime Analysis," *Int Org* 36, no. 2 (1982): 479–96.
[36] Andreas Hasenclever, Peter Mayer, and Volker Rittberger, *Theories of International Regimes*, Cambridge Studies in International Relations (Cambridge: Cambridge University Press, 1997).
[37] Robert Jervis, "Security Regimes," *Int Org* 36, no. 2 (1982): 357–78.
[38] J. M. Grieco, "Understanding the Problem of International Cooperation: The Limits of Neoliberal Institutionalism and the Future of Realist Theory.," in *Neo- Realism and Neoliberalism: The Contemporary Debate*, ed. D. A. Baldwin (New York, N.Y.: Columbia University Press, 1993).

states hope to minimise their relative losses that they would have to suffer, if they were left out of a regime, and in the perspective that they do not have other ways of gaining relative power than through international regimes.[39]

Neoliberals, in particular, argue that in a complex world of increased interdependence between states, cooperation, i.e. the emergence of international regimes, is more likely.[40] Neoliberal scholars argue that by establishing norms, and regimes more generally, states are able to decrease their costs of transaction, and reduce the likelihood of uncertainty that anarchy causes.[41] When the focus of realists is to focus on relative gains compared to others, neoliberals focus on individual absolute gains.[42] In neoliberal thinking a state might establish a regime with a major competing power, if both the former and the latter state's gains are equal. In realist thinking the former state might refrain from entering such a regime, since the relative gain would be close to 0 and considerably empower a major competitor.[43]

Constructivists for their part criticise neoliberalism, as well as realism, for their claim that identity and (rational) behaviour remain stable.[44] They posit that this leaves out the possibility of ideological competition affecting cooperation.[45] Constructivists emphasise that regimes are a product of the ideational objectives of states as much as they are a

[39] Ibid.
[40] Robert O Keohane and Joseph S Nye, *Power and Interdependence*, 2nd ed. (New York: Longman, 1989).
[41] Robert O Keohane, "The Demand for International Regimes," *International Organization* 36, no. 2 (1982): 325–55.
[42] Ibid.
[43] Stephen Krasner, "Transforming International Regimes: What the Third World Wants and Why," *International Studies Quarterly* 25, no. 1 (1981): 119.
[44] Benjamin Meiches and Raymond Hopkins, "Regime Theory," *Oxford Research Encyclopedia of International Studies*, 2018.
[45] Ibid.

product of their material interests.[46] This view follows a "logic of appropriateness", where states act in accordance with their identities that are tied to rules instead of merely following their rational calculations in pursuit of material interests.[47] Jack Donnelly, for instance, argues that states may follow the UN's human rights regime (e.g. UN Declaration of Human Rights) because of moral interests and that those ideational interests, which are engrained in an actor's identity are just as important as material interests.[48] Despite actors having subscribed to these norms, they have violated them repeatedly. However, Donnelly points to the fact that in the 1940s when the human rights regime first appeared, even such commitments and voicings to oblige with norms were surprising, taking into account that previously such commitments had been out of the question.

One major example of the logic of appropriateness is Finnemore and Sikkink's norms life cycle. It illustrates the transition of one state of affairs – where one logic of appropriateness (LoA 1 – women cannot and shall not vote) applies – to a new state of affairs where another logic of appropriateness applies (LoA 2 – women can and shall vote). According to the authors, the logic of appropriateness as regards to women's voting rights has diffused internationally, starting with an emergence of the regime, followed by a cascade (a considerable number of countries accepts a norm), and finally it was internalised by almost all countries.

[46] Finnemore and Sikkink, "International Norm Dynamics and Political Change"; Maurer, "Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-Security"; Acharya, "How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism."

[47] March and Olsen, "The Institutional Dynamics of International Political Orders."

[48] Jack Donnelly, "International Human Rights: A Regime Analysis," *Int Org* 40, no. 3 (1986): 599–642.

This thesis contends that the elements of the life cycle that quantify diffusion (measuring the depth and breadth of international diffusion) are useful for the study of internet freedom/sovereignty diffusion. The former – breadth – concerns the number of countries adopting a norm and relative weight of a country in the respective topical area, i.e., France and Great Britain in regard to land mines.[49] Depth pertains to how deeply ingrained a norm is within a country that has adopted it. This thesis draws on this literature by counting how many states US/Chinese/Russian information controls have diffused to (breadth of diffusion) as well as how many indicators (technology transfer, imitation, training) have proliferated to one single country (depth of diffusion).

However, the ideational elements of the life cycle framework may prove less helpful in explaining why internet freedom/sovereignty norms diffuse. A realist account (see 4.2.) of the life cycle framework, as proposed in this thesis, may provide better insight to the central question of why internet freedom/sovereignty has diffused successfully. The realist life cycle framework does so by keeping the basic structure of the life cycle (China, Russia, and the United States as norm promoters, who advance their norms through respective organisational platforms, e.g., Belt and Road Initiative). At the same time, the life cycle is adopted to reflect realist thinking. Zimbabwean elites do not adopt internet sovereignty because they were persuaded by China, but because they felt threatened at home by protesting citizens. This empirical example is discussed in more detail in Chapter 6. In short, the realist life cycle presented in this thesis, finds the source of norm diffusion in the materialist perception underlying exports (seeking of influence) and imports (regime survival concerns/economic growth expectations) of internet sovereignty/freedom. Furthermore, even if one were to accept the ideational explanation

[49] Finnemore and Sikkink, "International Norm Dynamics and Political Change."

of norm diffusion, the life cycle explains the action part of normative change (promotion of norms, ideas etc.) but it does not explain how norm entrepreneurs got the new idea/norm of appropriateness in the first place. The life cycle namely states that the dominant norm constitutes the norm entrepreneur's own identity and hence the prospect for a change in norms becomes problematic.[50] Here a linking of the norm life cycle theory with neoclassical realism would be very beneficial. Neoclassical realism, in effect, is focussing on studying the causes of changing perceptions and changing norms for that matter.[51] By relying on process tracing, it has also a sound methodological ground to do so meticulously.[52]

But back to the constructivist life cycle. The ideational mechanisms of the norm life cycle, as viewed by constructivists are laid out below. The characteristic of the first stage in the cycle is active persuasion by the diffusing country/norm entrepreneur. In this stage the entrepreneur engages in an act of moral proselytising and framing of the norm. This process is challenging, since entrepreneurs must present the norm for it to be adopted in an international setting, that is marked by different cultures and customs.[53] The transition to the second stage usually entails enshrining rules through international institutions. "Such institutionalization contributes strongly to the possibility for a norm cascade both by clarifying what, exactly, the norm is and what constitutes violation…and by spelling

[50] Ole Jacob Sending, "Constitution, Choice and Change: Problems with the `Logic of Appropriateness' and Its Use in Constructivist Theory," *European Journal of International Relations* 8, no. 4 (2002): 443–70.
[51] William Wohlforth, "Realism and the End of the Cold War," *International Security* 19, no. 3 (1994): 91–129.
[52] Steven E Lobell, Jeffrey W Taliaferro, and Norrin M Ripsman, "A Methodology of Neoclassical Realism," in *Neoclassical Realist Theory of International Politics*, vol. Oxford University Press (New York: New York: Oxford University Press, 2016).
[53] Margaret E. Keck and Kathryn Sikkink, *Activists beyond Borders* (Cornell University Press, 1998): 903.

out specific procedures by which norm leaders coordinate disapproval and sanctions for norm breaking."[54]

The second stage is marked by third-country imitation.[55] This dynamic is fostered by peer pressure. By joining a group of states, a norm adopting state gains legitimacy amongst this selected group of countries. If a state fails to conform to these norms, it faces "social" (e.g., public disapproval of its actions), or "material" sanctions (e.g., US imposed financial sanctions on Russia after the latter had invaded Ukraine).[56]

The third stage of norm diffusion is internalisation.[57] This situation arrives when norms become unquestioned, a habit, and part of the everyday of bureaucracies and professions within states or regional/international organisations. To illustrate this, few governments today question whether women ought to have the right to vote or seek election, a right which only became a global norm in the 20th century. Some countries' bureaucracies have even started a habit of establishing a norm of gender parity within elected governments.[58] This reflects internalisation of a norm in the workings of state bureaucracies.

The life cycle is neither linear, nor does it necessarily have to be completed.[59] At the centre of Finnemore and Sikkink's framework are individuals such as Henry Dunant and

---

[54] Ibid: 900.
[55] Ibid: 895.
[56] Ibid: 892.; Cass Sunstein, "Social Norms and Social Roles," *Columbia Law Rev.* 96, no. 4 (1996): 903–68; Congressional Research Service, "US Sanctions on Russia: An Overview," March 23, 2020, https://fas.org/sgp/crs/row/IF10779.pdf.
[57] Finnemore and Sikkink, "International Norm Dynamics and Political Change."
[58] Sebastian Fellner, "Kabinett Bierlein Angelobt, Van Der Bellen Bittet Bevölkerung um Vertrauen," 3 June 2019, *DER STANDARD*, accessed April 16, 2021, https://www.derstandard.at/story/2000104268475/kabinett-bierlein-angelobt-van-der-bellen-bittet-bevoelkerung-um-vertrauen.
[59] Ibid: 904.

Elizabeth Cady Stanton, who played seminal roles in, respectively, establishing norms around non-combatants within war and women's right to vote.[60] The underlying motivations of activists are ideational commitment, empathy, and altruism.

During the process of diffusion, norms change, since contexts of norm implementation in the exporting (China) and importing country (e.g. Tanzania) starkly differ.[61] Wayne Sandholtz argues that new environments for a norm inevitably trigger arguments about how the norms should be interpreted.[62] However, localisation of a norm should allow for some flexibility of the interpretation of the exported norm, as long as the two are still seen as similar enough by states to characterise a certain behaviour.[63] Acharya maintains that such reinterpretation of a norm is much more common during norm diffusion than pure acceptance or rejection of a norm.[64] By analysing the impact of transnational norms on Association of Southeast Asian Nations (ASEAN) countries, he shows that the capability of local actors to reconstruct the transnational norms to fit better with pre-existing norms, determines how accepted the norms will be. Reinterpretation of norms during the diffusion process is hence essential to their success.

Reviewing the constructivist literature shows that the ideational mechanisms of diffusion may provide an insight into the diffusion of women's rights norms, as well as those pertaining to the banning of land mines. However, the constructivist approach (ideational

[60] Ibid: 897.
[61] Antje Wiener, *The Invisible Constitution of Politics: Contested Norms and International Encounters* (Cambridge: Cambridge University Press, 2008): 63.
[62] Wayne Sandholtz, "Dynamics of International Norm Change: Rules against Wartime Plunder," *European Journal of International Relations* 14, no. 1 (2008): 101–31.
[63] Carla Winston, "Norm Structure, Diffusion, and Evolution: A Conceptual Approach," *European Journal of International Relations* 24, no. 3 (2018): 638–61.
[64] Acharya, "How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism."

mechanisms drive diffusion – logic of appropriateness) may be ill-suited to explain the freedom/sovereignty norm and its diffusion.[65]

In order to move ahead in studying the diffusion of internet freedom/sovereignty norm diffusion a linking of the norm life cycle theory and neoclassical realism is required. By merging those two approaches this thesis takes both the strengths of norm cycle theory, which pertains to providing an intellectual framework to study norms, e.g. norm entrepreneurs promote norms through organizational platforms, which can be analysed in stages of norm diffusion. At the same time, this thesis takes advantage of the strengths of neoclassical realism in answering *why* questions through process-tracing. It thereby aims to study the causal mechanism more closely that induce norm change in the first place, which norm cycle theory does not address properly (see page 59).

It is the leading argument of this thesis that the "diffusion" of internet freedom/sovereignty is a matter of realist thinking and that it is driven by material mechanisms, as well as a logic of expected consequences. When it comes to exports, China, Russia, and the US foster them to gain influence in other countries (influence is material in nature, see 4.2. for a more extensive discussion of the concept of influence used in this thesis). To be more precise, the export of internet freedom/sovereignty norms is driven by the Chinese and Russian wish to maintain/extend their technological (gain a privileged capability to control technology through backdoors) and normative influence (e.g., keeping in power dictators at the expense of democratic leaders). In this process they aim to build a coalition of like-minded countries that follow their view of how the internet should be governed.

[65] For a thorough empirical discussion of this ill-suitedness see 5.4., 6.4., 7.4.

On the import side, the calculation of adopting a norm is made in terms of what will assure regime survival. For instance, the attractiveness of the Chinese and Russian models of domestic internet governance is based on their models' materialistic promise of increasing the likelihood of regime survival of authoritarian leaders. When it comes to the diffusion of internet freedom, countries engaged in import because they perceived internet technologies, which inherently carried freedom, as a boost to economic growth.

In sum, while Finnemore and Sikkink claim that states sometimes adopt a certain norm in order to avoid becoming international pariahs, this thesis observes that norm promoters and adopters have not been exporting/importing censorship/internet tools because they think it is appropriate or because elites feel that they would gain/lose international reputation if they did so.[66] If states adopt – what is often perceived in liberally minded countries as a "repressive" internet sovereignty norm – their international reputation may indeed suffer, but this is a calculated consequence of authoritarian leaders' behaviour, which in their view gives them better chances of staying in power (logic of expected consequences, see 3.2.).

Having laid out the three dominant theories that study norms in IR, this thesis now proceeds to lay out the norm that lies at the heart of this thesis: sovereignty.[67] This thesis conceives this world as one where the sovereignty norm is violated frequently, especially

[66] Finnemore and Sikkink, "International Norm Dynamics and Political Change."

[67] In this thesis sovereignty is treated primarily as a norm, i.e., the aim is to show that internet sovereignty is increasingly emerging as an appropriate state behaviour. Nevertheless, sovereignty is also a principle, a belief of fact. shared amongst states, that "designates states as the only actors with unlimited rights to act in the international system." Krasner, "Structural Causes and Regime Consequences: Regimes as Intervening Variables": 202.

by more powerful vis-à-vis weaker states.[68] This way of thinking is well illustrated by Thucydides' narrative that "the strong do what they can and the weak suffer what they must."[69] To give an example, Afghanistan and Iraq were, in theory, sovereign countries in 2001 and 2003. Nevertheless, the US invaded those two countries in 2001 and 2003 respectively, practically violating their Westphalian sovereignty (principle of non-intervention).[70] As Krasner illustrates in his major oeuvre "Organized Hypocrisy", violations of sovereignty occur very regularly.[71] Despite frequent violations of sovereignty, this thesis does believe, as many realists do, that the norm of sovereignty and a socialisation into the system, as a way to survive, exist within the international system.[72] As this thesis shows, the norm of sovereignty is closely tied to the socialisation into (regime) survival. This thesis demonstrates this by analysing the regime survival perception of elites in selected countries and how this perception drives the import of Chinese and Russian internet sovereignty norms. The import of surveillance technology and techniques from China and Russia is here considered as a socialisation into regime survival. This is because elites in the norm adopting countries see the import of an internet governance model from the norm promoting countries as a way to increase chances of regime survival. This thesis studies the nexus between sovereignty and regime survival through a neoclassical realist lens in the sense that it looks at elite perception in the norm adopting countries, thereby conducting a unit level analysis, which is the focus of choice in neoclassical realist analyses.

---

[68] Amitav Acharya, "State Sovereignty After 9/11: Disorganised Hypocrisy," *Political Studies* 55, no. 2 (2007): 274–96.
[69] Laurie M. Johnson Bagby, "Thucydidean Realism: Between Athens and Melos," *Security Studies* 5, no. 2 (1995): 179.
[70] Acharya, "State Sovereignty After 9/11: Disorganised Hypocrisy."
[71] Krasner, *Sovereignty: Organized Hypocrisy*.
[72] Waltz, *Theory of International Politics*: 127-128.

For much of the 20th century, sovereignty was taken for granted by realism. The idea is that, internally, the unitary state exercises the ultimate authority. The authority structure is hierarchical. Externally, the international system is partly hierarchical due to the differences in relative power between states, although it remains largely anarchic and states are nominally equal.[73] As Waltz illustrates it, "none is entitled to command; none is required to obey."[74] In short, there is no global authority that reigns relations between states. Instead, there is anarchy. The consequence of anarchy is that states live in a self-help world and that their primary goal is survival.[75]

Starting in the 1970s, the realist conception of sovereignty was challenged by liberal interdependence theorists. They claimed that increased interdependence through transnational flows of people, goods, and information, undermines a state's control over these flows. In turn, this interdependence may constrain sovereignty, since this free flow creates powerful multinational enterprises "that are bound to reflect in some degree the global interests of the multinational network as a whole, and hence can never respond single-mindedly to the requirements of any one national jurisdiction."[76] One strand of realists countered by arguing that interdependence has not changed radically throughout the centuries.[77] Another strand argued that increased interdependence is a choice of states and in their interest.[78] Ultimately, this state of interdependence can be reversed by states if they choose to do so.[79]

---

[73] Lake, "The New Sovereignty in International Relations": 315.
[74] Waltz, *Theory of International Politics*: 88.
[75] Mearsheimer, *The Tragedy of Great Power Politics*.
[76] Raymond Vernon, *Sovereignty at Bay: The Multinational Spread of U.S. Enterprises* (London: Longman, 1971); Raymond Vernon, "Sovereignty at Bay Ten Years After," *International Organization* 35, no. 3 (1981): 523.
[77] Ibid: 138-146.
[78] Robert Gilpin, *US Power and the Multinational Corporation: The Political Economy of Foreign Direct Investment*, Political Economy of International Relations Series (New York: Basic Books, 1975).
[79] Ibid.

Another challenge arose in the 1990s by constructivist scholars. While realists see sovereignty arising from the Westphalian treaty in 1648, and largely unaltered since then, constructivists claim that anarchy is constantly changing through the practices of states. And thus, sovereignty is changing too. Sovereignty is a "social kind", which is largely fixed but also malleable, due to its social character.[80] Sovereignty, just as anarchy, is "what states make of it."[81] Constructivist arguments fall into the recurring theme of realists failing to explain change – in this case the change of the nature of sovereignty depending on which units interact. The sovereignty relationship between the Soviet Union and East Germany (satellite state) and member states of the European Union are an entirely different phenomenon, they posit.[82]

Stephen Krasner sheds light onto this question of how sovereignty varies from unit to unit in the international system. The classical concept of absolute sovereignty, as envisioned by Waltz, only applies to great powers, all other powers need to live with restricted sovereignties.[83] According to Stephen Krasner, sovereignty may be summed up as supreme authority within a given territory – authority here refers to the ability to govern.[84] Krasner considers states as unitary actors that always follow their self-interest. From this viewpoint, sovereignty is organised hypocrisy to cover up the self-interests of states. Powerful states disregard other states' sovereignty whenever it pleases them. Krasner's

[80] Wendt, *Social Theory of International Politics*.
[81] Alexander Wendt, "Anarchy Is What States Make of It: The Social Construction of Power Politics," *International Organization* 46, no. 2 (1992): 391–425.
[82] Thomas J. Biersteker and Cynthia Weber, *State Sovereignty as Social Construct*, Cambridge Studies in International Relations (Cambridge: Cambridge University Press, 1996).
[83] David A. Lake, "The New Sovereignty in International Relations," *International Studies Review* 5, no. 3 (2003): 311.
[84] Daniel Philpott, "Sovereignty," in *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta, Summer 2016 (Metaphysics Research Lab, Stanford University, 2016), https://plato.stanford.edu/archives/sum2016/entries/sovereignty/.

observations that sovereignty is often restricted in practice, is similar to constructivist analyses of Alexander Wendt and Daniel Friedheim, who study the restricted Westphalian sovereignty of the German Democratic Republic (GDR) during the Cold War vis-à-vis the Soviet Union.[85] Wendt and Friedheim argue that states such as the GDR sought security provision from the Soviet Union and in exchange offered the Soviet Union some influence in its internal affairs. Wendt and Friedheim further maintain that GDR leaders identified with the Soviet elites, which allowed for this relationship to exist.

Krasner diverges, with Wendt and Friedheim, however, with regards to what explains the GDR's subordination.[86] Krasner, argues that the arrangement between the Soviet Union and the German Democratic Republic was predominantly a result of the power asymmetries between the two countries and that shared understandings between the elites of the two countries do not play a large role in explaining the relationship. Since the relationship is a result of power asymmetries, it changes as soon as the distribution of power changes. In the words of Krasner, "rulers are calculators [reflecting on relative power capabilities], not agents manifesting some deeper international institutional structure …"[87]

When it comes to the concept of sovereignty itself, Stephen Krasner distinguishes between four types: Westphalian sovereignty (principle of non-intervention into a state's internal affairs), interdependence sovereignty (ability of states to control information, people and ideas across borders), domestic sovereignty (how authority is organised

[85] Alexander Wendt and Daniel Friedheim, "Hierarchy Under Anarchy: Informal Empire and the East German State," *International Organization* 49, no. 4 (1995): 689–721.
[86] Krasner, *Sovereignty: Organized Hypocrisy*.
[87] Krasner, *Sovereignty: Organized Hypocrisy*: 50.

domestically and how effectively those structures exert authority), and international legal sovereignty (principle of mutual recognition between states as members of the international system).[88]

Westphalian and international legal sovereignty have often been violated. After the First World War and after the dissolution of Yugoslavia, the obligation to recognise minority rights (in terms of race, colour, and language) within their borders was imposed on the newly created states in exchange for legal recognition. The International Monetary Fund coerced sovereignty through its conditionality agreements. States had to reform their economy in exchange for money, to avoid bankruptcy, and gain international recognition.[89]

One of the criticisms pertaining to Krasner's work is that he explores Westphalian and international legal sovereignty extensively but does not focus much on domestic and interdependence sovereignty. [90] He also aggregates cases of where Westphalian sovereignty is disregarded. However, he fails to formulate an analytical scheme that categorises individual instances into groups of similar cases.[91] He also does not provide an answer as to whether the sovereignty infringements only apply between great and smaller powers, which, if it was the case, would lead to the conclusion that the international system is to a large part defined by great powers and stays anarchic.[92]

---

[88] Ibid: 50.

[89] Catherine H. Lee, "To Thine Own Self Be True: IMF Conditionality and Erosion of Economic Sovereignty in the Asian Financial Crisis.(International Monetary Fund)," *University of Pennsylvania Journal of International Economic Law* 24, no. 4 (2003): 875–904.

[90] Benedict Kingsbury, "Krasner, Stephen D. 'Sovereignty: Organized Hypocrisy' (Book Review)," ed. Richard Bilder, *American Journal of International Law* 94, no. 3 (2000): 591.

[91] Lake, "The New Sovereignty in International Relations."

[92] Ibid: 310.

The concept of sovereignty is closely tied to the concept of survival. The core premise of realism is that states live in a self-help world and that their primary goal is survival.[93] Survival is about relative distribution of power. Some argue that states try to maximise power (offensive realists), whereas others maintain that they try to maximise security by maintaining a balance of power (defensive realists).[94] Burak Kadercan laments that realists, such as Waltz or Mearsheimer are notoriously bad at defining what they mean by survival and that they often equate the term with sovereignty and security.[95] Instead of providing a precise definition, Kadercan writes that it is more helpful to ask two questions. "First, what do states have to lose when they fail to pursue self-help strategies? Second, how do relevant losses motivate much of international outcomes, or to paraphrase Waltz, how can *concern* [emphasis in original] for such losses serve as the 'ground of action' in world politics?"[96] Kadercan maintains that states lose regime stability and their territorial integrity. Those concerns inform state calculus because leaders are afraid of post-tenure punishments.[97] While this thesis agrees that a distinction between survival and sovereignty is necessary, it argues that Kadercan's meta-definition of survival further confuses the concept. There is a direct relationship between the degree of state sovereignty and the survival of the state, such that the total loss of sovereignty represents the state's non-existence. This thesis, therefore, treats regime survival concerns as a central feature of state survival, at least in relation to autocratic regimes. As we will see in the empirical chapters, it is what motivates states to act in the adoption of information controls.

---

[93] Mearsheimer, *The Tragedy of Great Power Politics*.
[94] Waltz, *Theory of International Politics*; Mearsheimer, *The Tragedy of Great Power Politics*.
[95] Burak Kadercan, "Making Sense of Survival: Refining the Treatment of State Preferences in Neorealist Theory," *Review of International Studies* 39, no. 4 (2013): 1015–37.
[96] Ibid: 1026.
[97] Ibid: 1027.

In order to survive, elites sometimes give up aspects of state sovereignty. Some leaders may, for instance, cede parts of their sovereignty to one group of countries in order to save it from a larger nation-state threat. After Russia defeated the Ottoman Empire in 1878, the latter limited its authority over non-Muslim populations within its territory, meeting British and French demands.[98] In other words, the Ottoman Empire sacrificed some of its sovereignty to France and Britain, to shield the survival of the state from Russian ambitions.[99] This loss of sovereignty translates into influence of one state over another – spheres of influence (SOI) are thereby possibly created.

There are various definitions of SOI. Edy Kaufmann, for instance, states that an SOI can be best described as a geographic region characterised by the high penetration of one superpower to the exclusion of other powers and particularly of the rival superpower.[100] Paul Keal defines "a sphere of influence [as] a determinate region within which a single external power exerts a predominant influence, which limits the independence or freedom of action of political entities within it."[101]

What most definitions of SOIs have in common is that they are about the control of a geographic area by one power and at the same time about the exclusion of other powers from this specific territory. Because SOIs entail control over an area, Keal maintains that they violate sovereignty of the state that is subject to the control.[102] When it comes to the

[98] Ibid: 1029.
[99] Ibid: 1029.
[100] Edy Kaufman, *The Superpowers and Their Spheres of Influence: The United States and the Soviet Union in Eastern Europe and Latin America* (London: Croom Helm, 1976): 11.
[101] Paul Keal, "Contemporary Understanding About Spheres of Influence," *Rev. Int. Stud.* 9, no. 3 (1983): 156.
[102] Ibid: 155.

second part of the definition (exclusion), Keal maintains that exclusion is never absolute.[103] During the Cold War, the Soviet Union had a presence within central America (US SOI) and the US vice versa in Poland (Soviet Union SOI). According to Amitai Etzioni, the means of control is ideational and economic, rather than coercive.[104]

While the concept of SOI has received much attention within geopolitics, it is severely under-researched in the discipline of IR.[105] Susanna Hast, who wrote the most extensive IR book on the topic in the 21st century, claims that the gap in literature exists because there are already many other concepts within IR that describe influence in the international system, for instance, Joseph Nye's soft and hard power.[106] She says, however, that other concepts do not replace the term "spheres of influence" since the term is still much used, which shows that it has a continuous appeal amongst researchers and political commentators.[107]

Spheres of influence have historically been tied to geopolitics and the struggle over territories.[108] Scholars including E.H. Carr, Kenneth Waltz, or John Mearsheimer have not devoted much space to this concept in their scholarly works.[109] John Mearsheimer, for instance, mentions regional hegemons (a hegemon uses force and the threat of force to influence), but does not go further into detail what this means for states in the region

---

[103] Ibid: 157.
[104] Amitai Etzioni, "Spheres of Influence: A Reconceptualization," *The Fletcher Forum of World Affairs* 39, no. 2 (Summer 2015): 117–32.
[105] Hast, *Spheres of Influence in International Relations: History, Theory and Politics*.
[106] Ibid.
[107] Ibid.
[108] Halford John Mackinder, *Democratic Ideals and Reality: A Study in the Politics of Reconstruction* (London: Constable, 1919); Nicholas John Spykman, *America's Strategy in World Politics : The United States and the Balance of Power* (Hamden, Conn: Archon Books, 1970); Zbigniew Brzezinski, *The Grand Chessboard : American Primacy and Its Geostrategic Imperatives* (BasicBooks, 1997).
[109] Hast, *Spheres of Influence in International Relations: History, Theory and Politics*.

that are at the receiving end.[110] Susanna Hast herself takes a normative approach towards the study of spheres of influence. She states that the discourse surrounding spheres of influence is most often pejorative and associated with injustice. She goes on to say that the common normative discourse is that SOI should not be pursued. As opposed to Hast's approach, this thesis is not exploring the normative notion of spheres of influence but the term in its normal expression: where do we see (technological) SOIs, what do they entail, how do they come about, and how does one measure influence (see Chapter 4.2.; for an explanation of how the term spheres of influence relates to technological spheres of influence)?

3.3. Cyber norms

How do the concepts of sovereignty and survival apply to cyberspace? Can states uphold major parts of their sovereignty online, just as they do offline? David Betz and Tim Stevens argue that cyberspace has not challenged states' international legal sovereignty.[111] Challenging this type of sovereignty would entail states recognising cyberspace as a global space with an independent legal status. Quite the opposite seems to occur. As shown in this thesis, states are gaining more and more authority over cyberspace.

However, Westphalian sovereignty (principle of non-interference in a state's domestic affairs) is being violated on a constant basis. Stephen Krasner's concept of organised hypocrisy – whereby Westphalian sovereignty (principle of non-interference into domestic issues) is violated regularly – seems to apply to cyberspace too. States are in a

[110] Mearsheimer, *The Tragedy of Great Power Politics*: 40-42.
[111] Betz and Stevens, "Chapter Two: Cyberspace and Sovereignty."

mode of "unpeace": they are constantly within the adversary's networks.[112] As a result of this experience, the US, for instance, forged a strategy for cyberspace named "persistent engagement", which builds on this premise and perception of constant, "day-to-day" contact with the enemy. In this vein, the 2018 US Department of Defense Cyber Strategy states:

> "We are engaged in a long-term strategic competition with China and Russia. These States have expanded that competition to include **persistent campaigns** [emphasis added] in and through cyberspace that pose long-term strategic risk to the Nation as well as to our allies and partners… The Department must take action in cyberspace **during day-to-day competition** [emphasis added] to preserve U.S. military advantages and to defend U.S. interests."[113]

Interdependence sovereignty is being challenged constantly. But states like China and Russia are gaining interdependence sovereignty. China most prominently has built the so-called "Great Firewall" to reclaim this kind of sovereignty and reign in its cross-border flow of information. China has helped Iran, for instance, to implement a similar national firewall.[114] Russia has conducted exercises as to how to isolate its domestic internet from the global internet, thereby gaining more control over cross-national information flows.[115]

In order to maintain domestic sovereignty, Russia and China have implemented restrictive legal measures and created new structures, e.g., the Cyberspace Administration

---

[112] Lucas Kello, *The Virtual Weapon and International Order* (New Haven, CT: Yale University Press, 2017).
[113] US Department of Defense, "Summary - Department of Defense Cyber Strategy," 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF: 1.
[114] Mark C. Eades, "China's Newest Export: Internet Censorship," *US News & World Report*, January 30, 2014, https://www.usnews.com/opinion/blogs/world-report/2014/01/30/china-is-exporting-internet-censorship-to-iran.
[115] Hasan Chowdhury, "Russia's Test-Run for Its Alternative Internet a Success, Says Kremlin," *The Telegraph*, December 24, 2019, https://www.telegraph.co.uk/technology/2019/12/24/russia-successfully-tests-sovereign-internet/.

within China, that is the supreme body governing the domestic Chinese internet. They have also helped other nations with implementing domestic sovereignty through the sharing of techniques on how to best manage large flows of information online.

In order to increase chances of survival in the international system, states will sacrifice part of their own sovereignty or infringe upon the sovereignty of another state.[116] They might, for instance, give up sovereignty over a territory, in order to hold onto power in another. Saddam Hussein, for instance, sacrificed Kurdish territory in Iraq to preserve the stability of his regime.[117] In another instance, president Truman declared the Truman Doctrine, which claimed the US's rights to intervene abroad in order to prevent Communists from taking power in those countries (US violation of Westphalian sovereignty).[118] This doctrine was to assure the US' existential struggle with the Soviet Union during the Cold War and later justified US troop involvement in Vietnam.[119]

Similar dynamics also apply to sovereignty online. In regard to Westphalian sovereignty, China and Russia argue for non-interference into internal affairs in international fora.[120] However, China's and Russia's export endeavours potentially come at the expense of Westphalian sovereignty for many countries. This may be because China and Russia have access to infrastructure critical to national security in those countries and hence gives them a potential to exploit this access. Financing of large internet infrastructure projects may be another avenue that infringes on countries' Westphalian sovereignty. The import

[116] Kingsbury, "Krasner, Stephen D. 'Sovereignty: Organized Hypocrisy' (Book Review)": 592.
[117] Kadercan, "Making Sense of Survival: Refining the Treatment of State Preferences in Neorealist Theory": 1022.
[118] Howard Jones, "Mistaken Prelude to Vietnam: The Truman Doctrine and 'A New Kind of War' in Greece," *Journal of Modern Greek Studies* 10, no. 1 (1992): 121.
[119] Ibid.
[120] Goldsmith, "The Failure of Internet Freedom."

of technology from China is usually funded by large Chinese loans. Venezuela, for instance, is a bankrupt nation at the moment. However, it recently imported surveillance gear worth hundreds of millions of dollars with loans owed to China. Until it pays off the loans, China wields considerable influence over the government.[121]

3.4. Cyber norm diffusion

The topic of norm diffusion has received considerable attention in the IR literature that focuses on cyberspace.[122] As the following lines demonstrate, several scholars have applied the constructivist life cycle to cyberspace, but none of them has yet accounted for the regime survival concerns of states, which, this thesis argues, drive internet sovereignty norm diffusion. A realist life cycle, which accounts for countries' regime survival concerns is provided in Chapter 4 of this thesis.

Finnemore and Hollis argue that diffusion involves "norm entrepreneurs" that promote certain norms via "organisational platforms", such as international organisations. "Motives", such as ideational commitment, reputation and legitimacy underlie a norm entrepreneur's actions. Deibert and Crete-Nishihata explain the organisational platforms, or channels of diffusion in greater detail.[123] They identify several conduits of diffusion that they categorise into formal organisations and mechanisms, as well as informal mechanisms. In a way, they provide a categorisation of Finnemore and Hollis's

[121] 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; ibid.
[122] Toni Erskine and Madeline Carr, "Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace," in *International Cyber Norms: Legal, Policy & Industry Perspectives* (Tallinn: NATO CCD COE, 2016), 87–109, https://ccdcoe.org/multimedia/international-cyber-norms-legal-policy-industry-perspectives.html.
[123] Ronald J. Deibert and Masashi Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls," *Global Governance* 18 (2012): 339–61.

organisational platforms. Tim Maurer delves into one such organisational platform, the UN, and meticulously describes how norms have diffused in this multilateral organisation and argues that cybersecurity norms are still in the early stages of the life cycle (norms emergence), since the cyber domain is still quite new.[124] Maurer explores the entrepreneurial actions of the US, China and Russia within the United Nations as regards to cyber security norms emergence. He measures this norms emergence by looking at how many co-sponsors a draft proposer manages to mobilise. Russia, for instance, managed to attract more and more co-sponsors every year for the same draft proposal. The problem with Finnemore and Hollis, and Maurer's analyses is not the validity of their arguments but the focus of their attention of research on diffusion of internet freedom/sovereignty through multilateral fora. They focus on norms emergence within international organisations and miss, however, that cyber norms may also diffuse bilaterally through technology and technique diffusion, including from the US, China, and Russia.

Other scholars, such as Laura DeNardis or Milton Mueller have taken this bilateral aspect into consideration. They have looked at how internet standards and protocols embody either freedom or sovereignty norms and how, through the protocols' proliferation, internet freedom diffused. Laura DeNardis looks at the Internet Engineering Task Force (IETF), the institution behind many dominant internet protocols and standards. The IETF is a central internet governance body, which consists of engineers who DeNardis labels as the first internet freedom advocates.[125] Since its inception, engineers have had voting

[124] Maurer, "Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-Security."
[125] Laura DeNardis, *The Internet in Everything: Freedom and Security in a World With No off Switch* (New Haven: Yale University Press, 2020).

and discussion procedures within the IETF which are bottom-up and democratic.[126] This internet governance institution embodies the principles of internet freedom. Importantly, DeNardis mentions that the dominant internet standards of today (coming out of the IETF) have few to no property rights restrictions and are open for everyone to use free of charge. Internet freedom is at their core.

Mueller, too, looks at standards and protocols.[127] He calls them the virtual layer of cyberspace, as opposed to the physical layer of cyberspace which aligns with borders. The virtual layer (protocols) is more like the syntax that allows communications between individuals and is non-proprietary in nature.[128] Because of this phenomenon, he argues that sovereignty should not be applied to cyberspace.

The research on bilateral diffusion of internet freedom in this thesis takes into account the views of Mueller and DeNardis. Taking this baseline of knowledge, this thesis lays out how these technologies were exported from the US to the rest of the world – with them, internet freedom diffused across the globe.

When it comes to the analysis of the bilateral proliferation of the Russian and Chinese information controls, other scholars provided insightful research. However, the analysis is either outdated or shallow. In "Access Controlled", Ronald Deibert and Rafal Rohozinski claim that the Russian model is more advanced and that the future is already

[126] Ibid.
[127] Milton L Mueller, "Against Sovereignty in Cyberspace," *International Studies Review* 22, no. 4 (November 26, 2020): 779–801.
[128] Ibid.

visible in RUNET (Russian language internet community).[129] However, since their study, information controls have evolved strongly, and this description is out of date. It is increasingly visible that China's model is more advanced as it can filter more information via technical prowess. Samm Sacks, for her part, only mentions that laws and techniques are diffusing but leaves out censorship and surveillance technology that is diffusing.[130] Patrick M. Stewart argues that besides laws, technology is crucial as well.[131] However, the shortness of his blogpost does not allow for a thorough categorisation of all diffusing elements of China's information control model. Also, the aforementioned authors do not explain how and why individual information control models spread to some countries rather than others. Why are parts of China's, and not Russia's, model (norm) increasingly being adopted in Zimbabwe? Which model has been more successful in spreading across the globe and why? A more recent analysis by Alina Polyakova and Chris Meserole attempts to distinguish the Chinese and Russian models as well as trace their diffusion. They argue that "Moscow's model of low-tech surveillance, due to its relative low cost and adaptability, is finding appeal among resource-poor governments that lack China's economic prowess, human capacities, and centralized control."[132] They continue by saying that "[i]n the long run, the Russian model may prove to be more adaptable globally as emerging authoritarian regimes that cannot afford China's high-tech model seek greater control over domestic populations and influence abroad."[133]

---

[129] Ronald Deibert, ed., *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, Information Revolution & Global Politics (Cambridge, Mass.: MIT Press, 2010).
[130] Samm Sacks, "Beijing Wants to Rewrite the Rules of the Internet," *The Atlantic*, June 18, 2018, https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/.
[131] Patrick M. Stewart and Ashley Feng, "Belt and Router: China Aims for Tighter Internet Controls with Digital Silk Road," *Net Politics - Council on Foreign Relations*, July 2, 2018, https://www.cfr.org/blog/belt-and-router-china-aims-tighter-internet-controls-digital-silk-road.
[132] Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism," *Brookings Institution*, August 26, 2019, https://www.brookings.edu/research/exporting-digital-authoritarianism/.
[133] Ibid.

This thesis disagrees with Polyakova and Meserole's claims. While it is true that a lot of countries lack China's surveillance capabilities, these two authors do not emphasise the fact that China is actually exporting these capabilities and thereby allowing importing countries to imitate the Chinese model. Furthermore, the authors rely on outdated data. They claim that China has exported its surveillance equipment to 18 countries. They do not provide figures for Russia's exports. This thesis, however, shows that – to date – China has exported its technology to 75 countries and Russia only to 28. Polyakova and Meserole's argument is hence negated by evidence this thesis provides.

It is important to mention that China does not have one blueprint to export its domestic information control landscape. In his book "China, Africa, and the Future of the Internet", Iginio Gagliardone argues that China is very savvy in engaging with local contexts and in adjusting its engagement to the local environment.[134] Gagliardone provides in-depth studies of China's engagement with two democracies (Ghana and Kenya) as well as with two authoritarian regimes (Ethiopia and Rwanda). In Ghana, China built internet infrastructure by adjusting to an environment that is marked by public and private entities. Concurrently, in Ethiopia, an authoritarian-leaning country, China propped up information infrastructure that is completely managed and owned by the state and thereby supported the incumbent elite. Gagliardone also mentions that a dichotomy should be avoided between China spreading authoritarianism and a West that promotes openness. As highlighted by other scholars, it is often European companies that sell advanced surveillance tools to African governments.[135] In short, Gagliardone highlights the fact that China's and the West's engagement in Africa should not be portrayed as a dichotomy.

[134] Iginio Gagliardone, *China, Africa, and the Future of the Internet* (Zed Books, 2019).
[135] 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/.

Furthermore, he puts sometimes sensational news articles into perspective as to how China acts and thereby adds crucial nuance to the debate.

Having examined the relevant literature to (cyber) norms and their diffusion we will now turn towards using it to build a theoretical framework for the analysis of internet freedom and sovereignty diffusion.

Chapter 4: Internet norm diffusion: a framework of analysis

This chapter proposes a theoretical framework for the study of internet freedom/sovereignty diffusion. It first establishes a typology of information controls, which is used to differentiate the US, Chinese, and Russian cyber norms in the ensuing empirical chapters of the thesis. Information controls can take various forms, including surveillance, censorship, self-censorship, and strategic information dissemination. Different models of domestic internet governance emerge once one takes into account the extent to which a country "wishes to control information" coupled with how many "options" (tools) a country has to control information. These two factors define to which extent a country "uses" the various forms of information control. This thesis distinguishes itself from previous analytical frameworks by putting surveillance at the core of its concept of information controls and by analysing how surveillance affects other forms of managing information.[136]

The theoretical framework then turns to analyse the causes of US, Chinese and Russian cyber norm diffusion. Those are the "perception underlying export – seeking of influence" and the "perception underlying import – regime survival concerns for internet sovereignty and economic growth expectations for internet freedom". The framework also entails three indicators to measure norm diffusion (DV1): technology transfer, imitation, and training. Finally, the theoretical framework presents the concept of technological sphere of influence to frame the consequences of norm diffusion (dependent variable 2) for the importing countries (e.g., Thailand). The framework concludes by laying out the consequences of diffusion (DV2), that is implications for

[136] Deibert and Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls"; Margaret E. Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall* (Princeton N.J.: Princeton University Press, 2018).

sovereignty.

This theoretical framework presents a structured approach to filling the gaps in the literature mentioned above and to generating new knowledge that explains why the internet freedom/sovereignty norms have diffused successfully (or not). Chapter 4 will be followed by three empirical chapters (US, Chinese, and Russian norms), which will deploy the theoretical concept and fill it with data. This data is collected via a variety of social science research methods.

4.1. A typology of information control norms

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."[137] Others have categorised information controls into fear (i.e. self-censorship), friction (akin to censorship), and flooding (similar to strategic information dissemination).[138] This thesis 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 domestic internet governance emerge once one takes into account the extent to which a country "wishes" to control information and how many "options" (tools) a country has to control it, which then determines which

[137] Ronald J. Deibert and Masashi Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls," *Global Governance* 18 (2012): 339.
[138] Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall*.

is the preferred method of information control (censorship for China, inducing self-censorship for Russia, and strategic information dissemination for the US).

Types of control

Surveillance

Surveillance is an essential element of 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 internet users, it can induce self-censorship.[139] 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.

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).[140] Although fear can

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

[140] 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

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."[141] For the purposes of this thesis, self-censorship is defined as the "withholding of one's true opinion from an audience perceived to disagree with that opinion." [142] The more surveillance tools a government has at its disposal, the more avenues it has to nudge its population towards self-restraint. In China, for instance, extensive surveillance allows the government to draw from a wider toolkit to intimidate its citizens. In addition to low-tech intimidation, it can also threaten to ban citizens from using public transport or menace to prohibit them from using social media platforms.[143] It can do so because technology allows the government to see at all times where a citizen is and what online services they are using.

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.[144] It can be subtle when it comes as an increase in the costs of accessing

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

[141] 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.

[142] Ibid.

[143] Lily Kuo, "China Bans 23m From Buying Travel Tickets as Part of 'Social Credit' System," *The Guardian*, March 1, 2019, sec. World news, https://www.theguardian.com/world/2019/mar/01/china-bans-23m-discredited-citizens-from-buying-travel-tickets-social-credit-system; Stephen McDonell, "WeChat and the Surveillance State," *BBC News*, June 7, 2019, sec. China blog, https://www.bbc.com/news/blogs-china-blog-48552907.

[144] Hayes, Glynn, and Shanahan, "Willingness to Self-Censor: A Construct and Measurement Tool for Public Opinion Research."

information, such as slowing down certain online services (e.g., Tor Browser), or downranking undesired political content in search engines.[145] Censorship can also be large-scale and more indiscriminate through the shutting down of social media platforms, cell phone services, or internet connectivity.[146] Such network shutdowns can persist for weeks or even months. They have also become much more widespread throughout the years. While China was one of the first countries to conduct a network shutdown in 2009 to keep a lid on unrest in Xinjiang, the practice is now most commonly implemented across the world.[147] India is leading the number of counts of network shutdowns. Half of the recorded network shutdowns have occurred in India.[148] Although network shutdowns come at a considerable economic cost, states still prioritise regime stability over economic damage.[149]

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

[145] Tor Browser is a software that allows for anonymous communication and thereby shields users from surveillance.

[146] 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.

[147] Hogg, "China Restores Xinjiang Internet."

[148] Rydzak, "Of Blackouts and Bandhs."

[149] Darrell M. West, "Internet Shutdowns Cost Countries $2.4 Billion Last Year" (Brookings Institution, October 6, 2016), https://www.brookings.edu/research/internet-shutdowns-cost-countries-2-4-billion-last-year/.

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."[150] In the context of this thesis, an example of disinformation is Russia's fabrication and dissemination of the "news" that AIDS was a result of US government experiments.[151] An example of propaganda is the Chinese government's use of microblogs, such as Sina Weibo, which are usually used to share pictures, videos and texts.[152] An example that shows that propaganda is also prevalent in the US is CBS News's and Fox News's coverage of the 2012 US and Russian elections.[153] Like with censorship, strategic information dissemination can change with the surveillance capabilities of the disseminator. The more a country knows about citizens, the more options it has to manipulate them. This became apparent during the 2016 US presidential election, when Russia used automated microtargeting (based on personality characteristics to target specific parts of a population) to influence the elections. This technique allowed it to spread messages on Facebook based on identity, ethnicity, and race.[154]

---

[150] 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.

[151] 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.

[152] 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.

[153] Olga Lazitski, "Media Endarkenment: A Comparative Analysis of 2012 Election Coverage in the United States and Russia," ed. J. Gregory Payne, *American Behavioral Scientist* 58, no. 7 (2014): 898–927.

[154] Richard Fontaine and Kara Frederick, "The Autocrat's New Tool Kit," *Wall Street Journal*, March 15, 2019, https://www.wsj.com/articles/the-autocrats-new-tool-kit-11552662637.

Why the US, China, or Russia prefer different information controls

Willingness to control information

The first factor that defines an information control regime is the extent to which a government is willing to control information. The US, China, and Russia all wish to censor content related to terrorism or child abuse imagery. In China and Russia, an additional wish exists related to political information.[155] This is a natural, given that regime survival in China and Russia hinges on close control of the political information environment (e.g., of protests, government scandals, opposition voices). Hence, a first step in defining a domestic internet governance model is to define whether there exists a high (Russia, China) or low (US) willingness to control information.

Information control options for governments

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 and the US, for instance, have more surveillance capabilities than Russia and

[155] The US also controls political information, e.g., related to hate speech. However, compared to China and Russia, it is very much bounded control, i.e. some measure of control is imposed to preserve general freedom. Weber, "The Worldwide Web of Chinese and Russian Information Controls."

therefore have more options to implement information controls. Hence, the amount and diversity of surveillance tools is a major factor in understanding the distinctness of the US, Chinese and Russian models of domestic internet governance.

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

Both China and Russia have high ambitions to control information. However, they 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.[156] It therefore relies predominantly on intimidating its population (e.g., by imprisoning opposition candidates). Russia's reliance on these techniques may be because they require less technological sophistication. The US, for its part, has many options to control information, but its ambition to restrict the free flow of information is low, which leads it to rely on strategic information dissemination to control information domestically.

[156] 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.

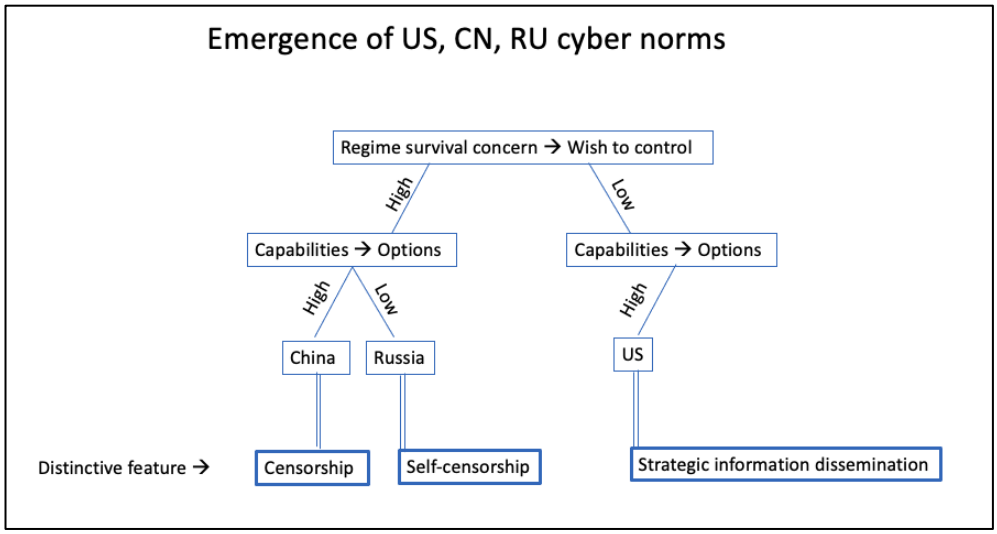


Figure 1: Emergence of US, Chinese, and Russian cyber norms

4.2. International cyber norm diffusion

The most prominent cyber norms diffusing are the US internet freedom and Chinese and Russian variants of internet sovereignty. For a long time, internet freedom was the predominant cyber norm internationally. However, China and later on, Russia, started seeing the internet as a potential/actual challenge to regime stability.[157] Since then, many countries followed their example and internet freedom has been receding concurrently.[158]

This thesis explores the international expansion of internet freedom/sovereignty through a neoclassical realist framework of IR, which means that this thesis focusses on explanatory variables at the unit level (perception underlying export/import).[159] The

[157] 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; Human Rights Watch, "Freedom of Expression and the Internet in China" (Washington, D.C., 2001), https://www.hrw.org/legacy/backgrounder/asia/china-bck-0701.pdf.
[158] Freedom House, "Freedom on the Net 2018."
[159] Rose, "Neoclassical Realism and Theories of Foreign Policy."

following paragraphs describe the sequence of how internet freedom/sovereignty has diffused. It starts by describing the independent variable of perception underlying exports – seeking of influence (IV1). It then continues by laying out the perception underlying imports – regime survival concerns for internet sovereignty and expectations of economic growth with regards to internet freedom (IV2). If both IV1 and IV2 are present, norm diffusion (DV1) is likely to occur. A limiting condition here is the absence of another supplier that already meets the demands of an importing country. For instance, if the surveillance market in Syria is largely met by European products, it will be more difficult, but not impossible, for China to supply products there. This may be the case even if both IV1 (China is seeking of influence in Syria, a country situated along the BRI trade routes) and IV2 (high regime survival concerns in Syria) are present. This chapter concludes by illustrating the consequence of DV1, which is implications for sovereignty (DV2).

Independent variable 1: Perception underlying exports – seeking of influence

The US has proclaimed that it wants to increase digital freedoms across the world.[160] And yes, there may be moral considerations in promoting internet freedom. However, this thesis finds a lot of evidence that points to the US promoting the export of internet (freedom) technologies with the aim to increase its political influence abroad, as for instance, over China, where exporting internet technologies has been linked by US leaders as a way to propel democratisation.[161] If the US really cared about empowering other countries through "liberation technologies", it would not have stayed silent with regards to digital human rights abuses in allied countries, such as Bahrain, Saudi Arabia, or the

[160] Weber, "Linking Cyber Strategy with Grand Strategy: The Case of the United States."
[161] "Clinton's Words on China"; Clinton, "Secretary Clinton Remarks Internet Freedom."

United Arab Emirates.[162] The empirical chapter, in particular, shows that while moral reasonings may be present in internet freedom promotion, the prime motivation to export internet freedom is US seeking of influence abroad.

China and Russia, for their part, often claim that the incentive for exporting internet sovereignty is normative, too. They promote sovereignty because they want to help governments to be able to restrict freedom of expression because they (Moscow, Beijing) deem it is the only way to preserve public order in countries across the globe. In other words, they provide altruistic help in a self-help world. Moscow and Beijing claim that they want to empower governments through multilateral institutions to reduce the digital divide between the North and South. However, as William E. Connolly explains, interests (motives) can also be unarticulated.[163] An alternative explanation that this thesis advocates for is that the two countries' interest in promoting sovereignty is a wish to increase their influence. If Russia truly cared about empowering other countries, it would not have invaded Crimea (Ukraine) and annexed Crimea's internet infrastructure. Russia and China, for instance, have very likely enjoyed access to intelligence because they implanted backdoors in the censorship and surveillance equipment that they exported to foreign governments.[164] It might also be the case that China and Russia have simultaneously moral and strategic reasonings when advocating for internet sovereignty. However, this thesis claims that even though Russia and China claim that their export endeavours are motivated by moral reasonings, the more plausible explanation is that

[162] Jillian C. York, "Internet Freedom Initiative Mere Lip Service?," November 3, 2011, https://www.aljazeera.com/indepth/opinion/2011/10/201110301020514111130.html.
[163] Connolly, *The Terms of Political Discourse*.
[164] 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); 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.

Beijing and Moscow wish to maximise their chances of survival by gaining as much influence as possible through exports. Their reasoning is strategic.

This perception is reflected in strategic initiatives. Countries involved in strategic initiatives receive more political and economic engagement by China and Russia than countries not involved in them. Hence, strategic initiatives have become proxies for substantial information control, 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. In this thesis, the two strategic initiatives – BRI and CIS – are considered to be alternative measures demonstrating what China and Russia perceive as their current or emerging spheres of influence. As this thesis shows, this is important, because countries that are embedded within Chinese or Russian strategic initiatives, are more likely to imitate Chinese or Russian information controls, which is an indicator for advanced norm diffusion.

Independent variable 2: Perception underlying imports – regime survival concerns/economic growth expectations

The theoretical framework then examines the major cause of why internet freedom/sovereignty has been embraced abroad (demand side of diffusion). This thesis claims that the material incentives of regime survival/economic growth related to the internet are the underlying reasons for the adoption of the internet sovereignty/freedom norms.

In the 1980s and 1990s, internet freedom diffused across the globe, since countries saw the internet as a potential to propel the expansion of their economies. States implemented

only few measures that would regulate people's behaviour online and the (predominantly American) companies that operated the infrastructure and the content. This landscape of widespread global internet freedom is laid out in Chapter 5 of this thesis.

This changed in the 2000s, when many hybrid/authoritarian regimes experienced large-scale protests, organised through internet connected devices. The perception of the internet being primarily a tool to achieve economic growth switched to the internet being a tool that can threaten regime survival. In terms of sovereignty, autocratic, just like democratic states, witnessed a challenge to domestic (control over domestic online content) and interdependence sovereignty (control over cross-border information flows). To extend these types of sovereignty to the internet, autocratic elites started increasingly imitating Chinese and Russian practices of information control.

One reason for this phenomenon might be that autocratic countries tend to be more willing to learn from each other because they perceive that they face similar threats to regime survival.[165] These ideas of survival gain particular relevance after major threats to stability. This inclination leads to the sharing of various techniques and policies among authoritarian countries. Already in 1848, autocrats of different polities shared techniques on how to counter revolutionary tendencies in Europe.[166] At that time, when revolutions swept through Europe, autocrats often exchanged letters with other autocrats on how to face revolutions. Due to the royal nature of the autocrats at the time, they were also

[165] Kurt Weyland, "Crafting Counterrevolution: How Reactionaries Learned to Combat Change in 1848" 110, no. 2 (2016): 215–31.

[166] Authoritarianism is defined here as "[a] style of government in which the rulers demand unquestioning obedience from the ruled" whereas autocracy is defined as "[a] regime in which power is concentrated in the person of a single individual—as, for example, in the case of 'the Stalinist autocracy'." Lincoln Allison, "Authoritarianism," *Oxford Reference*, 2021, https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095435698; Oxford Reference, "Autocracy," 2021, https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095435876.

conveniently each other's family members. "King Ernst August of small Hannover kept giving his nephew Friedrich Wilhelm IV. 'a hard time' about the 'excessive' concessions that the ruler of this European great power had made to his rebellious citizens."[167] Especially because they were family members, they could exchange frank viewpoints on how to crush dissent.[168]

Likewise, during and after the Arab Spring in the early 2010s, authoritarian-leaning leaders engaged in "elite learning", which allowed them to develop more informed policies. While in some cases assistance between elites 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.[169]

All this points to a larger phenomenon of domestic survival being the most basic expression of seeking international survival. A state first needs to create domestic hierarchy and only then a state can engage in strategies that will allow it to gain relative power within the anarchical international system. Autocratic elites believe that the better censorship and surveillance tools they have at their disposal, may translate into higher chances of domestical survival. In Zimbabwe, for instance, the political leadership has invested in facial recognition systems that allows the police to identify people in anti-government rallies more easily and to persecute them, as a consequence, more effectively. Chinese equipment in particular is seen as a way to increase chances of survival.[170]

[167] Ibid: 226.
[168] Ibid.
[169] Ibid.
[170] Interview with Senator David Coltart on 22 May 2020, Member of Parliament in Zimbabwe's National Assembly from 2000-2008; since 2008 a Member of the Senate; Minister of Education, Sport, and Culture from February 2009 – August 2013.

However, at the same time an importing state's (e.g., Thailand) position within the international system vis-à-vis the exporting hegemon is weakened, since Zimbabwe or Thailand expose their core internet infrastructure to a foreign power's intelligence gathering. While protecting themselves better from a domestic threat landscape, states expose themselves to an international threat landscape and hence give up some aspects of their sovereignty by allowing Russia and China to interfere in their domestic issues. It is a lesser evil for states to be exposed to Moscow and Beijing than to their domestic population. Their regime is more likely to survive that way.

Dependent variable 1: Norm diffusion

While the particular focus of this thesis if to focus on norm diffusion from China, the US, and Russia it is important to mention that norm diffusion from one country does not preclude norms from other countries diffusing to the same country concurrently. A country may imitate a law from China, while at the same time draft another law that draws inspiration from the UK or Uganda. A similar caveat applies to the training and technology transfer indicators. Countries do import technology from different countries or receive trainings from a variety of sources. In the case of Vietnam for instance, the country has not only taken inspiration from China for its 2017 cybersecurity law, but also from Japan, the Czech Republic, South Korea, and the US during the creation of the law.[171]

What norm shift occurs when US, Chinese, or Russian norms diffuse? Internet freedom diffusion did not produce a norm change because there was previously no norm as regards

[171] 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/.

to how to regulate the internet. The American norm, protocols, and technologies were imported and set a global standard. Internet freedom norm diffusion has decentralised power away from the elites. Authoritarian leaders woke up to this "decentralising/liberating" force of the internet only later when protests shook their streets. But once they woke up to the revolutionary potential of the internet, they started regulating it and reigning it in with the help of Russia and China. In short, Chinese and Russian norm diffusion has not changed "what" countries did (countries would have increased their control over the internet in any case with or without the assistance from China and Russia), but how those countries did it – they did it the Russian and Chinese way.

It is important to mention that partial norm diffusion can take place via technology transfers even if no training has taken place in a country. Similarly, a norm may diffuse partially, if only training was provided without technology transfer. But a broader norm diffusion can only take place if two or more indicators diffuse.

Diffusion indicator: Technology transfer

The first indicator of diffusion is technology transfer. For the purpose of this thesis, I focussed on US internet technologies (protocols and standards, which are present in every country of the world). As regards to Chinese and Russian surveillance and censorship technology, I included 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.[172]

Diffusion indicator: 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 thesis, however, includes only those cases where company documents or reliable newspaper articles 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.[173]

[172] Hikvision, "Hikvision Gives Japan a Culturally and Technically Relevant Solution," December 1, 2011, https://www.hikvision.com/en/Press/Success-Stories/Education/305528882360250.
[173] 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.

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.[174]

Diffusion indicator: Imitation

In Finnemore and Sikkink's life cycle, framework persuasion by the norm promoter (first stage of norm diffusion) is an essential precondition for imitation by norm followers (second stage of diffusion). Without persuasion, imitation is unlikely to occur. In the realist life cycle presented in this thesis, a similar observation is made. The norm promoter (US, China, Russia) needs to do its part (transfer technology and provide training) for imitation to take place. In this thesis, the "technology" and "training" indicators show norm diffusion, "imitation" indicates advanced norm diffusion. As later chapters of this thesis will show, the data of this thesis suggest that imitation very rarely (if ever) occurs without prior or concurrent diffusion of technology and training, while technology and training can sometimes be the only indicators of diffusion. Thus, imitation likely demonstrates the advanced diffusion of a norm.

For the purpose of this thesis, imitation is defined as the replication of US, Chinese or Russian information governance laws and techniques by another country. Examples include Austria, which is a member of the Freedom Online Coalition and subscribes to digital rights principles, such as the free flow of information. Other examples are

[174] 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.

Uzbekistan copying Russia's law on state surveillance, or Tanzanian government officials announcing that they intend to mimic China's replacement of foreign online content providers with homegrown ones to exert greater control.[175]

Dependent variable 2: Sovereignty

Dependent variable 2 is ultimately about consequences that arise due to state behaviour (dependent variable 1).[176] Information control diffusion draws countries into a technological sphere of influence (TSOI; "technosphere"). TSOIs are geographical areas and spheres of influence to which information control technology, techniques of handling information, and law have diffused. Within a TSOI, for instance, China and Russia increase countries' internal sovereignty (the ability of the elites to exert authority vis-à-vis their populations) through export of technology and techniques, but they undermine the Westphalian sovereignty of importing countries. Moscow and Beijing strengthen countries' power vis-à-vis their domestic populations but gain influence over those countries in return. In turn, through the export of the internet freedom norm, the US adds checks and balances on, e.g., Zimbabwe's execution of authority (internal sovereignty) and makes it resemble the internal sovereignty in the US. In the US, for instance, domestic authority is put under checks and balances from the media, and people have the tools to organise themselves (social media) in order to hold those in power accountable. At the same time, the US undermines the Westphalian sovereignty of Zimbabwe through internet freedom diffusion, by gaining a privileged capability to control technology within

[175] Asterius Banzi, "Tanzania: Govt Seeks Chinese Help in Social Media," *The East African (Nairobi)*, August 1, 2017, https://allafrica.com/stories/201708020658.html; 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-.

[176] Colin Elman, "Horses for Courses: Why Not Neorealist Theories of Foreign Policy?," *Security Studies* 6, no. 1 (1996): 7–53.

the importing country and by influencing that country's information governance landscape.

While traditional spheres of influence are characterised by the influencer's control over a geographic area as well as some exclusion of rival powers, the exclusion of rival powers is impossible when it comes to technology.[177] Hence, TSOIs are not about exclusion, but primarily about a hegemon's privileged capability to control technology overseas and to influence information control techniques abroad.

Influence itself has many definitions. Dennis Wrong, for example, sees it as an outcome.[178] This vision is difficult to measure in practice. How can one prove that the US has continuous control over a piece of Moroccan internet infrastructure that it exported recently? How can one enter the minds of thousands of journalists that have been trained in information management by China and the US and see whether the training was impactful or not? Since this is very difficult, and beyond the scope of this work, this thesis uses a definition proposed by Moyer et al., who provide an extensive literature review of influence in a 2018 report.[179] Moyer et al. define influence as a "capacity", not an outcome:

"[I]nfluence derives partially from discrepancies in access to national resources … National resources include economic, political, and security means... Such imbalances allow state A to exert influence over state B both explicitly and implicitly.[180]

[177] Several states, such as Iran, Russia, US and China are trying to substitute vital equipment from rival powers. However, none has yet managed to produce its entire technology supply chain natively. Furthermore, exclusion from networks is impossible. There is no 100 % security from cyber intrusions. Iran has not supplied the US with core components for its networks and nevertheless it has managed to gain a foothold in US territory through cyberspace repeatedly. Valentin Weber, "Making Sense of Technological Spheres of Influence," Strategic Update (LSE IDEAS, April 2020), http://www.lse.ac.uk/ideas/publications/updates/technological-spheres-of-influence.

[178] Dennis H Wrong, *Power: Its Forms, Bases, and Uses*, Key Concepts in the Social Sciences (Oxford: Blackwell, 1979).

[179] Moyer et al., "Power and Influence in a Globalized World."

[180] Ibid.

In the process of norm diffusion, too, influence should be seen as a capacity, not an outcome, or something that can be achieved. The norm entrepreneur (US, China, Russia) accumulates means to influence the importing country. When technology diffuses, the US gains a greater opportunity to insert backdoors into the same technology in the future (software updates as backdoors). Whenever a country imitates China's internet sovereignty approach, the potential to draw on this country in a vote, for instance, on internet governance issues at the UN General Assembly, likely increases with it. When China invites Thai journalists to Beijing for training, it builds a pool of journalists that will likely share China's worldview on how to report media stories or to manage content in the future.

The type of influence that is created during internet sovereignty/freedom diffusion is similar to what some call normative/soft power.[181] The type of influence referred to in this thesis is similar to soft power/normative power in the sense that it is, amongst other factors, created by attraction. Zimbabwe imitates China because its model is attractive. But some soft power/normative power scholars emphasise that "attraction" is being built through persuasion and argumentation.[182] This thesis claims that material incentives are much more crucial to build attraction. Zimbabwe or Thailand did not imitate China because of Chinese persuasion and argumentation, but because their norm import was driven by regime survival concerns. They did not have to be persuaded to adopt the norm. Technology transfer gives China, Russia, and the US the privileged capability to control

[181] André Gerrits, "Normative Power in a Changing World: A Discussion" (Clingendael, December 2009), https://www.clingendael.org/sites/default/files/pdfs/20091200_cesp_paper_gerrits.pdf; Emilian Kavalski, "Normative Power Beyond the Eurocentric Frame," Oxford Bibliographies, (August 28, 2018), https://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0239.xml.
[182] Gerrits, "Normative Power in a Changing World: A Discussion."

the exported technology through inserted backdoors. Here, the type of influence is material, since influence is related to having the privileged capacity (a national resource akin to, for instance, a fleet of stealth espionage planes) to access overseas hardware and software. To give an example, the exporting state can conduct supply chain interdictions – by intercepting products before they are exported abroad, with or without the knowledge of the US/Chinese/Russian company in question – to insert backdoors.[183]

This thesis measures a hegemon's influence in a TSOI through the diffusion indicators of technology, training, and imitation. Through the export of technology, for instance, the exporting country gains insight into importing countries' networks. The export of information control technology, which is often extractive in nature, translates into revenues and employment for the exporting countries. If countries within a TSOI imitate US, China or Russia, those countries exert political control, not through coercion, but through attraction. If states undergo trainings by the US, China and Russia in information control, they may also follow their information control practices. This gives Washington, Beijing, and Moscow influence over a TSOI.

TSOIs, just like traditional spheres of influence, vary by the extent of influence a hegemon exerts. This thesis distinguishes between two categories of influence in a TSOI: the core and the periphery. The TSOI's core is marked by the diffusion of technology and trainings as well as by the presence of imitation of information governance techniques. It shows the most advanced state of norms diffusion.

[183] Glenn Greenwald, "Glenn Greenwald: How the NSA Tampers With US-Made Internet Routers," *The Guardian*, May 12, 2014, sec. US news, https://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden.

In the TSOI's periphery, diffusion and influence are not yet that extensive. If only technology or training have diffused, for instance, it means that the importing state can only be influenced to some extent. Since the hegemon supplies and operates the exported equipment, the importing state's critical infrastructure is very likely exposed to the hegemon, through covert backdoors. Through training of foreign entities, too, China influences how those foreign entities manage information online. Whenever a state within a TSOI undergoes training, acquires surveillance/censorship technology, or imitates Russian and/or Chinese techniques, it is drawn deeper into the sphere and closer to the core of a TSOI.

Norm diffusion indicator	Type of influence	Extent of influence of norm entrepreneur
Technology	Privileged capability to control technology	In the **peripheral technosphere** – where 1 or 2 indicators diffused to a country – the hegemon has **low influence** In the **core technosphere** – where all 3 indicators diffused to a country – the hegemon has **high influence**
Training	Influencing journalist reporting and the cyber security practices of law enforcement	
Imitation	Influencing of elite/leadership ideas	

Table 4: Measuring influence

Not all states are equal. GDP (Gross domestic product) defines how resistant states are to influence. A country that has a GDP of over $100 billion is considered a country that is more resistant to technological influence.[184] Large and wealthy states have more resources to invest into security and hence have better chances of mitigating risks of their critical infrastructure being undermined by another hegemon's technology. Germany or the United States will have a much better chance of mitigating potential cyber intrusions in critical infrastructure provided by Russia and China than Mauritius will.[185] States with larger GDPs generally hold larger populations, hence diminishing the influence that can be built through trainings in information controls. A training in Argentina or Antigua and Barbuda will have a much greater impact on the latter than on the former.

This chapter proposed a framework to distinguish cyber norms as well as to study their diffusion. It made the following conceptual arguments. Internet freedom/sovereignty norms are characterised by surveillance, censorship, self-censorship, and strategic information dissemination. Norm diffusion is not explained by US, Chinese or Russian persuasion of countries abroad or by geographical closeness. Instead, diffusion occurs wherever supply of and demand for US, Chinese and Russian technology and techniques meet. The export side of information control diffusion is motivated by the US', China's, and Russia's interest in increasing their influence abroad. Washington, Moscow, and Beijing have laid out where they aim to wield influence (the US across the world, China along the BRI trade routes, Russia within the CIS) and, as a consequence, foster their exports to these geographical areas. This has propelled the diffusion of technology and

[184] Steven Levitsky and Lucan Way, *Competitive Authoritarianism: Hybrid Regimes After the Cold War*, Problems of International Politics (New York: Cambridge University Press, 2010).
[185] At the same time, all states, including large states such as the US and Germany remain vulnerable to cyberattacks, even if they spend large resources on cybersecurity measures.

training to certain geographical areas. Importing countries' regime threat concerns and economic growth expectations, with regards to the internet, explains their demand for US, Chinese or Russian cyber norms. The consequence of diffusion is the creation of US, Chinese and Russian technospheres.

While this chapter proposed a theoretical framework to study cyber norms, the next chapter deploys the framework to analyse the internet freedom norm and its diffusion.

Chapter 5: Internet freedom in a brave new world

"The main thing I was declaring was that cyberspace is naturally immune to sovereignty and always would be. I believed that was true then [1996], and I believe it's true now [2016]."[1] John Perry Barlow, cyber-libertarian, poet, and cattle-rancher.

"In the new century, liberty will spread by cell phone and cable modem." Bill Clinton, president of the United States of America, in 2000.[2]

Chapter 5 illustrates internet freedom's rise and subsequent decline. Understanding this is crucial to answering the research question of why the Chinese and Russian internet sovereignty norms (Chapters 6 and 7) have supplanted the internet freedom norm in several parts of the world.

The rise of the internet freedom norm was driven by the US seeking influence abroad (supply side) and countries aiming at boosting their economies through the internet (demand side). Internet technologies, and with it, freedom (high amount of online freedoms compared to offline freedoms in many countries) swept through the world. Once the internet became more widely available across the world it also turned into a tool for citizens to organise protests, e.g., during the Arab Spring. As soon as authoritarian-leaning governments realised this (~early 2010s), they turned to increasingly control information online. While the perception of the internet as a tool for economic growth still plays a role amongst political elites in authoritarian countries, a new perception has joined it more recently – that the internet can cause regime instability. Because of this new perception, internet freedom has declined in recent years. In short, countries'

[1] Andy Greenberg, "It's Been 20 Years Since John Perry Barlow Declared Cyberspace Independence," *Wired*, February 8, 2016, https://www.wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence/.
[2] "Clinton's Words on China."

perception has changed. The internet is not seen only as a tool for economic growth (rise of internet freedom) anymore, but also as a fundamental challenge to regime survival in authoritarian countries (rise of Chinese and Russian internet sovereignty norms).

This chapter starts by examining the internet freedom norm by tracing the norm's historical roots in the US. The chapter proceeds by analysing the internet freedom norm through the information governance framework presented in the theoretical chapter of this thesis. The next part sheds light on the international diffusion of the cyber norm by looking both at the supply (IV1) and demand side (IV2) of diffusion (DV1). This part is followed by an analysis of the consequence of diffusion (DV2), that is impacts on sovereignty of the importing country. More recently, however, the internet freedom norm has been receding. The ensuing section measures the receding of the norm by looking at data published by Freedom House.

5.1. The internet freedom norm

5.1.1. A history

Internet freedom is seen by many experts and activists as the right to exercise human rights online.[3] This may involve the application of human rights law online, the right to receive and give information and to communicate with each other, as well as the access to the internet *per se*. This definition is reflected in government bureaucracies, too. Jason

[3] Interview with Christopher Painter on 2 May 2019 [First Coordinator for Cyber Issues in the US Department of State]; Chinmayi Arun on 27 May 2019, Resident Fellow at Yale Law School; David Kaye on 20 May 2019, Former UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression; David Sullivan on 23 April 2019, Program Director at the Global Network Initiative; Jason Pielemeier on 20 May 2019, Policy Director at the Global Network Initiative and previously a Special Advisor at the US Department of State, where he led the Internet Freedom, Business and Human Rights section in the Bureau of Democracy, Human Rights and Labor; Rebecca MacKinnon on 14 June 2019, Founding Director Ranking Digital Rights; Nani Jansen Reventlow on 4 June 2019, Director of Digital Freedom Fund.

Pielemeier, Policy Director at the Global Network Initiative, a US not-for-profit, mentions, for instance, that when he used to work in US government, the State Department was divided into different sections:

"I was working in the Human Rights Office and the way we thought about these things rightly or wrongly was really about 'are people's rights being violated'. Almost a negative analysis. For those who have access to those digital platforms and services and products what does it mean what is it like both in terms of technological interface as well as the legal interface. Whereas other parts of that same building [State Department] were much more focussed [on] … building access out. So, they had a whole set of concerns about how do we develop the regulatory environment that incentivises investments and basically building out the core infrastructure of the internet."[4]

The definition of internet freedom as "human rights online" has its roots in the early 1970s when the first internet pioneers started their research funded by ARPA (Advanced Research Projects Agency, a US military agency that focusses on emerging technologies) within academic institutions. At that time, internet freedom was largely a project of academics that saw it as a liberating force. Those first decades of the internet were marked by an atmosphere of freedom and absence of government control.[5]

Such a vision of the internet was cemented by John Perry Barlow's "A Declaration of the Independence of Cyberspace", which famously calls for governments to keep their hands off the internet.[6] In the words of Barlow:

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave

[4] Interview with Jason Pielemeier on 20 May 2019, Policy Director at the Global Network Initiative and previously a Special Advisor at the US Department of State, where he led the Internet Freedom, Business and Human Rights section in the Bureau of Democracy, Human Rights and Labor.

[5] Jack L Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (New York: Oxford University Press, 2006).

[6] Barlow, "A Declaration of the Independence of Cyberspace."

us alone. You are not welcome among us. You have no sovereignty where we gather. We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear."[7]

The declaration was written primarily as a response to the "Telecommunications Act of 1996", which deepened internet regulation by the US government. As John Naughton notes, before being commercialised, there was little profit and hence less crime online. However, with the commercialisation of the internet in the 1990s, Naughton argues that a need for regulation emerged.[8] Barlow considered many government actions online as being excessive and, as a result, co-founded the Electronic Frontier Foundation (EFF), a non-governmental organisation, that has since its foundation in 1990 fought for civil liberties online and uncovered government infringements on those liberties.[9] Both Barlow's letter and the founding of the EFF pinpointed to a larger trend – the internet's pioneers (e.g., Mitchell David Kapor, John Gilmore, and Steve Wozniak – all co-founders of the EFF) saw an assertion of governments in cyberspace, that is a space that had previously been considered to be a utopian safe haven free from governmental control.[10]

With time, a US government vision of internet freedom became increasingly adopted nationally (a vision where the government interferes to a very limited extent to assure liberties of individuals), and the cyber-libertarian vision (where government does not

[7] Ibid.

[8] John Naughton, "The Evolution of the Internet: From Military Experiment to General Purpose Technology," *Journal of Cyber Policy* 1, no. 1 (2016): 5–28.

[9] Electronic Frontier Foundation, "A Not Terribly Brief History of the Electronic Frontier Foundation," *Electronic Frontier Foundation*, July 15, 2014, https://www.eff.org/pages/not-terribly-brief-history-electronic-frontier-foundation.

[10] Goldsmith and Wu, *Who Controls the Internet?: Illusions of a Borderless World*.

interfere and individual liberties are hence more extensive) progressively marginalised.[11] While cyber-libertarians believed that the internet can self-regulate (one vision of internet freedom), the US government perceived that a certain, if limited, regulation of content (e.g., curbing hate speech) and individuals (e.g., punish criminal behaviour online) was necessary to uphold internet freedom. As it turned out, the latter vision of internet freedom, pursued by the US government, prevailed. The US view of internet freedom is divergent from other regions' view of internet freedom (see 8.3.3. for a more in-depth discussion thereof). While the US puts a lot of emphasis on free speech, other digital human rights, such as privacy, which have been more of a concern in, e.g., Europe, have not been a major focus in the US internet freedom agenda.[12]

In the 1990s, for the first time "internet freedom" became a US government policy.[13] Internet freedom started to be mentioned throughout the decades in US government policy documents. For instance, I previously examined six key US strategy documents, dating from 2010-2016, pertaining to cyberspace. All of them call for an open, interoperable, secure, and reliable internet. In short, they call for internet freedom.[14]

Internet freedom has also been prominently represented in speeches of US politicians. Internet freedom is based on two principles, commercial non-regulation and anti-censorship. These two principles are sometimes hard to distinguish, because policy makers often use them interchangeably to describe internet freedom.[15] This thesis

[11] Lincoln Dahlberg, "Oxford Research Encyclopedia of Communication," 2017.
[12] Nani Jansen Reventlow and Jonathan McCully, "Internet Freedom Without Imperialism," *Knight First Amendment Institute*, June 13, 2018, https://knightcolumbia.org/content/internet-freedom-without-imperialism.
[13] Goldsmith, "The Failure of Internet Freedom."
[14] Weber, "Linking Cyber Strategy with Grand Strategy: The Case of the United States."
[15] Goldsmith, "The Failure of Internet Freedom."

primarily focusses on the second principle, since it strongly aligns with the thesis' research focus on the diffusion of Chinese and Russian internet sovereignty norms.

The first principle is the commercial non-regulation principle.[16] Clinton's administration opposed trade barriers, government taxes and any other forms of regulating the internet. The guiding forces of the internet should be, at home and abroad, individuals and the private sector and not the government. The non-regulation principle is embodied in the US' support for a multi-stakeholder internet governance model that envisions a participation of many stakeholders such as the private sector and civil society to administer and develop the internet.[17]

The second principle, the anti-censorship principle, arose from promoting internet trade; in this sense it is interwoven with the first principle. It translates into a belief that the internet ought to allow freedom of expression and operators should minimise the amount of censorship. The US' norm is hence located at the opposite extreme of China's information control norm which emphasises censorship. The US also focusses primarily on promoting anti-censorship and does not focus on promotion of its other aspects of information controls, namely surveillance and strategic information dissemination. At first, only the non-regulation principle was advanced when the US pushed for open markets for its technology giants. While the potential of the internet for political change started to emerge, the anti-censorship principle was not yet pursued actively, since the

[16] William J. Clinton and Albert J. Gore, "The Framework for Global Electronic Commerce," 1997, https://clintonwhitehouse4.archives.gov/WH/New/Commerce/index.html.
[17] US Department of State, "Department of State International Cyberspace Policy Strategy" (Department of State, March 2016), https://www.state.gov/documents/organization/255732.pdf; Barack Obama, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Clinton administration believed that it is technically impossible to impose censorship.[18] In 2000, Bill Clinton had declared: "In the new century, liberty will spread by cell phone and cable modem ... We know how much the Internet has changed America … Imagine how much it could change China … [The Beijing regime] has been trying to crack down on the Internet–good luck. That's sort of like trying to nail Jello to the wall."[19]

Only under George W. Bush and China's increasing repressive information controls, the US realised that it had to actively promote the anti-censorship principle. Starting with George W. Bush and continued under the Obama and Trump administrations, the US pushed for internet freedom abroad through funding of censorship circumvention tools and techniques. In 2010, Foreign Secretary Hillary Clinton captured this spirit well by saying that "[b]oth the American people and nations that censor the internet should understand that our government is committed to helping promote internet freedom."[20]

Under George W. Bush, the State Department founded the "Global Internet Freedom Task Force" (GIFT), which was equipped with a $500,000 grant to support circumvention tools.[21] Under the Obama administration, GIFT was succeeded by the "NetFreedom Task Force".[22] Since 2008, the US has spent in total $145 million on internet freedom endeavours.[23] This effort was maintained under president Trump, where the State

[18] "Clinton's Words on China."
[19] Kate Merkel-Hess and Jeffrey N. Wasserstorm, "Will the Real Chinese Internet Please Stand Up?," *Dissent Magazine*, February 11, 2010, https://www.dissentmagazine.org/online_articles/will-the-real-chinese-internet-please-stand-up.
[20] Clinton, "Remarks on Internet Freedom."
[21] Department Of State. The Office of Electronic Information, "Global Internet Freedom Task Force (GIFT) Strategy: A Blueprint for Action," December 28, 2006, https://2001-2009.state.gov/g/drl/rls/78340.htm.
[22] Patricia Moloney Figliola, "Promoting Global Internet Freedom: Policy and Technology," October 22, 2013.
[23] U.S. Deparment of State, "Internet Freedom," accessed November 2, 2018, https://www.state.gov/j/drl/internetfreedom/.

Department's Bureau of Democracy, Human Rights, and Labor continued to coordinate the promotion of internet freedom.[24] Since 2017, the budget dedicated to internet freedom has increased by 30 per cent, and amounted to $65.5 million for the year 2020.[25]

US companies, too, have been strong advocates for internet freedom. Google, Facebook, and Twitter, for instance, issued statements or lobbied against restrictive internet regulations and for the maintenance of the free flow of information.[26] However, their efforts sometimes appear hypocritical considering that their reasoning is driven by profits and that they have to comply with local laws in a given country.[27] Civil society for their part has focused mostly on promoting the anti-censorship principle of internet freedom abroad.[28]

5.1.2. Internet freedom in practice

Surveillance

Following the 9/11 terror incident, the US has established what is probably the most advanced online surveillance system in the world. In 2013, whistle-blower Edward

---

[24] Ibid.

[25] Katrina Manson, "US Boosts Funding of Tech Companies to Help Anti-Tehran Protests," *Financial Times*, January 19, 2020, https://www.ft.com/content/740a385a-3924-11ea-a6d3-9a26f8c3cba4.

[26] Google, "Enabling Trade in the Era of Information Technologies: Breaking Down Barriers to the Free Flow of Information," November 15, 2010, https://static.googleusercontent.com/media/www.google.com/de//googleblogs/pdfs/trade_free_flow_of_information.pdf; Biz Stone, "The Tweets Must Flow," January 28, 2011, https://blog.twitter.com/official/en_us/a/2011/the-tweets-must-flow.html; Mai Nguyen, "Exclusive: Vietnam Cyber Law Set for Tough Enforcement Despite Google, Facebook Pleas," *Reuters*, October 10, 2018, https://www.reuters.com/article/us-vietnam-socialmedia-exclusive/exclusive-vietnam-cyber-law-set-for-tough-enforcement-despite-google-facebook-pleas-idUSKCN1MK1HL.

[27] Noah Smith, "Google's Prototype Chinese Search Engine Links Searches to Phone Numbers," *The Guardian*, September 19, 2018, sec. Technology, https://www.theguardian.com/technology/2018/sep/18/google-china-dragonfly-search-engine.

[28] Freedom House, "Freedom in the World 2018," January 13, 2018, https://freedomhouse.org/report/freedom-world/freedom-world-2018; Human Rights Watch, "Freedom of Expression and the Internet in China"; Privacy International, "Private Interests: Monitoring Central Asia," November 2014, https://privacyinternational.org/report/837/private-interests-monitoring-central-asia.

Snowden revealed several mass surveillance programmes, amongst them PRISM, Xkeyscore, Bullrun, and Upstream.[29] PRISM is a system that requires major US companies to hand over data to law enforcement without the knowledge of the user.[30] Upstream is the name of the US and UK's programme of network tapping, and the software that allows the extraction of key information is called Xkeyscore.[31] Bullrun, for its part, has been intended to break encryption through collaboration with the information technology industry and forging public key certificates.[32] After the Snowden revelations, Congress passed the USA Freedom Act of 2015 that was supposed to reign in the National Security Agency (NSA) and its bulk collection of data, by requiring it to request data from telecommunications companies instead of having direct access to it.[33] Since 2015, however, it has been revealed that the NSA had at least at two separate events unauthorised access to text messages and calls, which raises questions as to the effectiveness of regulation aimed at reigning in surveillance.[34]

Despite these considerable capabilities to collect information, the US collection of data needs to be continuously approved by court orders or other legal authorisations. In

[29] Zygmunt Bauman et al., "After Snowden: Rethinking the Impact of Surveillance," *International Political Sociology* 8, no. 2 (2014): 121–44.
[30] Ibid.
[31] David Lyon, "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique," *Big Data & Society* 1, no. 2 (2014).
[32] National Security Agency, "Project Bullrun," 2010, https://search.proquest.com/docview/1679098764/abstract/7B14BB5285C84FFBPQ/1.
[33] U.S. Congress, "Text - H.R.2048 - 114th Congress (2015-2016): USA FREEDOM Act of 2015," legislation, (February 6, 2015), 2015/2016, https://www.congress.gov/bill/114th-congress/house-bill/2048/text.
[34] Dustin Volz, "NSA Improperly Collected U.S. Phone Records a Second Time," *Wall Street Journal*, June 26, 2019, https://www.wsj.com/articles/nsa-improperly-collected-u-s-phone-records-a-second-time-11561541520.

contrast, no such accountability mechanisms are present in China and Russia to check surveillance by the state apparatus.[35]

Censorship

The First Amendment to the US Constitution protects freedom of speech in the country. As a result, very little content is blocked, apart from two exceptions: child abuse imagery and copyright infringement. As regards to the former, the Child Online Protection Act of 1998 is intended to shield minors from harmful content online and the Child Protection and Obscenity Enforcement Act of 1988 prohibits child sexual abuse images.[36] The Digital Millennium Copyright Act (DMCA) regulates content takedowns when it comes to copyright infringement. The DMCA has sometimes been abused during election periods to take down content of political opponents who used sound bites or video clips from copyrighted material.[37] Usually, the use of such content bits is protected by the "fair use" legal provision.[38]

---

[35] Dahlia Peterson, "Designing Alternatives to China's Repressive Surveillance State" (Center for Security and Emerging Technologyy, October 2020), https://cset.georgetown.edu/publication/designing-alternatives-to-chinas-repressive-surveillance-state/; 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).

[36] Jeffrey (Chien-Fei) Li, "Internet Control or Internet Censorship? Comparing the Control Models of China, Singapore, and the United States to Guide Taiwan's Choice," *Pittsburgh Journal of Technology Law and Policy* 14, no. 1 (2014): 1–43; William J. Hughes, "H.R.3889 - 100th Congress (1987-1988): Child Protection and Obscenity Enforcement Act of 1988," webpage, (November 18, 1988), 1987/1988, https://www.congress.gov/bill/100th-congress/house-bill/3889.

[37] Elliot Harmon, "Once Again, DMCA Abused to Target Political Ads," *Electronic Frontier Foundation*, November 17, 2015, https://www.eff.org/deeplinks/2015/11/once-again-dmca-abused-target-political-ads.

[38] The fair use doctrine establishes the right for the unpermissioned, or unlicensed, use of a copyrighted piece in some circumstances, such as in parody, search engines, scholarship, and commentary. U.S. Congress, "17 U.S. Code § 107 - Limitations on Exclusive Rights: Fair Use," *LII / Legal Information Institute*, accessed July 7, 2020, https://www.law.cornell.edu/uscode/text/17/107.

Tim Wu argues that the First Amendment was written in a time when speech and public speakers were scarce and intended to protect the voicing of opinions.[39] Today, there is a sheer endless amount of speech in the US and the problem is not so much too little free speech, but too much. Troll armies are flooding online fora with propaganda and hence often drown meaningful speech – in a process that some dub "reverse censorship."[40] Twitter and Facebook, for instance, are filled with dozens of million fake accounts and human-posing robots that increase the visibility of some content by reposting it automatically, thereby marginalising otherwise meaningful conversations.[41]

Strategic information dissemination

Strategic information dissemination is the use of choice for the US government to shape the information landscape. Whether it was through Hollywood movies in the Cold War to encourage recruitment into the military services or to demonise the Soviet Union – propaganda has been a key part of the US information governance model.[42] In their book "Network Propaganda", Yochai Benkler and his co-authors Robert Farris and Rob Weiss demonstrate how Fox News has been transformed into a propaganda machine under former president Donald Trump, where the president could voice his opinions without any critical judgement by Fox News, or deliberately promulgate false news that support his agenda on, e.g., immigration issues.[43] A Wall Street Journal and Los Angeles Times investigation showed how former presidential candidate Michael Bloomberg had hired 500 people and offered them $2,500 a month to post thousands of messages that support

[39] Tim Wu, "Is the First Amendment Obsolete?" (Knight First Amendment Institute at Columbia University, September 1, 2017), https://knightcolumbia.org/content/tim-wu-first-amendment-obsolete.
[40] Ibid.
[41] Ibid.
[42] Tony Shaw and Denise Youngblood, "Cold War Sport, Film, and Propaganda: A Comparative Analysis of the Superpowers," *Journal of Cold War Studies* 19, no. 1 (2017): 160–92.
[43] Yochai Benkler, Robert Farris, and Rob Weiss, *Network Propaganda* (New York, U.S.: Oxford University Press, 2018).

his campaign, including people who did not support Bloomberg but took the job to secure some income.[44]

More recently, former president Trump has instigated a number of changes in the US international media that operate under the umbrella of the US Global Media Agency, an independent agency of the US government. According to several employees of the USAGM, the changes were intended to make US international media a mouthpiece of the president.[45] Under normal circumstances, this should be difficult to achieve, since under the US International Broadcasting Act of 1994, US international broadcasting services, such as Voice of America, Radio Free Asia, Radio Free Europe/Radio Liberty, Office of Cuba Broadcasting, and Middle East Broadcasting Networks are guaranteed independence.[46] The Act establishes the procedure of key personnel being appointed by the president and the necessity to be approved by the Senate.[47] Then, however, the National Defense Authorization Act for Fiscal Year 2017 brought the USAGM under a single CEO appointed by the president.[48] In order to potentially exert greater control over USAGM, former president Trump appointed a new CEO of the USAGM, Michael Pack, a close ally of Steve Bannon, a former Trump White House Chief Strategist and right-wing sympathiser.[49] After being confirmed in the Republican controlled Senate, one of

---

[44] Hussain Suhauna, "'Please Disregard, Vote for Bernie': Inside Bloomberg's Paid Social Media Army," *Los Angeles Times*, February 23, 2020, https://www.latimes.com/business/technology/story/2020-02-23/mike-bloomberg-paid-twitter-social-media.

[45] Jennifer Hansler and Brian Stelter, "'Wednesday Night Massacre' as Trump Appointee Takes Over at Global Media Agency," *CNN*, June 18, 2020, https://www.cnn.com/2020/06/17/media/us-agency-for-global-media-michael-pack/index.html.

[46] U.S. Congress, "International Broadcasting Act," *USAGM*, 1994, https://www.usagm.gov/who-we-are/oversight/legislation/international-broadcasting-act/.

[47] Ibid.

[48] U.S. Congress, "Text - S.2943 - 114th Congress (2015-2016): National Defense Authorization Act for Fiscal Year 2017," May 18, 2016, https://www.congress.gov/bill/114th-congress/senate-bill/2943/text.

[49] Russell Brandom, "After OTF Takeover, Trump Appointee Faces Pressure From Lawmakers and Courts," *The Verge*, June 24, 2020, https://www.theverge.com/21301542/otf-usagm-michael-pack-lawsuit-congress-open-technology-fund.

Pack's first actions was to fire the heads of Middle East Broadcasting, Radio Free Europe/Radio Liberty, Radio Free Asia, and the Open Technology Fund, some of which have opposed Trump's plans for their respective organisations.[50]

Self-censorship

A large part of self-censorship in the United States is induced into the population by public knowledge of the US' mass surveillance apparatus. Reporting on the NSA/PRISM surveillance programme has induced a large-scale chilling effect on, e.g., users consulting Wikipedia for certain topics.[51] Search for topics that raise privacy concerns, such as terrorism-related content, dropped significantly after the US surveillance programme revelations.[52] Similarly, journalists, attorneys, and activists were likely shocked to know that they were on a secret database of the Federal Bureau of Investigation (FBI) that contained names of individuals that have been particularly vocal when it comes to the US' immigration actions on its border with Mexico.[53]

5.2. The diffusion of the internet freedom norm

5.2.1. Understanding the supply side of diffusion

Scholars such as Madeline Carr have maintained that, while promoting internet freedom, the US had to balance strategic and moral reasoning. In her book on US power in the internet age, Carr argues that by promoting internet freedom, US policy makers choose

[50] Hansler and Stelter, "'Wednesday Night Massacre' as Trump Appointee Takes Over at Global Media Agency."
[51] Penney, "Chilling Effects: Online Surveillance and Wikipedia Use."
[52] Ibid.
[53] U.S. Customs and Border Protection, "CBP Response to DHS Coalition Letter," November 11, 2019, https://web.archive.org/web/20191111201841/https://www.documentcloud.org/documents/6009352-CBP-Response-to-DHS-Coalition-Letter.html; Ryan Devereaux, "Border Official Admits Targeting Journalists and Human Rights Advocates With Smuggling Investigations," *The Intercept*, May 17, 2019, https://theintercept.com/2019/05/17/border-smuggling-journalists-activists/.

values and ideas over the risk which cyber insecurity poses to their power.[54] She thereby claims that a US-promoted open internet is inherently insecure and thereby contradicts the US' security interests. She claims that "[u]ltimately, [Hillary] Clinton observed that the United States will have to struggle to balance ideational and material power concerns and that, in a sense, this will be a key feature of US power in the information age."[55]

This thesis argues that Carr disregards the fact that the US has always had outstanding access to most of the world's internet communication networks and hence its promotion of internet freedom has not been at odds with its security concerns. The Edward Snowden leaks and the US cyber capabilities revealed in them are a case in point. It is rather likely that the US is promoting an open internet in order to allow for the expansion of US tech giants and weaken authoritarian regimes. Of course, the US may have moral considerations, but its main goal is to seek influence abroad.

The Open Technology Fund Authorization Act in Congress, for example, emphasises that promoting open-source and secure technology is in the interest of the US.[56] This shows that promoting internet freedom is a calculated interest-based decision. In this vein, the internet freedom fund is used specifically to increase pressure on authoritarian regimes abroad, as for example in Iran.[57]

---

[54] Madeline Carr, *US Power and the Internet in International Relations - The Irony of the Information Age* (Basingstoke, Hampshire: Palgrave Macmillan, 2016), www.palgrave.com/gp/book/9781137550231: 114.

[55] Ibid: 114.

[56] Michael T. McCaul, "Text - H.R.6621 - 116th Congress (2019-2020): Open Technology Fund Authorization Act," webpage, (April 24, 2020), 2019/2020, https://www.congress.gov/bill/116th-congress/house-bill/6621/text.

[57] Manson, "US Boosts Funding of Tech Companies to Help Anti-Tehran Protests."

Jablonski and Powers also argue that US internet freedom promotion is driven by influence seeking, i.e., American commercial and geopolitical interests rather than democratic and humanitarian visions.[58] They argue that data has become the new oil and that it is effectively used by the US to increase its influence overseas.

Jillian C. York, the Electronic Frontier Foundation's Director for International Freedom of Expression mentions that she is sceptical of the internet freedom agenda's "moral" dimensions. She remarks that the State Department's programme aimed strongly at states where the US was interested in regime change, such as China, Iran, and Syria.[59] She mentions the examples of Bahrain, Saudi Arabia, and the United Arab Emirates (all three countries are US allies), where prominent bloggers were detained but the US remained silent.[60] Other scholars and activists have voiced similar concerns.[61] During the Trump administration the angle on internet freedom has become a more personal matter.[62] Political groups that sympathise with former president Trump, e.g. Falun Gong, have lobbied to promote anti-censorship tools that were developed by them and were pushing the former president to focus even more on China, where Falun Gong has been repressed.[63]

---

[58] Powers and Jablonski, *The Real Cyber War: The Political Economy of Internet Freedom*.

[59] Jillian C. York, "The Trump Administration Is Attacking Critical Internet Privacy Tools," July 10, 2020, https://www.vice.com/en_us/article/v7gz4d/the-trump-administration-is-attacking-critical-internet-privacy-tools.

[60] Jillian C. York, "Internet Freedom Initiative Mere Lip Service?," November 3, 2011, https://www.aljazeera.com/indepth/opinion/2011/10/201110301020514111130.html.

[61] Sami Ben Gharbia, "The Internet Freedom Fallacy and the Arab Digital Activism," *Nawaat*, September 17, 2010, https://nawaat.org/portail/2010/09/17/the-internet-freedom-fallacy-and-the-arab-digital-activism/; Morozov, *The Net Delusion: The Dark Side of Internet Freedom*.

[62] Russell Brandom, "A New Trump Appointee Has Put Internet Freedom Projects in Crisis Mode," *The Verge*, June 23, 2020, https://www.theverge.com/2020/6/23/21300424/open-technology-fund-usagm-circumvention-tools-china-censorship-michael-pack.

[63] International Religious Freedom Roundtable, "Template Multi-Faith Letter," *21Wilberforce*, 2020, https://wilberforce.salsalabs.org/internetfreedom/index.html.

The underlying US institutional architecture of internet freedom

The previous paragraphs served to shed a light on the motivation of the US in its internet freedom promotion endeavour. The following lines seek to demonstrate that the US' internet freedom agenda is not only present in discourse but in actual policy actions. The US' commitment to promoting internet freedom abroad is most visible in the institutional structure it set up to further its internet freedom agenda. In 2011, the State Department established the Office of the Coordinator for Cyber Issues to address, amongst other topics, internet freedom. Its first Coordinator was Christopher Painter. He defines internet freedom as "the ability of people to exercise their human rights including their right to free expression online. Both to receive information and give information and to communicate with each other."[64] He also emphasises that internet freedom and the protection of vulnerable populations is a cross-cutting issue, spanning security and economics. Since there are so many stakeholders and interests involved, his office started to set up bilateral meetings with countries that would try to address internet freedom in a multistakeholder approach:

> "We started this idea of doing this cross-cutting bilats [bilateral talks] with other countries where we would for example with Japan … have all the government players from our side and they'd have all the players from their side trying to break down the siloes and then we started to add industry and civil society we did that with Brazil, India, and others. So, I think it is important to involve all those stakeholders."[65]

He further emphasises the importance of promoting internet freedom in multilateral fora and how important it was that the UN Human Rights Council recognised that human rights apply both offline and online.[66]

[64] Interview with Christopher Painter on 2 May 2019. He served as the first Coordinator for Cyber Issues in the US State Department.
[65] Ibid.
[66] Ibid.

Painter also mentions other ways of promoting internet freedom in a world where countries would not always be interested in implementing human rights in their countries:

"One of the things we also recognised is that countries would often be interested in the cybersecurity aspect, you know 'help us build a strategy, help us do this', so it provided a good entrée to say 'we're happy to do that', 'we also want to talk about a larger set of values with you.'"[67]

A large share of the funding for the internet freedom agenda comes from the State Department's Bureau for Democracy, Human Rights and Labor (DRL). From 2007-2017, the DRL provided $125 million to support internet freedom. The main purpose of these grants was to protect vulnerable populations and foster technological innovation to improve their ability to communicate.[68]

A central body that coordinates and funnels these resources into projects on technological innovation to civil society groups and academia is the Open Technology Fund (OTF). Through its organisational and operational structures, it represents the internet freedom community's values (see later sections of this chapter for a more in-depth description of the internet freedom community). Those are open-source technology, transparency in allocation of funding of internet freedom projects, and most importantly the affirmation that human rights which apply offline also apply online. By following these principles, the OTF has, despite being funded by the US government, gained and retained the trust of the internet freedom community.[69]

---

[67] Ibid.

[68] Ibid.

[69] Maria Xynou 2020-07-22, "Support the OTF: Support a Free and Open Internet," July 22, 2020, https://ooni.org/post/2020-support-otf/; Save Internet Freedom, "All Signatories," July 29, 2020, https://saveinternetfreedom.tech.

The OTF has for a long time operated as a part of Radio Free Asia but has more recently become an independent grantee of the US Agency for Global Media.[70] OTF receives a considerable portion of the internet freedom fund. For fiscal years 2021 and 2022, it is planned to receive $20,000,000 and $25,000,000 respectively.[71]

OTF organises regular calls for projects and then decides which projects to fund. In this way, it has already supported the Tor Browser (a browser that anonymises users) and the Signal Messenger (an open-source messenger that promises high security communications).[72] In this endeavour it has created technology that is used by billions of users worldwide. Even WhatsApp, one of the largest messaging apps on the market currently (2 billion users), uses the Signal Protocol for end-to-end encrypting messages.[73]

In addition to being an important funder of the internet freedom community, the OTF is also the primary docking station for the internet freedom community. The OTF maintains a mailing list both for ongoing projects [OTF-active] and one for the larger community [OTF-talk], both of which give the community a forum to communicate with each other, share ideas/research, and discuss current topics. The OTF is also a partner of the annual Internet Freedom Festival (IFF) in Valencia, where various projects and activists meet to

[70] Open Technology Fund, "A New, Independent OTF," *Open Technology Fund*, November 25, 2019, https://www.opentech.fund/news/new-independent-otf/.
[71] McCaul, "Text - H.R.6621 - 116th Congress (2019-2020)."
[72] Open Technology Fund, "Projects We Support," *Open Technology Fund*, 2020, https://www.opentech.fund/results/supported-projects/.
[73] Jon Porter, "Whatsapp Now Has 2 Billion Users," *The Verge*, February 12, 2020, https://www.theverge.com/2020/2/12/21134652/whatsapp-2-billion-monthly-active-users-encryption-facebook; K. G. Orphanides, "Why Everyone Should Be Using Signal Instead of WhatsApp," *Wired UK*, April 16, 2020, https://www.wired.co.uk/article/signal-vs-whatsapp.

discuss how to advance digital rights.[74] The first IFF was held in 2014 with around 600 participants and has grown to host 1,700 registrants in 2018 of which a large proportion identifies as women and gender non-conforming as well as representing the Global South.[75] In addition, OTF organises an annual summit for actively funded projects.[76] The 2017 summit brought together 150 participants of which more than half identified as coming from the Global South.[77] The key role that OTF plays was reflected during spring 2020, when the Trump administration attempted to dismantle it.[78] As a response to the political interference, the internet freedom community mobilised and brought the Save Internet Freedom Initiative to life, whose primary goal is to ensure the political independence of OTF's work.[79] A letter in Congress that was written with this intent gathered signatures from 526 organisations [as of 29 July 2020] and 4285 individuals.[80]

Another organisation that is part of the internet freedom infrastructure is the Information Safety and Capacity Project (ISC), which is funded by USAID (United States Agency for International Development).[81] The organisation's primary purpose is to assist human rights activists, media, and civil society organisations to strengthen their cyber security. Since 2011, ISC has engaged with 365 local partner organisations and provided training

[74] Internet Freedom Festival, "Partners and Supporters," *Internet Freedom Festival*, 202AD, https://internetfreedomfestival.org/partners-supporters/.
[75]Interview with Sandy Ordonez on 5 August 2020, Head of Communications and Outreach at the Open Internet Tools Project and driving force behind the Internet Freedom Festival.
IREX, "Internet Freedom Festival," 2020, http://www.irex.org/project/internet-freedom-festival.
[76] Rebecca MacKinnon, "The U.S. Just Undercut Its Mission to Support Internet Freedom Worldwide," *Slate Magazine*, June 26, 2020, https://slate.com/technology/2020/06/us-open-technology-fund-hong-kong-protest.html.
[77] Sandra Ordónez and Dan McDevitt, "Open Technology Fund Summit 2017: Community Snapshot," *Open Technology Fund*, August 31, 2018, https://www.opentech.fund/news/open-technology-fund-summit-2017-community-snapshot/.
[78] Brandom, "After OTF Takeover, Trump Appointee Faces Pressure From Lawmakers and Courts."
[79] Save Internet Freedom, "All Signatories."
[80] Ibid.
[81] The ISC Project, "Home," 2020, https://www.iscproject.org.

and assistance to over 5,200 individuals. The ISC also provides so called "Small Technology Grants" to developers in order to promote these goals.[82]

USAID will, in the future, award grants under the "Greater Internet Freedom" programme, which aims to build cybersecurity capacity within independent media and civil society actors in countries that USAID is active in.[83] The programme also mentions the goal to expand the internet freedom community and encourage traditional human rights groups to include digital rights into their operational remit.[84]

5.2.2. Understanding the demand side of diffusion

The main reason internet freedom has diffused so successfully is that countries were unaware of the challenges it could pose to their regime and only saw the economic and scientific benefits of the internet.[85] Regime security concerns were simply not yet present to that extent in the 1980s, 1990s, and most of the 2000s. The internet has been seen as a huge opportunity to increase the Gross Domestic Product [GDP] of a country and make the economy more efficient. To give an example, this vision of adopting and further deepening the internet infrastructure to raise economic growth has been voiced by numerous African governments and their ministers.[86]

---

[82] Ibid.

[83] USAID, "Greater Internet Freedom," 2020, https://www.grants.gov/web/grants/view-opportunity.html?oppId=323976.

[84] Ibid.

[85] The demand side of internet freedom is not only driven by the economic interests of governments. Across the world a vibrant community of people has emerged that wish to expand freedoms online primarily for moral reasons. However, governments' demand for internet (freedom) technologies has been the primary driver of diffusion.

[86] United Nations Economic Commission for Africa, "CoM2019 Ends With African Governments Being Urged to Embrace Digital Transformation," March 26, 2019, https://www.uneca.org/stories/com2019-ends-african-governments-being-urged-embrace-digital-transformation; World Bank, "African Leaders Committed to Building a Digital Economy," May 30, 2018, https://blogs.worldbank.org/voices/african-leaders-committed-to-building-digital-economy.

Numerous studies underpin this worldview and show what growth rates the internet brings to countries that are connected as opposed to countries that have sparser access to the internet. A 2011 McKinsey study, for instance, showed how the internet has contributed to 21 percent of GDP growth in developed economies from 2007-2011.[87] Often the term Digital Economy is used to describe the sizeable part of the economy that is founded on the internet these days, both in developed and developing countries.[88] This digital economy is associated with high growth rates, showing again the opportunity that governments can seize if they increase internet connectivity.[89] In contrast, restricting internet access can come at an economic cost. Darell M. West, of the Brookings Institution, has highlighted how network shutdowns hurt economies.[90] In a study published in 2016, he calculates that in 2015, 81 short-term network shutdowns in 19 countries came at a cost of $2.4 billion to the global economy.[91] India and Morocco lost $968 million and $320 million respectively.[92]

In short, many countries have leaped into the internet age due to its scientific value and promise for economic growth that first propelled the US economy.[93] However, numerous governments were not aware that they had unwittingly also signed up to the anti-

[87] James Manyika and Charles Roxburgh, "The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity," *McKinsey*, October 1, 2011, https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-great-transformer.
[88] The Boston Consulting Group, "The Internet Economy in the G-20," March 2012, https://image-src.bcg.com/Images/The_Internet_Economy_G-20_tcm9-106842.pdf.
[89] Ibid.
[90] Darrell M. West, "Internet Shutdowns Cost Countries $2.4 Billion Last Year," *Brookings Institution*, October 6, 2016, https://www.brookings.edu/research/internet-shutdowns-cost-countries-2-4-billion-last-year/.
[91] Ibid.
[92] Ibid.
[93] Ben Geier, "What Did We Learn From the Dotcom Stock Bubble of 2000?," *Time*, March 12, 2015, https://time.com/3741681/2000-dotcom-stock-bust/.

censorship principle that came ingrained in the internet protocols, social media platforms and the decentralised nature of the internet (infrastructure is mostly owned by a plethora of private entities).[94] In Iran, for instance, the internet was seen for a long time as a tool to be used for science rather than a tool that would be used for political or journalistic purposes.[95] With the increasing availability of the internet to wide swaths of the population in these countries, information and the internet have become more crucial not only to the economy but also to regime survival. Hence, the anti-censorship principle, which was ingrained in internet technologies, became an increasingly unwelcome option for many authoritarian-leaning governments.[96] Once they realised (especially after the Arab Spring) the subversive nature of the internet, countries around the world started importing Chinese and Russian technology in a wish to gain more control over the internet.[97] With more and more tools and techniques available globally, which were also provided by Western suppliers, governments started reigning in the internet. As a result, internet freedom went into decline in recent years.[98]

While many countries have shunned internet freedom recently and imposed repressive information control, a small group of countries still embraces digital rights online.

The main goal of the next section is to examine the group of countries constituting the "Freedom Online Coalition +" as an observation as well as the internet freedom community within those countries. The aim is to get a better sense as to what has driven

---

[94] Timothy S. Wu, "Cyberspace Sovereignty? The Internet and the International System," *Harvard Journal of Law & Technology* 10, no. 3 (1997): 647–66; Mueller, "Against Sovereignty in Cyberspace."
[95] Babak Rahimi, "Censorship and the Islamic Republic: Two Modes of Regulatory Measures for Media in Iran," *The Middle East Journal* 69, no. 3 (2015): 358–78.
[96] Powers and Jablonski, *The Real Cyber War: The Political Economy of Internet Freedom*.
[97] Mueller, "Against Sovereignty in Cyberspace."
[98] Valentin Weber, "Why China's Internet Censorship Model Will Prevail over Russia's," December 12, 2017, https://www.cfr.org/blog/why-chinas-internet-censorship-model-will-prevail-over-russias.

those countries to adopt internet freedom and get a better idea of what constitutes the internet freedom community within those countries, and how it is organised. Despite the significance of non-state actors in forming the internet freedom norm, this thesis sees state actors as central to the internet freedom norm, whether it relates to organisational or funding aspects.

"Freedom Online Coalition +"

The US can rely on the Freedom Online Coalition+ (FOC+) to regularly support its multistakeholder approach in international organisations and when implementing internet governance in their jurisdictions. The like-mindedness of these countries is a powerful tool in the US' confrontation with China and Russia, who are proponents of a more state-centric approach to internet and technological governance more broadly.

The FOC+ consists of 36 countries in total: 31 members of the FOC and 5 countries that have a free internet environment. The Freedom Online Coalition was founded in December 2011 in the Hague, the Netherlands, by 15 countries.[99] The 2011 event took place after the launch of the US internet freedom agenda in 2008.[100] The. FOC is an intergovernmental group of 31 countries, excluding the US, that have vowed to promote internet freedom: Argentina, Australia, Austria, Canada, Costa Rica, the Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Ghana, Ireland, Japan, Kenya, Latvia, Lithuania, the Maldives, Mexico, Moldova, Mongolia, the Netherlands, New

[99] Freedom Online Coalition, "History," *Freedom Online Coalition*, 2020, https://freedomonlinecoalition.com/about-us/history/.
[100] Ryan Henry, Stacie L. Pettyjohn, and Erin York, "Portfolio Assessment of the Department of State Internet Freedom Program" (RAND Corporation, 2014), https://www.rand.org/content/dam/rand/pubs/research_reports/RR700/RR794/RAND_RR794.pdf.

Zealand, Norway, Poland, Spain, Sweden, Switzerland, Tunisia, and the United Kingdom.

The second group of countries that make up the FOC+, are countries that have a "free" internet according to the 2019 Freedom on the Net report by Freedom House.[101] Those are: Armenia, Hungary, Iceland, Italy, and South Africa.[102]

In total the "Freedom Online Coalition +" consists of 36 countries that explicitly (part of the Freedom Online Coalition) or implicitly (free online environment according to the Freedom on the Net index) endorse the internet freedom norm through domestic practices and international proclamations.

According to Painter, "the launch of the Freedom Online Coalition … was also a recognition that we had to bring governments together at a high level to deal with that issue too and particularly with internet freedom…[103] He continues by saying "I think it's a success when we have the Freedom Online Coalition and act together in a number of instances."[104]

Even after 2011 and the Arab Spring events, which have showcased the revolutionary potential of open internet technologies and platforms, Freedom Online Coalition+ countries still embrace the idea of internet freedom, which is particularly enshrined in the freedom of expression and the right to assembly online. Why? It is simply because FOC+

[101] Freedom House, "The Crisis of Social Media," *Freedom House*, 2020, https://freedomhouse.org/report/freedom-net/2019/crisis-social-media.
[102] Ibid.
[103] Interview with Christopher Painter on 2 May 2019.
[104] Interview with Christopher Painter on 2 May 2019.

countries have lower regime survival concerns when it comes to the internet. While the governments of these countries might still be uncomfortable with people organising themselves on major social media platforms and organising major protests, leaders in FOC+ countries know that if they are ousted, the worse that can happen is that they lose their job. Authoritarian leaders, such as the ones in Russia, have memories of coup d'états, or killings after leaders have left office.[105]

While the ensuing chapters will show how China and Russia are trying to build a community of like-minded countries, the US has launched the FOC with the Netherlands, which serves the similar purpose of organising the demand side of norm diffusion.[106]

The FOC+ and its internet freedom community

The internet freedom demand side does not only consist of the FOC+ member countries, but also of a plethora of non-state actors, which are located within these countries. Internet freedom organisations and individuals are also located in other countries, but the predominant part of the active organisations is resident in FOC+ countries. The next few lines are dedicated to mapping the internet freedom community. In the mapping process, the chapter identifies different sub-communities within the internet freedom community.

Many organisations that are part of the community can be classified into different categories, such as, for instance, the Citizen Lab, which is situated both in academia and takes on the role of a facilitator through its annual Citizen Lab Summer Institute.[107] If the

[105] Keir Giles, *Moscow Rules: What Drives Russia to Confront the West*, What Drives Russia to Confront the West (Washington, D.C. : London: Brookings Institution Press, 2019).
[106] Rebecca MacKinnon, "It's Not Too Late to Save the Internet," *Slate Magazine*, August 19, 2020, https://slate.com/technology/2020/08/save-the-internet.html.
[107] "Citizen Lab Summer Institute on Monitoring Internet Openness and Rights," *The Citizen Lab*, 2019, https://citizenlab.ca/summerinstitute-2019/.

reader perceives the Citizen Lab more as a research organisation, she can consider it being in the academia category. The categories are fluid and not supposed to be rigid. Many individuals are at some point part of one, two, or more communities, or delve into one at one point and into another at a future point in time. The enumerations of organisations and individuals in each category are non-exhaustive and could not include all projects and individuals involved due to space constraints. Keeping this in mind, this thesis outlines the following sub-communities within the internet freedom community: the cyber-libertarians and technologists; the facilitators; the philanthropists; the academics; human rights organisations and think tanks.

Cyber-libertarians and technologists: The first line of defence on the digital frontline

While state actors are primarily driven by materialistic calculations of gaining influence, the internet freedom community is driven by ideational goals and the belief that the internet is something special, a free space, largely separate from the offline space. These perceptions of internet freedom have had a strong impact on the community. In a 2014 talk, Nathan Freitas, an American software developer and internet freedom activist said, for instance:

> "I want the whole world to be more free to communicate directly and privately with each other, no matter where they are or what they have to say. I want the promise of the Internet to be fulfilled, and to not be turned against users/humans/citizens as a mechanism of increased control. I have no interest in beating the drums of cyberwar.[108]

Individuals with these ideas also hold key positions within internet governance institutions and have been vocal critics of China's proposals to make the internet more

[108] Nathan Freitas, "The Great Firewall Inverts," *Berkman Klein Center*, January 13, 2014, https://cyber.harvard.edu/events/luncheon/2015/01/freitas.

state centric. One of those personalities is Patrik Fälström, a long-haired hippie engineer and known in Sweden as the father of the internet.[109] He wrote internet protocols in the 1980s and was part of a community of engineers in the US and Europe who were instrumental in shaping the internet landscape.[110] More recently, he has been Sweden's representative at internet organisations such as the ITU (International Telecommunication Union).[111] It is also at the ITU where he criticised China's "New IP" [internet protocol] that is allegedly intended to make the state more central to running the internet, which has until now been largely run by private companies and individuals.[112] The Financial Times describes him as the embodiment of "the cyber-libertarian western ideals that were woven into its foundation."[113]

The community's heart is its technological community, which has taken on censors by developing tools to monitor and evade censorship and surveillance. Some of the nodes within the technological community are the Tor Project, which was an early pioneer in the anonymisation of users, OONI (Open Observatory of Network Interference) and GreatFire.org, (leaders in large-scale detection of censorship), Signal (by championing end-to-end encryption for the masses through its Signal Protocol), the Guardian Project, eQualit.ie, Google's Jigsaw (which are developing mobile security software with the aim of furthering digital rights), and Psiphon (which has been developing and maintaining censorship-circumvention software).[114]

---

[109] Madhumita Murgia and Anna Gross, "Inside China's Controversial Mission to Reinvent the Internet," March 27, 2020, https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f.
[110] Internet Assigned Numbers Authority, "Patrik Fallström," July 28, 2014, https://www.ianacg.org/icg-files/bios/bio-falstrom-28jul14-en.pdf.
[111] Murgia and Gross, "Inside China's Controversial Mission to Reinvent the Internet."
[112] Ibid.
[113] Ibid.
[114] OONI, "OONI - Open Observatory of Network Interference," n.d., https://ooni.torproject.org/; GreatFire.org, "Home," 2020, https://en.greatfire.org/; Signal Messenger, "Home," *Signal Messenger*, 2020, https://signal.org/; Guardian Project, "About," *Guardian Project*, 2020,

Internet freedom community's critical nodes: The facilitators

The "facilitators" category focusses (1) on organisations that are entirely dedicated to internet freedom and (2) bring together various organisations/individuals of the internet freedom community. They hence serve as critical nodes of the internet freedom community. Those nodes are: Access Now, Citizen Lab, Global Network Initiative, Digital Freedom Fund, and European Digital Rights.

Access Now is a non-profit with several headquarters across different continents. It focusses on defending and extending the rights of citizens to the digital space through maintaining a 24/7 digital security helpline for frontline activists, and by providing grants, advocacy, and legal support to civil society groups.[115] The major public activity of Access Now is its annual RightsCon conference, which is the world's largest conference dedicated to human rights online.[116] The first conference took place in 2011 in Silicon Valley and has since taken place in Rio de Janeiro, Tunis, Manila, and Brussels, amongst other locations.[117] The conference provides a great insight into the composure of the internet freedom community. In the 2017 iteration of RightsCon in Brussels, 1, 518 people from 105 countries participated.[118] In 2018, there were already 2,520 participants

https://guardianproject.info/; eQualitie, "Home," 2020, https://equalit.ie/portfolio/censorship-no/; Jigsaw, "Issues," 2020, https://jigsaw.google.com/issues/; Psiphon, "Home," 2020, https://psiphon.ca/.

[115] Access Now, "About Us," *Access Now*, 2020, https://www.accessnow.org/about-us/.

[116] Access Now, "History," *RightsCon Summit Series*, 2020, https://www.rightscon.org/about-and-contact/.

[117] Ibid.

[118] Access Now, "RightsCon Brussels - Outcomes Report," 2017, https://www.rightscon.org/cms/assets/uploads/2017/06/Rightscon-2017-Brux-Outcome-Report.pdf; Access Now, "RightsCon Toronto - Outcomes Report," 2018, https://www.rightscon.org/cms/assets/uploads/2018/07/RightCon2018-outcomes-report.pdf; Access Now, "RightsCon Tunis - Outcomes Report," 2019, https://www.rightscon.org/cms/assets/uploads/2019/10/RC19-Tunis-outcomes-report.pdf; Nikki Gladstone, "Thank You for a Historic RightsCon Online," *RightsCon Summit Series*, July 31, 2020, https://www.rightscon.org/thank-you-for-a-historic-rightscon-online/.

from 118 countries, in 2019, 2,797 participants from 122 countries, and in 2020, 7,828 attendees from 158 countries.[119] The rise in numbers from 2019-2020 can probably be attributed to the fact that the 2020 iteration has taken place entirely online and provided ease of access to many people that could sometimes not afford to attend a conference or obtain a visa/travel permit. Taking these numbers into consideration, one can estimate the global internet freedom community amounting to between 5,000 – 10,000 people.

Most participants have historically been from North America and Europe. However, participation from other regions has grown. For the 2019 RightsCon in Tunis, for instance, 36% of participants were from Africa, followed by North America (22%), Europe (21.5%), Middle East and Asia Pacific (each 6%), Latin America (5%), and 3.5% did not disclose.[120]

[119] Access Now, "RightsCon Brussels - Outcomes Report"; Access Now, "RightsCon Toronto - Outcomes Report"; Access Now, "RightsCon Tunis - Outcomes Report"; Gladstone, "Thank You for a Historic RightsCon Online."
[120] Access Now, "RightsCon Tunis - Outcomes Report."

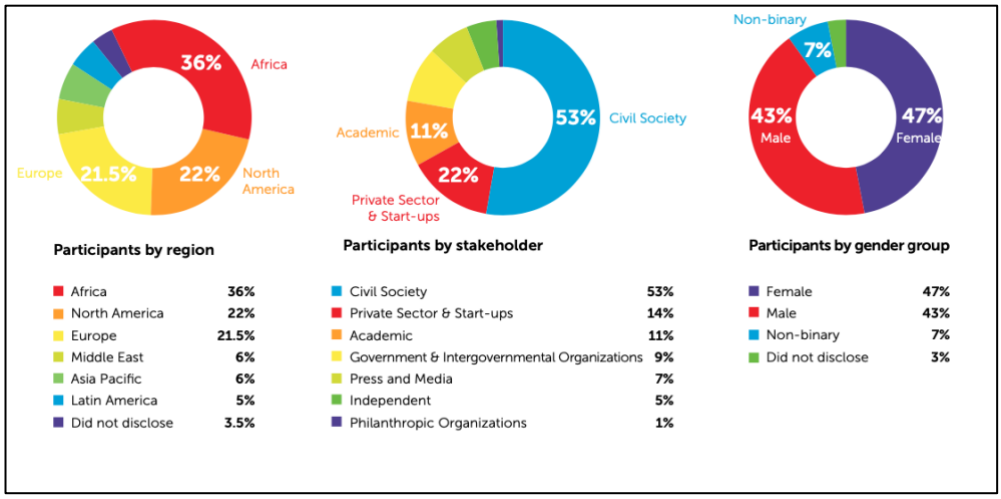


Figure 2: 2019 RightsCon Tunis participant breakdown by region, stakeholder, and gender.[121]

The Citizen Lab is an interdisciplinary laboratory within the University of Toronto's Munk School of Global Affairs.[122] Its scope of work includes technical and social science research, and advocacy related to digital human rights.[123] Once per year, it organises the Citizen Lab Summer Institute (CLSI), which is intended to bring together researchers from different disciplines to create synergies.[124] The 2018 CLSI, for instance, included between 50-100 participants that are active researchers in the online human rights field.[125] Some of the projects that are a result of the CLSI, such as Exposing the Great Cannon or Documenting Internet Filtering in Zambia, show how important interdisciplinary collaboration is and the Citizen Lab's facilitation and fostering of such research.[126]

[121] Ibid.
[122] Citizen Lab, "About the Citizen Lab," *The Citizen Lab*, 2020, https://citizenlab.ca/about/.
[123] Ibid.
[124] "Citizen Lab Summer Institute on Monitoring Internet Openness and Rights."
[125] The information was provided to the author by the Citizen Lab.
[126] "Citizen Lab Summer Institute on Monitoring Internet Openness and Rights."

The Global Network Initiative (GNI) is a non-governmental organisation that works with major companies on reducing censorship and protecting privacy rights.[127] It established a set of principles, such as commitment to freedom of expression, responsible company decision-making, and multistakeholder collaboration.[128] Companies that are part of the GNI have committed to deeply implement those principles into their business operations.[129] GNI members include Ericsson, Google, Facebook, Line, Microsoft, Nokia, and Telefónica. While the commitment of major companies to implementing the principles is encouraging, they are at the same time driven by profit considerations.[130] Google, for instance, has had a troubled past of attempting to enter the Chinese market at the expense of human rights considerations.[131] The company's Project Dragonfly encompassed a search engine that would censor at the behest of the Chinese government and expose its users to state monitoring.[132] Nokia for its part has been complicit in running parts of Russia's SORM surveillance system.[133]

The Digital Freedom Fund (DFF) serves as a catalyst for strategic litigation (which involves cases that have impacts that go beyond the individual case) concerning digital rights within member countries of the Council of Europe.[134] It provides grants to support such litigation, e.g., pre-litigation research, and a platform for networking and training of

[127] Global Network Initiative, "GNI Home," *Global Network Initiative*, accessed October 16, 2019, https://globalnetworkinitiative.org/.
[128] Global Network Initiative, "The GNI Principles," *Global Network Initiative*, 2020, https://globalnetworkinitiative.org/gni-principles/.
[129] Ibid.
[130] Global Network Initiative, "GNI Home."
[131] Matt Sheehan, "How Google Took on China—and Lost," *MIT Technology Review*, December 19, 2018, https://www.technologyreview.com/2018/12/19/138307/how-google-took-on-china-and-lost/.
[132] BBC News, "Google's Chinese Search Engine 'Terminated,'" July 17, 2019, sec. Technology, https://www.bbc.com/news/technology-49015516.
[133] Interview with Nani Jansen Reventlow on 4 June 2019, Director of Digital Freedom Fund. Zack Whittaker, "Documents Reveal How Russia Taps Phone Companies for Surveillance," *TechCrunch*, accessed July 31, 2020, https://social.techcrunch.com/2019/09/18/russia-sorm-nokia-surveillance/.
[134] Digital Freedom Fund, "About," 2020, https://digitalfreedomfund.org/about/.

litigators in the field.[135] In short, the DFF is a critical node for legal practitioners within the internet freedom community. In a 2018 strategy meeting, the DFF convened 32 different organisations and 48 organisations in 2019.[136]

European Digital Rights (EDRi) is a Brussels-based association of human rights organisations.[137] As of 5 August 2020, it counts 42 member organisations, including Chaos Computer Club (Germany), Internet Society Bulgaria, and Panoptykon Foundation (Poland).[138] Its core focus is on surveillance, privacy, copyright reform, and net neutrality. It also conducts public awareness campaigns to draw attention to these issues.[139]

The enablers: Philanthropists

Several organisations and individuals are crucial to the internet freedom community, because of their financial support. Those include the Hewlett Foundation, John D. and Catherine T. MacArthur Foundation, Ford Foundation, Mozilla, the Berkman family, and Michael R. Klein.[140] While those entities have a wider philanthropic engagement, their specific commitment to the internet freedom community has enabled the work of many.

Ponderers: Academics and think tankers

Academic and think tank institutions contain another important ecosystem of the community. Computer Science, Politics & International Relations, Internet Studies, and

[135] Ibid.
[136] Interview with Nani Jansen Reventlow.
[137] EDRi, "About," 2020, https://edri.org/about/.
[138] Ibid.
[139] Ibid.
[140] Access Now, "Funding," *Access Now*, 2020, https://www.accessnow.org/financials/; Berkman Klein Center, "Funding & Support Policies," December 11, 2019, https://cyber.harvard.edu/about/support; Citizen Lab, "About the Citizen Lab."

Communications departments at universities are crucial suppliers of research on surveillance and censorship. Academic conferences such as USENIX's Foci or PETS (Privacy Enhancing Technologies Symposium) serve as additional meeting points for the academic community in this research stream.[141] Academic research labs that have invented and refined circumvention tools as well as enabled important network monitoring of censorship and surveillance are University of California's San Diego's Center for Applied Internet Data Analysis, University of Michigan's Censored Planet, the Centre for Doctoral Training in Cyber Security and Oxford Internet Institute at the University of Oxford, the Journalism and Media Studies Centre at the University of Hong Kong, the University of Maryland's computer science department, and Harvard University's Berkman Klein Center, to name just a few.[142]

Think tanks, too, have contributed to the community's research output. The Digital Asia Hub in Hong Kong, or New America's Open Technology Institute are examples, just like Kenya's ICT Network is, the Ugandan-based CIPESA, or the Waterloo-based Centre for International Governance Innovation. Various research institutions' initiatives, such as Ranking Digital Rights' Corporate Accountability Index, or Freedom House's Freedom on the Net have also enriched the discussion surrounding internet freedom.[143]

---

[141] Proceedings on Privacy Enhancing Technologies Symposium, "PoPETs/PETS," 2020, https://petsymposium.org/; USENIX, "FOCI '20," December 17, 2019, https://www.usenix.org/conference/foci20.

[142] CAIDA: Center for Applied Internet Data Analysis, "About CAIDA," *CAIDA*, 2020, https://www.caida.org/home/about/index.xml; University of Michigan, "Censored Planet," *Censored Planet*, 2020, https://censoredplanet.org/; Oxford Internet Institute, "People - Joss Wright," 2020, https://www.oii.ox.ac.uk/people/joss-wright/; Twitter, "Greg Walton (@meta_lab) / Twitter," *Twitter*, 2020, https://twitter.com/meta_lab; Oxford Internet Institute, "Mahsa Alimardani," 2020, https://www.oii.ox.ac.uk/people/mahsa-alimadeni/; University of Hong Kong, "WeChatSCOPE | an Insight to Censorship in China," 2020, https://wechatscope.jmsc.hku.hk/; University of Maryland, "Geneva: Evolving Censorship Evasion," *Censorship.Ai*, 2020, https://geneva.cs.umd.edu/; Berkman Klein Center, "Home," 2020, https://cyber.harvard.edu/.

[143] Digital Asia Hub, "Home," 2020, https://www.digitalasiahub.org/; New America, "Open Technology Institute," 2020, https://www.newamerica.org/oti/; KICTAnet, "About KICTANET | KICTANet Think Tank," accessed July 31, 2020, https://www.kictanet.or.ke/about-kictanet/; CIPESA, "Online Freedoms,"

On the physical frontline: Human rights organisations and investigative media

The internet freedom community could not function without this sub-community, which often reveals online human rights violations and thereby brings the public's attention to it. More recently, several investigative stories have shown how important media are in the internet freedom community's endeavour to promote online human rights. The Wall Street Journal's investigative story showing how Huawei facilitates the oppression of opposition politicians and activists in Zambia and Uganda, or Andrei Soldatov's and Irina Borogan's revelations about Russia's surveillance assistance to countries within the former Soviet Union, serve as examples.[144]

One of the most important parts of the community are the many human rights organisations that operate on the physical frontlines of combatting illiberal online measures, whether this is in courtrooms, out on the streets, or lobbying in parliaments. Examples include Human Rights Watch's uncovering of the IJOP (Integrated Joint Operations Platform), which has been deployed by the Chinese police in Xinjiang, China. Further organisations dedicated to this vision include the Digital Security Lab Ukraine,

2020, https://cipesa.org/thematic-areas/online-freedoms/; Centre for International Governance Innovation, "Centre for International Governance Innovation," 2020, https://www.cigionline.org/search?search_api_fulltext=censorship&sort_by=publishing_or_event_date; Ranking Digital Rights, "2019 Ranking Digital Rights Corporate Accountability Index," *Ranking Digital Rights*, 2020, https://rankingdigitalrights.org/index2019/; Freedom House, "Freedom on the Net," *Freedom House*, 2020, https://freedomhouse.org/report/freedom-net.

[144] Human Rights Watch, "China: How Mass Surveillance Works in Xinjiang," May 1, 2019, https://www.hrw.org/news/2019/05/01/china-how-mass-surveillance-works-xinjiang; 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; Soldatov and Borogan, *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*.

Digital Society of Africa, Amnesty International, Electronic Frontier Foundation, Article 19, American Civil Liberties Union, and the Taiwan Association for Human Rights.[145]

5.3. Variation in the dependent variable

Internet freedom diffused alongside the internet to every corner of the world – except to two countries: China and North Korea.[146] Those two countries have since the start of diffusion established a national intranet. In contrast, even authoritarian regimes like Iran or Zimbabwe had a lax internet environment in the early days. In Iran, the internet arrived in 1992 but more stringent measures were only put in place in 2005.[147] In Zimbabwe, major international social media companies have had a strong presence throughout the years, and the regime has difficulties to reign them in.[148] In Russia too, services of major companies such as Google and Facebook are still widely accessible, although they have come under increasing pressure from the Russian government. So why did internet freedom diffuse across the globe but not to China and North Korea? As opposed to the

[145] Digital Security Lab Ukraine, "Лабораторія цифрової безпеки – Захищаємо громадянське суспільство," 2020, https://dslua.org/; Digital Society of Africa, "About," 2020, https://www.digitalsociety.africa/; Human Rights Watch, "China"; Amnesty International, "Amnesty Tech," 2020, https://www.amnesty.org/en/tech/; Electronic Frontier Foundation, "Home," *Electronic Frontier Foundation*, 2020, https://www.eff.org/; Article 19, "What We Do," 2020, 19, https://www.article19.org/what-we-do/; American Civil Liberties Union, "Privacy & Technology," *American Civil Liberties Union*, 2020, https://www.aclu.org/issues/privacy-technology; Taiwan Association for Human Rights, "Home," *台灣人權促進會 | Taiwan Association for Human Rights Since Dec.10 1984*, 2020, https://www.tahr.org.tw/.

[146] One may argue that internet freedom is not present in countries like Eritrea or Somalia because the percentage of individuals of the population that has internet access is close to zero, but one can still access the global internet from these two countries. In contrast the North Korean internet has also few internet users but is sealed off from the internet beyond its national borders. World Bank, "Individuals Using the Internet (% of Population) | Data," 2020, https://data.worldbank.org/indicator/IT.NET.USER.ZS.

[147] Ryan Grace, "Shatter the Web: Internet Fragmentation in Iran," *Middle East Institute*, December 14, 2020, https://www.mei.edu/publications/shatter-web-internet-fragmentation-iran.

[148] Interview with Senator David Coltart on 22 May 2020, Member of Parliament in Zimbabwe's National Assembly from 2000-2008; since 2008 a Member of the Senate; Minister of Education, Sport, and Culture from February 2009 – August 2013.

rest of the world, both Beijing and Pyongyang perceived the internet as a potential challenge to their regimes from the outset.

In the case of China, internet freedom never gained a foothold because Beijing has from the beginning considered the internet, like any other technology, as something that needed to be controlled tightly.[149] It unlikely felt threatened by the internet because it had controlled it from the outset. The internet was still an imagined threat to regime survival. At the same time, China wanted to reap the economic benefits of the internet. As a consequence, rather than only importing internet technologies from the US, China also changed those technologies in a way that allowed it to control them.[150] As a market entry requirement, it made Western companies remove the "freedom part" from internet technologies. It could do so because of its large market size, which made trade very attractive for Western companies. As such, China was for a long time the only country that managed to combine digital market growth and censorship. This was also aided by a belief amongst American policy makers and companies that it is only a matter of time until China would open up. For instance, president Bill Clinton proclaimed prominently in 2000:

> "When China joins the W.T.O. [World Trade Organization], by 2005 it will eliminate tariffs on information technology products, making the tools of communication even cheaper, better and more widely available. We know how much the Internet has changed America, and we are already an open society. Imagine how much it could change China. Now there's no question China has been trying to crack down on the Internet. Good luck! That's sort of like trying to nail Jell-O to the wall. But I would argue to you that their effort to do that just proves how real these changes are and how much they threaten the status quo.[151]

[149] Griffiths, *The Great Firewall of China : How to Build and Control an Alternative Version of the Internet*.
[150] Elizabeth C. Economy, "The Great Firewall of China: Xi Jinping's Internet Shutdown," *The Guardian*, June 29, 2018, sec. News, https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown.
[151] "Clinton's Words on China."

Clinton and other US policy makers were highly optimistic in their belief that the internet would transform China. American companies flocked into the country with the mindset that they will open up China, that they will be a force for liberalisation. Rebecca MacKinnon, Director of Ranking Digital Rights, a US non-profit, wrote:

"There are a lot of companies that went into China in the 90s. People were much more hopeful. When Cisco first went into China, when Yahoo! Apple and Google first went into China, I was a journalist in China in the 90s and the assumption was that things were going to change. It was just a matter of time that the country would open up."[152]

In the corporate sector, there was a strong belief that China would change. The perception was that, while China was very stringent, American companies would make repressive information controls less bad than they would have been without them.[153] American corporations would provide a rayon of internet freedom in a country where things would have been doomed anyway. Yahoo! founder Jerry Yang stated in 2006 that: "You have to balance the risk of not participating…and people don't realize that being in the market every day there, and being on the ground, we are seeing changes, on the whole, for the positive."[154] Jerry Yang stated this sentence in defending the company after it had turned over internet protocol data that identified a journalist who had publicly disclosed an e-mail from the Chinese state bureaucracy to journalists ordering them not to report on the Tiananmen Square incident of 1989.[155] But Yahoo! was not the only complicit company in making internet technologies compatible with surveillance and censorship. Cisco was

[152] Rebecca MacKinnon on 14 June 2019, Founding Director Ranking Digital Rights.
[153] Interview with Rebecca MacKinnon on 14 June 2019, Founding Director Ranking Digital Rights.
[154] Rebecca MacKinnon, "Yahoo! Abomination. (YHOO)," *RConversation*, March 29, 2006, https://rconversation.blogs.com/rconversation/2006/03/yahoo_abominati.html.
[155] The New York Times, "Yahoo Chief Apologizes to Chinese Dissidents' Relatives," November 7, 2007, sec. Business, https://www.nytimes.com/2007/11/07/business/worldbusiness/07iht-yahoo.1.8226586.html.

crucial in the building of China's Great Firewall. This led Jack Goldsmith and Tim Wu to write that "the modern 'Great Wall of China' is, in effect, built with American bricks."[156] This thinking within American companies persists even into the present. In 2019, revelations showed that Google had worked on a search engine for the Chinese market, dubbed Dragonfly, that blacklisted hundreds of words, such as, "student protest" or "human rights".[157] The project was terminated after mounting public pressure and employee resistance within the company.[158] Nevertheless, Eric Schmidt, former Google CEO, stated that Google's censored search engine would help change China to "be more open".[159]

The only other country where internet freedom has not diffused to is North Korea. This is likely to be because, already for a long time, North Korea had been the most isolated country in the world. In this context, the leadership wanted to control the internet and related technologies from the outset, like everything else entering the country. The hereditary Kim dynasty and elites more broadly did not give the internet even the slightest chance to become a challenge to their regime.[160] Like in China, North Korea sealed itself off the global internet completely while establishing a domestic intranet, with a separated information ecosystem. The internet (without its freedom component) hence never really

---

[156] Jack L Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (New York: Oxford University Press, 2006): 93.
[157] Ryan Gallagher, "Google's Censored Search Would Help China 'Be More Open,' Said Ex-CEO Eric Schmidt," *The Intercept*, May 14, 2019, https://theintercept.com/2019/05/14/google-search-china-eric-schmidt-comments/.
[158] BBC News, "Ex-Google Boss Defends Multiple Controversies," May 13, 2019, sec. Technology, https://www.bbc.com/news/technology-48262148; BBC News, "Google's Project Dragonfly 'Terminated' in China," July 17, 2019, sec. Technology, https://www.bbc.com/news/technology-49015516.
[159] Gallagher, "Google's Censored Search Would Help China 'Be More Open,' Said Ex-CEO Eric Schmidt."
[160] Fragkiska Megaloudi, "Transforming the World's Most Isolated Nation," *Al Jazeera*, December 18, 2014, https://www.aljazeera.com/features/2014/12/18/transforming-the-worlds-most-isolated-nation; Martyn Williams, "How the Internet Works ('Works') in North Korea," *Slate Magazine*, November 28, 2016, https://slate.com/technology/2016/11/how-the-internet-works-in-north-korea.html.

posed a challenge to the North Korean regime. In the words of Martyn Williams, a North Korea Watcher and Fellow at the Stimson Center think tank based in Washington, D.C., puts it this way:

> "In place of the internet, the North Korean government is doing something that no other country has done: building a nationwide intranet that offers email and websites but is totally shut off from the rest of the world. It's an audacious attempt to usher in some of the benefits of electronic communications while maintaining complete control on an entire population. It probably wouldn't work anywhere else in the world, but the North Korean government keeps its people in such fear that few dare attempt dissent."[161]

This thesis agrees with Williams' assessment but adds that in addition to North Korea, China is the only other country where the project of a national intranet has worked and been pursued since the arrival of internet technologies in the country.

North Korea's domestic intranet, which is completely sealed off the world, is called Kwangmyong (광명).[162] On the intranet one can find email services, e-learning platforms, and a few domestic websites (mostly government news agencies and a website with recipes for North Korean dishes).[163] The history of the internet in North Korea is rather recent. In 2001, an email connection was established between China and North Korea.[164] Then in 2010, the government created a full-time connection for foreign organisations and domestic government and ministries.[165] In a country of 25 million people, today's access to the intranet network is physically restricted and limited to a few

[161] Williams, "How the Internet Works ('Works') in North Korea."
[162] Ibid.
[163] Rebecca Hersher, "North Korea Accidentally Reveals It Only Has 28 Websites," *NPR.Org*, accessed December 28, 2020, https://www.npr.org/sections/thetwo-way/2016/09/21/494902997/north-korea-accidentally-reveals-it-only-has-28-websites.
[164] Williams, "How the Internet Works ('Works') in North Korea."
[165] Ibid.

thousand people at universities and government offices.[166] Internet usage has increased recently, but this hike in usage is largely linked to government institutions that are involved in state-sponsored cyber operations.[167]

In contrast, the inner circle of the North Korean leadership, estimated to a few dozen families, has unrestricted access to the global internet.[168] Recorded Future, an American cyber threat intelligence firm, maintains that North Korean military and political elites use the internet for revenue generation (cybercrime), the acquiring of prohibited knowledge (missile technology), reading international news (to understand what political repercussions their actions have), visiting health and gaming content, and video streaming platforms.[169]

In addition to segregating the North Korean intranet from the rest of the world, the leadership has changed technology with the aim to limit the freedom of Korean citizens. For instance, the Kwangmyong does not use Windows or Mac operating systems, but a modified version of Linux open-source software (Red Star Operating System), which is geared towards suppressing free speech on the network.[170] Two researchers who analysed the North Korean Red Star OS have concluded that it "provides a set of surveillance

---

[166] Ibid.

[167] David E. Sanger, "North Korea's Internet Use Surges, Thwarting Sanctions and Fueling Theft," *The New York Times*, February 10, 2020, sec. U.S., https://www.nytimes.com/2020/02/09/us/politics/north-korea-internet-sanctions.html.

[168] Alicia P. Q. Wittmeyer, "Why Is Google's Eric Schmidt Heading to North Korea?," January 2, 2013, https://foreignpolicy.com/2013/01/02/why-is-googles-eric-schmidt-heading-to-north-korea/; Joyce Hackel, "When the Internet Goes Down in North Korea, There Aren't Many to Notice," *The World from PRX*, December 23, 2014, https://www.pri.org/stories/2014-12-23/when-internet-goes-down-north-korea-theres-not-many-notice.

[169] Recorded Future, "How North Korea Revolutionized the Internet as a Tool for Rogue Regimes," February 10, 2020, https://www.recordedfuture.com/north-korea-internet-tool/; Recorded Future, "North Korea Is Not Crazy," June 15, 2017, https://www.recordedfuture.com/north-korea-cyber-activity/.

[170] Florian Grunow and Niklaus Schiess, "Lecture: Lifting the Fog on Red Star OS," *Chaos Computer Club*, December 27, 2015, https://fahrplan.events.ccc.de/congress/2015/Fahrplan/events/7174.html.

features like the capabilities to watermark different types of files that can be used to track the distribution of documents and multi-media files," which allows for an all-encompassing surveillance of the network.[171] The browser available on the operating system is called Naenara (내나라) and is an outdated version of Mozilla Firefox.[172]

Naenara is tightly controlled and regularly sends user data to the central administrators and all email and calendar entries are routed centrally, according to Robert Hansen, a security researcher that analysed the code of Naenara.[173]

5.4. Why geographical proximity and constructivist explanations fail to explain internet freedom norm diffusion

Constructivism provides a partial and insufficient explanation for internet freedom diffusion. It gives an understanding of the motivation underlying diffusion but not a full explanation. There is no doubt that there has been an ideational commitment to freedom within the various US administrations. Whenever presidents Clinton, Bush, Obama, and Trump promoted internet freedom, there was, however, often an overlap with material interests, whether those are economic (expansion of US internet giants) or political (regime change in Iran and China). It is difficult to disentangle the ideational and material interests in the promotion of internet freedom, but one has to acknowledge that both have been major motivations in the process.[174]

---

[171] Ibid.

[172] Robert Hansen, "North Korea's Naenara Web Browser: It's Weirder Than We Thought | WhiteHat Security Blog," January 8, 2015, https://web.archive.org/web/20150108223420/https://blog.whitehatsec.com/north-koreas-naenara-web-browser-its-weirder-than-we-thought/.

[173] Ibid.

[174] Connolly, *The Terms of Political Discourse*.

Constructivism is partially right when it comes to pointing to the ideational motivation of internet freedom export. However, the theory is wrong when it comes to explaining where diffusion would occur. Constructivists would have expected diffusion to countries that share US ideational views about freedom, e.g. United Kingdom, Japan, South Korea, maybe India or Malaysia, but they would not have expected internet freedom to be present in authoritarian regimes like Zimbabwe or Iran.[175] The US could have never "persuaded" dictators into accepting a revolution-propelling technology. In fact, the US did not manage to "persuade" those countries into accepting the TCP/IP protocol or access to social media networks. Those countries imported those technologies/services because they only saw the scientific/economic benefit and were not aware of the political repercussions the technology could have, and when they did (end of 2000s, beginning of 2010s), it was too late. The technology diffused and major monopolistic US companies established themselves in their countries offering services that would allow for easier organisation of protests and dissemination of political information.

Geographical proximity scholars do not believe in the mechanisms of persuasion to the extent that constructivists do. They believe in the explanatory power of political and economic interdependence between countries. Whenever there is great economic and political interaction between two countries, internet freedom is likely to diffuse. A basic premise of geographical proximity theorists is that geographical closeness translates into greater interdependence. Hence, geographical proximity scholars would expect geographical proximity to be the most important indicator to explain internet freedom diffusion. Nevertheless, this is not the case. Internet freedom has diffused to every corner

[175] To give an example, constructivists would have expected women's rights to protrude to most countries but, for instance, not to Saudi Arabia, where male leaders hold other ideational views.

of the world (except China and North Korea). The cyber norm is present in Ghana (Africa), just as it is in South Korea, Japan (Asia), or Slovenia (Europe).

Geographical proximity scholars may interject that internet freedom has not diffused to North Korea because there was little economic and political interdependence between the US and North Korea. But interestingly, internet technologies have diffused to North Korea, but Pyongyang has amended them and taken out all the freedom aspects of the technology. Every keystroke is being openly monitored by the state (inducing self-censorship), access to the global internet is cut off (censorship), and the only information available on the North Korean intranet is provided by national news agencies (propaganda).

Neoclassical realism provides a more accurate explanation than constructivism or geographic proximity theory do. It claims that internet freedom would diffuse to all countries where the US seeks influence (in the US case this quest for influence is global) and where elites perceive the internet as a tool to boost economic growth, rather than a threat to their regime. Most countries did have such low threat perception for years, when they had not yet realised the internet's potential for organising social upheaval and protests. Only China and North Korea imagined the internet as a "potential threat" from the beginning. It was not yet a "threat" to them, but a "potential threat." As a result, they heavily restricted or modified the technology entering their countries. China allowed Google and Yahoo! to offer internet services, but they had to abide to censorship. Because China's market was so large, it could force internet giants to comply with its terms. North Korea changed the Linux operating system in a way that would allow for all-

encompassing surveillance. In short, North Korea and China imported internet, but without the "freedom component" in order to maintain regime stability.

5.5. The US technosphere and sovereignty

This chapter has so far traced the diffusion of the internet freedom norm and looked at the underlying causes as well as the institutional infrastructure the US has set up to promote internet freedom. The following discussion examines the emergence of a US technosphere and the implications of internet freedom diffusion for a norm-adopting country's sovereignty.

5.5.1. The US introduces checks and balances to domestic and interdependence sovereignty

The US invests millions of dollars every year in the development and dissemination of internet freedom technologies. By exporting internet technologies and censorship circumvention/anonymisation tools in particular, the US introduces checks and balances on domestic and interdependence sovereignty. It thereby makes the domestic and interdependence sovereignty of countries abroad look more like the one in the US. Domestic/interdependence sovereignty in the United States translates into independent media and citizens being able to question domestic authorities, through investigative reporting and protesting in the streets. Internal sovereignty in the US is not only about the ability of the elites to control the information of their citizens, but of citizens to hold their elites accountable.

Software, such as Signal Messenger and Tor Browser, helps citizens evade surveillance and remain anonymous. This makes it more difficult for countries to investigate and

prosecute political dissidents or voices of the opposition. In turn, this ability to stay anonymous allows for political dissent and for checks and balances on political authorities to emerge.

Circumvention and anonymisation tools such as Psiphon and VPNs give citizens in Iran and Zimbabwe unrestricted access to websites and services that are otherwise banned in Tehran or Harare. By intentionally funding these technologies with precisely this purpose in mind, the US changes countries' interdependence sovereignty, i.e., their ability to control cross-border information flows, and remakes Iranian and Zimbabwean interdependence sovereignty look more like interdependence sovereignty in the US, where uncensored information flocking in from around the world shapes citizens' views on their own authorities.

By providing media and cybersecurity trainings to journalists in 100 countries, the US strengthens the role of independent media in a given country and shapes how media report. In Vietnam, for instance, the goal of the USAGM-provided training is to "strengthen free and open media…and provide accurate, objective, and balanced news and information to audiences overseas."[176] In Africa, the USAGM held sessions on "principles of reporting in a democracy."[177] By providing trainings on how to report independently, fact check, counter misinformation, protect free speech, conduct investigative reporting, the US strengthens journalists' ability to question political authority. By giving them cybersecurity trainings, it shields journalists from authorities'

[176] US Agency for Global Media, "BBG Provides Bird Flu Reporting Workshops," April 9, 2013, https://www.usagm.gov/2013/04/09/bbg-provides-bird-flu-reporting-workshops/.
[177] US Agency for Global Media, "News Coverage: Delivering News to Television," August 16, 2019, https://www.usagm.gov/2019/08/16/news-coverage-delivering-news-to-television/.

surveillance. In sum, through these trainings, the US enhances the check and balances on authorities in authoritarian-leaning countries, where independent media are threatened on a daily basis.

5.5.2. The US erodes Westphalian sovereignty

Through the export of US technology and international expansion of the internet freedom norm, a technosphere has emerged. The US technosphere is a geographical area where the US has both a privileged capability to control technology and where it influences the information control landscape in that country. [178] While US technology has diffused to 192 countries, the US provided training to 100. This is the so-called "peripheral technosphere" and in that sphere, the US' influence is less pronounced.

In contrast, the so-called "core technosphere" consists of countries that check all three indicators of diffusion. Here, the US hold more influence. Countries that are part of the technosphere are: Austria, Argentina, Armenia, Costa Rica, Germany, Georgia, Ghana, Kenya, Lithuania, Mexico, Moldova, Mongolia, the Netherlands, Poland, South Africa, Tunisia, and the UK.

[178] A part of this section and Chapter 8, on technospheres, was extracted from Weber, "Making Sense of Technological Spheres of Influence."

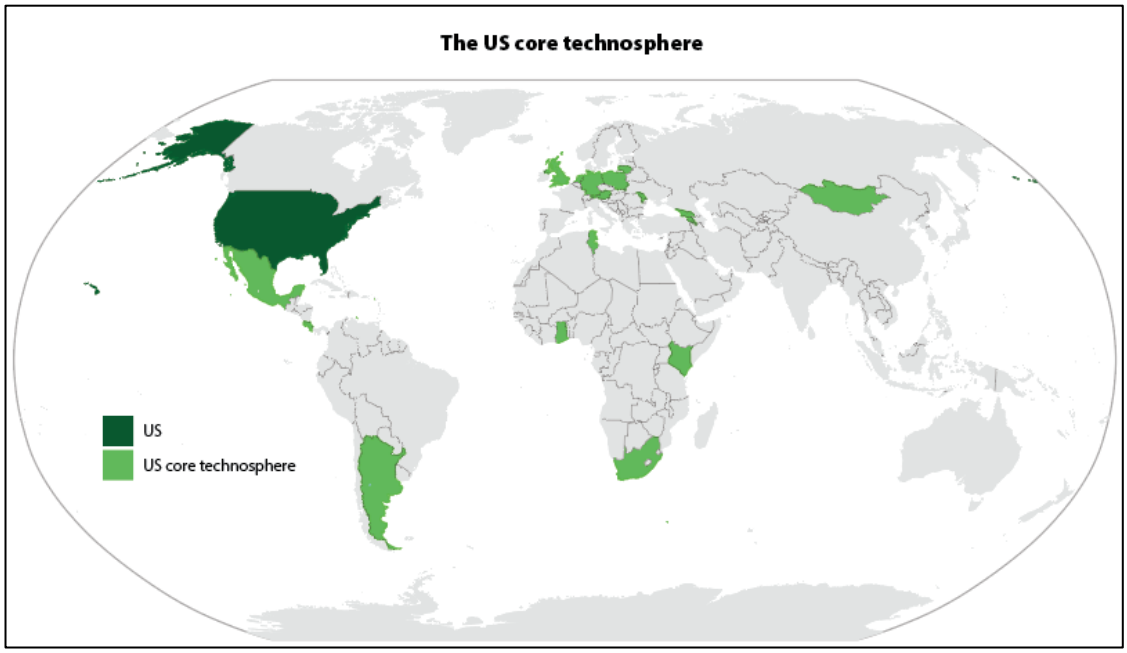


Figure 3: US core technosphere

The US derives political, economic, and intelligence benefits from internet freedom diffusion. Politically, the provision of journalist trainings may enhance US political influence abroad. Sometimes, US political interests overlap with trainings. In 2011, news made the headlines that the Central Intelligence Agency (CIA) conducted a polio vaccination programme in the area that Bin Laden lived in order to obtain his family's DNA, which would help the US government to find him.[179] The CIA move received a strong rebuke by Médecins Sans Frontières, which claimed that the fake vaccination programme "threatens immunisation work around the world."[180] In 2014, the White House declared that the CIA had stopped using vaccination programmes in its spying operations in August 2013.[181] Interestingly, in 2018, the US Agency for Global Media

[179] Saeed Shah, "CIA Organised Fake Vaccination Drive to Get Osama Bin Laden's Family DNA," *The Guardian*, July 11, 2011, sec. World news, https://www.theguardian.com/world/2011/jul/11/cia-fake-vaccinations-osama-bin-ladens-dna.
[180] Saeed Shah, "CIA's Fake Vaccination Programme Criticised by Médecins Sans Frontières," *The Guardian*, July 14, 2011, sec. Society, https://www.theguardian.com/world/2011/jul/14/cia-fake-vaccination-medecins-frontieres.
[181] The White House, "Monaco Letter on Vaccine Workers," May 16, 2014, https://www.documentcloud.org/documents/1164764-monaco-letter-on-vaccine-workers.html.

conducted journalist trainings in Afghanistan and Pakistan on "best practices of polio reporting."[182] The identical subject-matter of the previous CIA activities and US journalist trainings may be a coincidence, but it may also suggest a deliberate US strategy to repair its damaged image with regard to polio vaccinations amongst journalists and influence reporting on the issue in Afghanistan and Pakistan.

In intelligence terms, the US government has shown, through its PRISM surveillance programme, that it has the intent and capacity to harvest data directly from US companies with the aim to gather intelligence on foreign targets.[183]

Because the internet was initially rolled out within the US, a lot of the world's data traffic still flows through its territory. More than 70% of the worldwide internet traffic passes through Loudoun County, Virginia every day.[184] This opens a great opportunity for US intelligence services to intercept that traffic and derive intelligence from it. The US is also a prime supplier of hardware and software across the globe. In 2014, it was revealed that the NSA took advantage of that and intercepted Cisco equipment that was on its way to be exported.[185] In this way, the NSA could target specific customers abroad by inserting backdoors through supply chain interdiction.[186]

---

[182] "Afghanistan/Pakistan Workshop on Best Practices of Polio Reporting," *USAGM*, accessed December 30, 2020, https://www.usagm.gov/2018/07/12/afghanistanpakistan-workshop-best-practices-polio-reporting/.
[183] Sottek, "Everything You Need to Know About PRISM."
[184] Loudon Virginia, "Business & Industry Stats," *Loudon County Economic Development, VA*, n.d., https://biz.loudoun.gov/information-center/business-industry-stats/.
[185] Sean Gallagher, "Photos of an NSA 'Upgrade' Factory Show Cisco Router Getting Implant," *Ars Technica*, May 14, 2014, https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/.
[186] Ibid.

The revelations surrounding Crypto AG have shown how supplying key technology abroad can turn intelligence into influence abroad. Until recently, US and German intelligence agencies owned Crypto AG, a Swiss cryptographic equipment maker, which allowed them to snoop on dozens of countries.[187] The US used this capability to spy on Argentinian communications during the Falklands War (the US shared information with the UK), thus demonstrating how control over technology can enhance other forms of statecraft.[188] Still, this privileged capability to exert control is not exclusive. A Cisco router or subverted cryptography machine may give the US a head-start in hacking a device, but this does not prevent Iran or China from gaining access as well.

In general, one has to assume that the US has the capability to control every state's internet-connected technology, if it wishes so. It might have greater sway over some states than others, such as over the UK and Japan, because these states rely more heavily on US technology procurement as a result of the exclusion of Chinese technology in their key networks.[189]

Jablonski and Powers give an overview of how internet freedom policies were tailored to increase US economic power.[190] These claims warrant further elaboration and a short account of how US commercial interests and an increase in power have gone hand in hand in the past few decades. The commercialisation of the internet started in the mid-

[187] Sean Gallagher, "For Decades, US and Germany Owned Swiss Crypto Company Used by 120 Countries," *Ars Technica*, November 2, 2020, https://arstechnica.com/tech-policy/2020/02/us-german-intel-owned-swiss-crypto-used-by-dozens-of-countries/.
[188] Ibid.
[189] Hadas Gold, "UK Bans Huawei From Its 5G Network," *CNN*, July 14, 2020, https://edition.cnn.com/2020/07/14/tech/huawei-uk-ban/index.html; Li Tao, "Japan Latest Country to Exclude Huawei, Zte From 5G Roll-Out," *South China Morning Post*, December 10, 2018, https://www.scmp.com/tech/tech-leaders-and-founders/article/2177194/japan-decides-exclude-huawei-zte-government.
[190] Powers and Jablonski, *The Real Cyber War: The Political Economy of Internet Freedom*.

1990s through the privatisation of internet infrastructure spearheaded by DARPA (Defense Advanced Research Projects Agency) and the NSF (National Science Foundation).[191] For the first time, the internet could be used for non-research purposes, i.e. commercial purposes.[192] Soon, Mosaic and Netscape, the first web browsers, were launched, which allowed for a lay person utilisation of the World Wide Web.[193] E-commerce started to gain traction and West Coast companies rose in value and quickly expanded from America across the globe.[194] The US government aided with the expansion across the world through internet freedom policies. Jablonski and Powers hold the view that:

> "U.S.-backed ventures to build up underdeveloped countries constituted a policy of creating new markets for U.S. products. As a global information economy developed, U.S. economic policy increasingly required that the rest of the world be able to import and consume "soft" products such as media content."[195]

As part of the internet freedom agenda, information was framed in the following way to promote American economic interests abroad. On the one hand, the US framed political information, and content related to American companies (software, social media platforms) in a way that they deserved free flow under free trade and open market principles.[196] On the other hand, the US framed content of American companies (copyright material), once exported, as deserving restricted dissemination to protect investors.[197] In short, the US promoted free flow/restriction on topics that suited them. In

[191] Naughton, "The Evolution of the Internet: From Military Experiment to General Purpose Technology."
[192] Ibid.
[193] Ibid.
[194] Ibid.
[195] Shawn M Powers and Michael Jablonski, *The Real Cyber War: The Political Economy of Internet Freedom* (Urbana, Chicago, and Springfield: University of Illinois Press, 2015): 28.
[196] Ibid.
[197] Ibid.

this economic sense, the internet freedom strategy was immensely successful. Even after 30 years of the internet's expansion, the top 10 list of the largest technology companies is still dominated by US entities.[198] In 2019, 8 out of the 10 largest technology companies were American, led by Apple as number one.[199]

5.6. Measuring the receding of internet freedom

Despite the international diffusion of internet freedom and the resulting emergence of a US technosphere, the norm has been receding recently:

> "As data and information are treated more and more as resources to be accumulated, processed, and traded, it becomes difficult to envision a world wherein governments will collectively agree on the need for their free flow across borders. This reasoning offers at least a partial explanation as to why information-control policies are becoming more prominent throughout the world today."[200]

The Freedom on the Net indices show that internet freedom has declined for the ninth consecutive year in 2019.[201] There has been a debate as to how steep that decline has been. Numerous scholars and experts have lamented the (near) death of internet freedom.[202] Others, such as Jason Pielemeier, have pinpointed that the internet is, even in 2018, in almost every country a freer space than "meatspace", that is, the offline space.[203] He compares the Freedom Online Press Index (offline world) and the Freedom on the Net

---

[198] Jonathan Ponciano, "The Largest Technology Companies In 2019: Apple Reigns As Smartphones Slip And Cloud Services Thrive," *Forbes*, May 15, 2019, https://www.forbes.com/sites/jonathanponciano/2019/05/15/worlds-largest-tech-companies-2019/.
[199] Ibid.
[200] Powers and Jablonski: 208.
[201] Freedom House, "The Crisis of Social Media," 2020.
[202] Kalev Leetaru, "The Death Of Internet Freedom: Mourning The Demise Of A 20-Year-Old Dream," *Forbes*, February 17, 2016, https://www.forbes.com/sites/kalevleetaru/2016/02/17/the-death-of-internet-freedom-mourning-the-demise-of-a-20-year-old-dream/; Jon Evans, "'The Dream Of Internet Freedom Is Dying,'" *TechCrunch*, August 5, 2015, https://social.techcrunch.com/2015/08/05/the-dream-of-internet-freedom-is-dying/.
[203] Pielemeier, "Reports of the Death of Internet Freedom Are Greatly Exaggerated."

index (online world) and comes to the conclusion that every country compared in these studies is freer online compared to citizens' offline rights.[204] If one compares, however, the latest Global Freedom Scores and Internet Freedom Scores, one perceives that out of sixty-five countries, fifty-one are ranked same online as they are offline.[205] Eight fare better online (Angola, Armenia, Cambodia, Georgia, Hungary, Libya, Rwanda, Uganda) and six worse (Brazil, India, Pakistan, South Korea, Thailand, Tunisia).[206] Considering the vastness of countries (e.g. India, Pakistan) that do worse online than offline it appears that more people have less rights online today than offline.

Paradoxically, while global internet freedom has declined, the number of people actively engaged in defending digital rights has grown. This trend – where an increasing danger/threat has been accompanied with growing activism – has precedent in history. In the 1970s, environmental concerns in the US, for instance, brought over 20 million people to the streets.[207] Protesters showed despair over recent environmental disasters, such as the Santa Barbara oil spill. At the same time, the first photos of earth from space brought a new perception of the earth to humans, showing them the fragility of the planet.[208] A similar perceived threat to online rights may have galvanised engagement in digital rights issues.

---

[204] Ibid.
[205] Freedom House, "Countries and Territories," *Freedom House*, 2020, https://freedomhouse.org/countries/freedom-world/scores.
[206] Ibid.
[207] Sophie Yeo, "How the Largest Environmental Movement in History Was Born," April 22, 2020, https://www.bbc.com/future/article/20200420-earth-day-2020-how-an-environmental-movement-was-born; NASA, "Earthrise," February 23, 2015, http://www.nasa.gov/multimedia/imagegallery/image_feature_1249.html.
[208] Yeo, "How the Largest Environmental Movement in History Was Born."

5.7. Conclusion

To conclude, this chapter highlighted the emergence of the internet freedom norm starting in the US of the 1970s. It showed how the US's model focusses on surveillance and propaganda and not so much on self-censorship (Russia), or censorship (China). The chapter then demonstrated that the US has promoted internet freedom because it has sought soft power abroad, in terms of economic (by promoting US technology companies abroad), as well as political influence (by pushing for democratisation in Iran through censorship circumvention tools) and to advance ideological goals (it wishes to increase the level of digital human rights across the world). The chapter continued by laying out the institutional architecture and funding schemes that the US has established to promote internet freedom.

The chapter then explored the demand side of diffusion and maintains that internet freedom was able to diffuse that broadly across the world because initially, countries only saw the economic benefit of the internet. They did not realise the internet's potential to create regime instability. After the Arab Spring, many countries started to repress online liberties and only a handful of countries (Freedom Online Coalition +) still pursued policies that allowed considerable amount of free speech and guarded digital human rights. As more and more countries started to become repressive online, a thriving internet freedom community of activists, researchers, and journalists, largely coordinated (Open Technology Fund) and funded (USAGM, USAID) by the US, emerged.

The chapter has also shown why internet freedom has diffused all over the world but not to China and North Korea, because they perceived very early on the "potential for regime threat" posed by an unfettered internet. In contrast, other authoritarian-leaning countries

only made this discovery later, when people empowered by the internet took to the streets. The chapter ensued by demonstrating that constructivist and geographical proximity theories of diffusion fail to fully explain the global diffusion of internet freedom. Constructivists have difficulties explaining the cyber norm's diffusion to Iran or Zimbabwe, which the US could not have persuaded to import a regime threatening technology. Geographical proximity scholars on the other hand see geographical closeness (a proxy for economic and political interconnectedness) as a factor for diffusion. But geographical closeness did not really play a role in diffusion. Internet freedom has diffused across the globe, largely independent of geography and interdependence. As opposed to geographical proximity explanations and constructivism, the neoclassical realist premise (diffusion occurs where the US seeks influence and where there is a perception within the elite of the importing country that the internet is a tool for economic growth, rather than a tool that would threaten their regime survival) provides a more accurate representation of diffusion. In addition to this, the chapter showed how the diffusion of internet freedom reshapes domestic and interdependence (US adds checks and balances) and weakens Westphalian sovereignty (US gains influence over the country) of an importing country. Finally, the chapter has measured the decline of the internet freedom norm in recent years. This leads the thesis to the next chapters, which analyse the rise of the Chinese and Russian internet sovereignty norms.

Chapter 6: The worldwide web of Chinese information controls

"… shutting down the internet in a state of emergency should be standard practice for sovereign countries…When China's Xinjiang region faced a similar national security threat a few years ago, the Chinese government responded with a similar strategy. However, it attracted sharp criticism from mainstream media in Europe and the U.S.

…The internet shutdown in India has once again proved that the necessary regulation of the internet is a reasonable choice of sovereign countries based on national interests, and a natural extension of national sovereignty in cyberspace…

The internet was first adopted in developed countries within Europe and America, which determines that these countries inevitably have a different cognitive concept from others. They strive to spread their jurisdiction online and squeeze the sovereignty of developing countries." Qing Qiu, People's Daily Online, 17 December 2019[1]

This chapter provides a definition of China's internet sovereignty norm (focus on censorship) and why it diffused to some countries and not others. This chapter presents a few cases of countries: that are part of the core technosphere (Iran, Egypt, Tanzania, Thailand, Uganda, Zambia, and Zimbabwe), the peripheral technosphere (Vietnam), where no diffusion occurred (Bahrain, Nicaragua, Syria). Why was diffusion more likely to occur to some countries than others? Firstly, the above-mentioned countries, where successful diffusion occurred, were affected by major anti-government protests in the early 2010s. These protests dramatically increased regime survival concerns amongst the leaders of these hybrid/authoritarian regimes, which in turn increased their demand for surveillance gear. Secondly, China fosters the supply of technology and training to those countries who are part of the BRI, because it sees it as its emerging sphere of influence, i.e., the prime geographical area where it wants to wield influence. In that context, the

[1] Qiu, "India's Internet Shutdown Shows Normal Practice for Sovereign Countries."

Chinese authorities have stated that the export of surveillance technologies will add a "secure" layer to the BRI, provide stability to those countries and thereby stability to Chinese imports.[2] At the same time, China has an unarticulated goal of seeking political influence by propping up elites in overseas countries through advanced surveillance equipment. This is the case, e.g., in several African countries, where China helped weaken political opposition through surveillance assistance.[3]

Having laid out the causal mechanisms underlying Chinese information control diffusion, as well as a section that examines countries where this thesis would have expected diffusion, but diffusion did not occur, this chapter shows how geographical proximity explanations and constructivism fail to provide explanations as to why internet sovereignty diffused to one country and not another.

The Chinese norm did not diffuse because countries were persuaded into adopting the norm (constructivist theory) or because countries were geographically close to China (geographical proximity theory). Importing countries were more than ready to buy and adopt Chinese information controls, because they feared for the survival of their regime and because China fostered exports where it sought influence.

Finally, this chapter demonstrates how this diffusion resulted in a sovereignty trade-off for importing countries. While the import of Chinese information control increased elites' internal sovereignty vis-à-vis their populations (better chances of regime survival), it

[2] Lianyungang Forum, "Focusing on 'Made in China' Weapons and Strong Police Prestige," accessed March 14, 2020, http://www.lygforum.gov.cn/index.php?m=news&a=details&content_id=306.
[3] Parkinson, Bariyo, and Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents."

decreased their external sovereignty vis-à-vis China (increased likelihood of espionage and economic dependence as a result of extractive surveillance deals).

6.1. China's internet sovereignty norm

When the internet arrived in China, its (handful of) users were euphoric. The first email that was circulated in China in September 1987 famously said: "Across the Great Wall we can reach every corner of the world."[4] Just like in the US, the internet was first reserved for officials and academics. Gradually, it was rolled out to a larger population. Concurrently, with that larger rollout, first information controls were put in place. Most prominently, in 1997, China had instituted laws against sanctioning online content that was deemed harmful to public security.[5] Authorities also started with the building of the "Great Firewall of China". The "Great Firewall" was meant to insulate the Chinese internet from the global internet. These are the early stages of the Chinese internet sovereignty norm that is quintessentially different to the US norm of internet freedom.

The Chinese sovereignty norm is distinct from the US norm in several ways. It sees the state at the centre of all internet processes, from regulation governing the internet, to content moderation. In short, the state has sovereignty over all aspects of the domestic internet, but also over flows that enter and exit the country through its international borders. To facilitate this norm, the authorities passed sweeping laws that require participation of Communist Party Committees at decision-making levels at domestic and international (technology) firms operating in China.[6] Authorities passed laws to facilitate

[4] Economy, "The Great Firewall of China."
[5] Ibid.
[6] Emily Feng, "Chinese Tech Groups Display Closer Ties with Communist Party," *Financial Times*, October 10, 2017, https://www.ft.com/content/6bc839c0-ace6-11e7-aab9-abaa44b1e130.

control, e.g., laws that allow them to access data on servers based in China at any time.[7] All in all, sovereignty over the internet has grown throughout the years and become more and more imposing on the domestic internet landscape. The amount of control China exerts over its internet users (compared to Russia and the US) is seen in China's surveillance, censorship, strategic information dissemination, and self-censorship inducing practices.

Surveillance

Compared to Russia, China has more options to monitor its citizens, because surveillance equipment is pervasive in modern Chinese society. China has also more options than the United States, since the US is domestically bound by judicial processes, independent courts on matters of surveillance. In Xinjiang, for example, citizens are constantly monitored through a combination of intrusive apps, facial recognition cameras, and other types of technology.[8] 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.[9] Although this monitoring is carried out by schools, the government supports such deployments through the "intelligent education" initiative.

---

[7] Steve Dickinson, "China's New Cybersecurity Program: NO Place to Hide," *China Law Blog*, September 30, 2019, https://www.chinalawblog.com/2019/09/chinas-new-cybersecurity-program-no-place-to-hide.html.

[8] 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.

[9] 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/.

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.[10] 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 sites like 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.[11] A significant portion of this censorship is still performed manually, but some tasks are now automated, such as known-keyword blocking.[12] Recently, China has increased censorship even against 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 the Tencent App Store.[13]

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

[10] Penney, "Chilling Effects: Online Surveillance and Wikipedia Use."
[11] 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.
[12] 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.
[13] Weber and Ververis, "Measuring Censorship on Mobile App Stores."

goal is not to engage in controversial topics, but rather to steer content away from controversy and towards pro-government posts.[14] As far back as 2004, Chinese authorities employed people to sway public opinion online.[15] 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 Party-friendly content online. Those were dubbed the 50 Cent Party.[16] It is estimated that there are now up to two million such employees, creating around 450 million posts per year.[17]

Self-censorship

Inducing self-censorship through intimidation was a widespread technique during the Mao era in China.[18] Since then, methods have shifted towards information control based on censorship and strategic information dissemination.[19] 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).[20] 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

[14] 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.
[15] Rongbin Han, "Manufacturing Consent in Cyberspace: China's 'Fifty-Cent Army,'" *Journal of Current Chinese Affairs* 2 (2015): 105–34.
[16] 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.
[17] King, Pan, and Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument."
[18] Margaret E. Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall* (Princeton N.J.: Princeton University Press, 2018).
[19] Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall*: 94.
[20] Ibid: 13–14.

media mandatory.[21] 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.[22]

6.2. The diffusion of China's internet sovereignty norm

6.2.1. Understanding the supply side of diffusion

The following section seeks to demonstrate that China's rationale for exporting information controls is strategic and that the ultimate goal is to increase influence abroad. In this vein, its efforts focus on exporting technology and techniques to countries of the BRI. Commercial gains are one motivation for exports. However, Beijing also aims to influence the political landscape abroad by reinforcing authoritarian leaders that endorse Beijing's model of information control.

The predominant part of Chinese exports go to the BRI, which is a strategic initiative that was officially launched in 2013 and comprises 138 countries.[23] 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.[24] 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. The initiative goes back to historical narratives, which highlight the tight connection between China and the

[21] 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; Cyberspace Administration of China, "Internet Forum Community Service Management Regulations," August 25, 2017, http://www.cac.gov.cn/2017-08/25/c_1121541921.htm.

[22] 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.

[23] 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.

[24] 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.

other countries of the initiative. In short, Beijing sees BRI as a revival of ancient silk trading roads.[25]

The revival receives active commitment from China. Beijing encourages the exchange of ideas, goods, and social interactions along the BRI. China, for instance, weaves journalist and media trainings into the BRI framework.[26] Most importantly for this thesis, Beijing actively encourages the export of information controls to countries of the BRI to secure and stabilise the BRI for its economic exports.

China's Ministry of Public Security set out to construct a "safe road", or "'Belt and Road' security corridor" between Asia and Europe.[27] This vision of connecting Europe and Asia in security terms was laid out at the Lianyungang Forum. The Forum is an annual event held in Lianyungang, where China and invited countries discuss law enforcement cooperation.[28] The central idea behind the Forum, which is hosted by China's Ministry of Public Security is to create a "community of security destiny."[29]The term derives its meaning from China's foreign policy goal of creating a "community of common destiny", which can be understood as a "new order" replacing an old Western-centric order.[30] The means to achieve the community of common destiny is the BRI. Hence, the "community

[25] 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.
[26] 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.
[27] Lianyungang Forum, "Focusing on 'Made in China' Weapons and Strong Police Prestige."
[28] Lianyungang Forum, "The 4th Lianyungang Forum Was Successfully Held."
[29] Lianyungang Forum, "The First Training Seminar on Law Enforcement Cooperation of the New Asia-Europe Continental Bridge Security Corridor," 2017, http://www.lygforum.gov.cn/index.php?m=news&a=details&content_id=318.
[30] Jacob Mardell, "The 'Community of Common Destiny' in Xi Jinping's New Era," accessed March 16, 2020, https://thediplomat.com/2017/10/the-community-of-common-destiny-in-xi-jinpings-new-era/.

of security destiny" can be understood as the security component of the "community of common destiny".

During the annual Forum, representatives from invited countries, including Ecuador, Fiji, Germany, Kazakhstan, Latvia, Poland, Tajikistan, and Uzbekistan, have been encouraged to attend the forum's security exhibition and view security products from companies such as Huawei, ZTE, Hikvision.[31] On the one hand, Chinese companies are trying to find new export markets in search of profit. On the other hand, foreign trade is 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 Figure 5). 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.[32] The Safety Corridor is currently planned to cover Kazakhstan, Russia, Belarus, Poland, Germany, and the Netherlands.[33]



[31] Lianyungang Forum, "Participating Countries and Organizations," accessed March 14, 2020, http://www.lygforum.gov.cn/index.php?m=countries&a=index&classify_id=209; Lianyungang Forum, "Focusing on 'Made in China' Weapons and Strong Police Prestige."
[32] "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.
[33] Ibid.

Figure 4: Illustrates the planned strategic Safety Corridor project.[34]

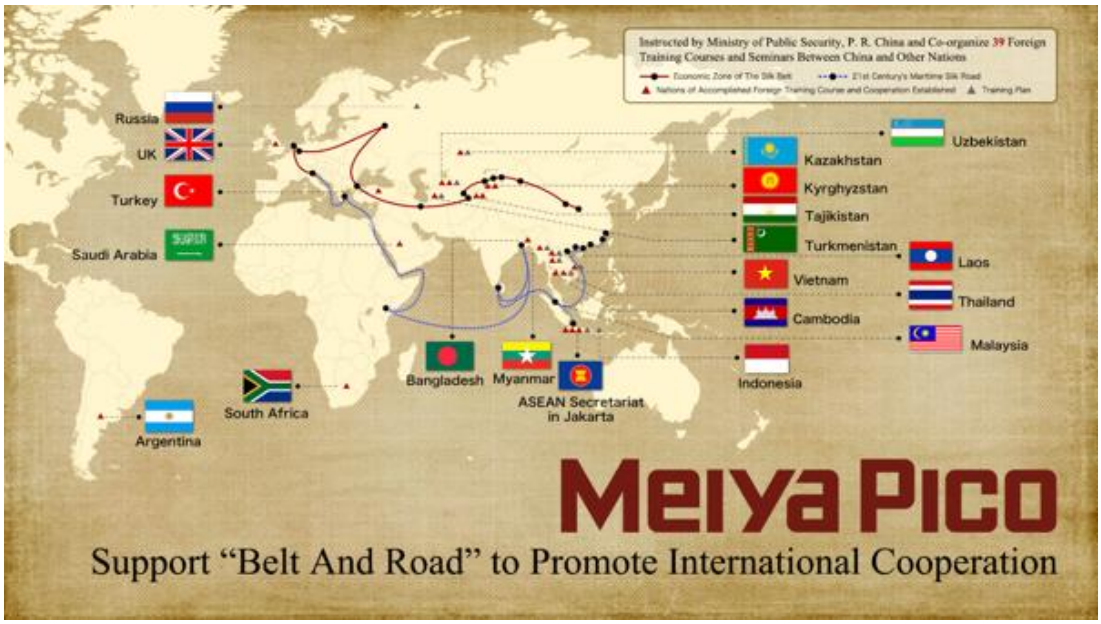


Figure 5: Meiya Pico was instructed by the Chinese Ministry of Public Security to train countries of the BRI in digital forensics.[35]

6.2.2. Understanding the demand side of diffusion

The ensuing sub-section of the thesis examines eight countries – all part of the BRI – where the internet sovereignty norm has diffused. The examined countries have one important common characteristic: they have all experienced large-scale protests shortly before emulating China's norm (advanced norm diffusion). The following lines show the causal effect of the IV2 (perception underlying import – regime survival concern) on the DV1.

Egypt

[34] Ibid.
[35] Meiya Pico, "Training," 2019, https://meiyapico.com/training/index.html.

In January 2011, mass protests erupted in Egypt.[36] In order to keep a lid on the protest movement, the government responded by disrupting the internet and mobile phone text messages, on 28 January.[37] The internet was unavailable until 2 February.[38] However, the protest movement was well underway and, even during the network shutdowns, hundreds of thousands of people went to the street.[39] On 11 February 2011, after the continuation of protests, Hosni Mubarak stepped down and the Supreme Council of the armed forces took over.[40] Then, democratic elections took place in 2012.[41] During the period of 2011 to 2013, the political environment was relatively free online and offline (flourishing of political parties, uncensored print media).[42] However, as president el-Sisi took power through a coup in the summer of 2013, the new government shifted to "controlling the narrative online."[43] They started blocking websites and blogs that had facilitated protests in 2011.[44] In that endeavour, Egypt also turned to China. In 2014, the two countries signed a "comprehensive strategic partnership agreement", which included cooperation on fighting cybercrime.[45] Both countries found strategic value in the agreement. While Egypt intended to deepen information control cooperation with like-minded Beijing, China saw el-Sisi as someone that will stay in power for a long time, unlike the Egyptian governments between 2011 and 2013, which lasted only a few months each.[46] Four years

[36] Al Jazeera, "Timeline: Egypt's Revolution," February 14, 2011, https://www.aljazeera.com/news/middleeast/2011/01/201112515334871490.html.
[37] Noam Cohen, "Egyptians Were Unplugged, and Uncowed," February 20, 2011, https://www.nytimes.com/2011/02/21/business/media/21link.html.
[38] Ibid.
[39] Al Jazeera, "Timeline."
[40] Ibid.
[41] Ibid.
[42] Interview on 26 March 2020 with Joey Shea, internet researcher and Egypt expert.
[43] Interview with Joey Shea.
[44] Interview with Joey Shea.
[45] 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?.
[46] Interview with Allison McManus on 8 April 2020, Non-Resident Fellow at the Tahrir Institute for Middle East Policy.

later, Egypt passed a cybercrime law for regulating social media that mimics China's way of handling "cybercrime."[47] Just like in China, provisions on what constitutes cybercrime, public morality, or national security are very vague and broad, which allows the government to censor content easily and punish political dissidents. During the parliamentary session when the law was passed, parliamentarian Bassam Feifel called for even more stringent measures and proclaimed that "Egypt must have its own Facebook just like China."[48] Egypt had tried to launch a Facebook-like platform but it did not find widespread appeal within the population because of technical glitches.[49] While Egypt's attempt was "influenced by China, certainly, Egypt lacks the technical capacity to have its own social media platform of this kind."[50] The closer cooperation in information controls between Egypt and China was accompanied by a considerable transfer of surveillance technology. Huawei built a safe city in the country and Hikvision supplied CCTV cameras for the Suez Governate's bus fleet.[51] Alongside these technology transfers, Egyptian journalists have visited Beijing for ten month-long media fellowships, organised by the China Public Diplomacy Association, a non-profit organisation with close ties to the Chinese authorities.[52] There, they were exposed to an authoritarian media

---

[47] 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/; Wafa Ben-Hassine, "Egyptian Parliament Approves Cybercrime Law Legalizing Blocking of Websites and Full Surveillance of Egyptians," *Access Now*, June 20, 2018, https://www.accessnow.org/egyptian-parliament-approves-cybercrime-law-legalizing-blocking-of-websites-and-full-surveillance-of-egyptians/; Government of Egypt, "2018 Cybercrime Law," May 1, 2018, https://www.youm7.com/story/2018/5/1/تعرف-على-كيفية-التصالح-فى-الجرائم-الإلكترونية-وفقا-للقانون-الجديد/3773230.

[48] Al-Youm, "Egyptian Parliament Approves Law to Combat Cybercrime."

[49] Interview with Joey Shea.

[50] Interview with Joey Shea.

[51] 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.

[52] China Public Diplomacy Association, "Executives," July 24, 2018, https://web.archive.org/web/20180724123348/http://www.chinapda.org.cn/eng/xhgk/cwls/.

landscape through visits to media houses like the People's Daily.[53] Egyptian officials, for their part, visited Meiya Pico to learn about digital forensics.[54] Clearly marked by the revolutionary shock of 2011 and with the help from China, Egypt has deteriorated from "partly free" (2011) to "not free" (2018) in Freedom House's online freedom ranking.[55]

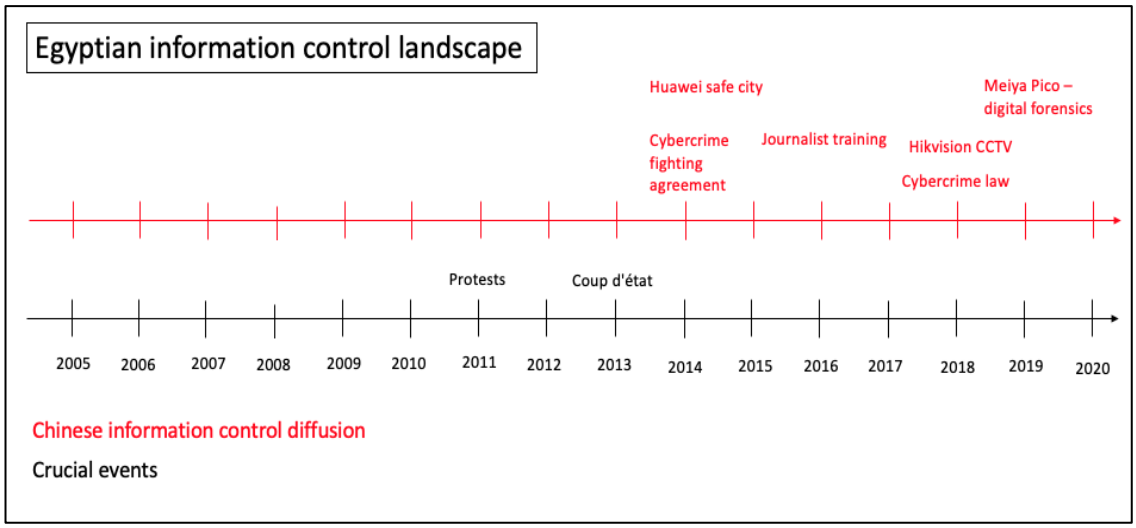


Figure 6: Egyptian information control landscape

Iran

Shortly before the Arab Spring, Iran experienced massive protests surrounding its 2009 presidential elections.[56] The government responded with a bloody crackdown. Most European surveillance companies pulled out, since they saw their equipment was openly used for nefarious purposes.[57] With growing isolation from the West, Iran increased its

[53] 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.
[54] 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.
[55] Freedom House, "Egypt," January 13, 2012, https://freedomhouse.org/report/freedom-net/2009/egypt.
[56] Human Rights Watch, "Iran: Violent Crackdown on Protesters Widens," *Human Rights Watch*, June 23, 2009, https://www.hrw.org/news/2009/06/23/iran-violent-crackdown-protesters-widens.
[57] 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.

political and economic relations with China. Chinese companies did not have similar human rights concerns and expanded their presence in Iran. One of the earliest surveillance equipment exports to Iran was Huawei's sale of gear that gives government agencies access to mobile phones, which occurred between 2009 and 2011.[58] In December 2010, ZTE, another Chinese company, also sold surveillance equipment to Iran that could be used to intercept citizens' communications.[59] However, despite the considerable technology transfer, protests erupted again in 2011 and 2012.[60] In order to prevent further uprisings, leaders deepened cooperation with China – Chinese technology needed to be complemented by Chinese techniques of information control. In a 2014 meeting between Chinese and Iranian state officials it was agreed that China would help Iran with the implementation of Iran's National Information Network.[61] 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.[62] And the head of Iran's Information Technology Organization lauded China for its "four

[58] Ibid.

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

[60] Thomas Erdbrink and Rick Gladstone, "Clashes and Protest Over Iran Currency Plunge Hit Tehran - The New York Times," October 3, 2012, https://www.nytimes.com/2012/10/04/world/middleeast/clashes-reported-in-tehran-as-riot-police-target-money-changers.html; Saeed Kamali Dehghan, "Iran Protests See Reinvigorated Activists Take to the Streets in Thousands," *The Guardian*, February 14, 2011, sec. World news, https://www.theguardian.com/world/2011/feb/14/iran-protests-reinvigorated-activists.

[61] Ministry of Communications and Information Technology of Iran, "مهندس جهانگرد در دیدار با مقام های چین' شورای اطلاعات China-Iran ICT Cooperation2014," تبادل :خبرداد, https://www.ict.gov.ir/fa/news/10162/-مهندس-جهانگرد-در-دیدار-با-مقام-های-شورای-اطلاعات-چین-خبرداد-تبادل-تجربیات-با-کشور-چین-در-حوزه-توسعه-ICT; 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/.

[62] 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.

decades of good experiences in the application development of services for information technology", and noted, "[w]e hope to use these experiences."[63]

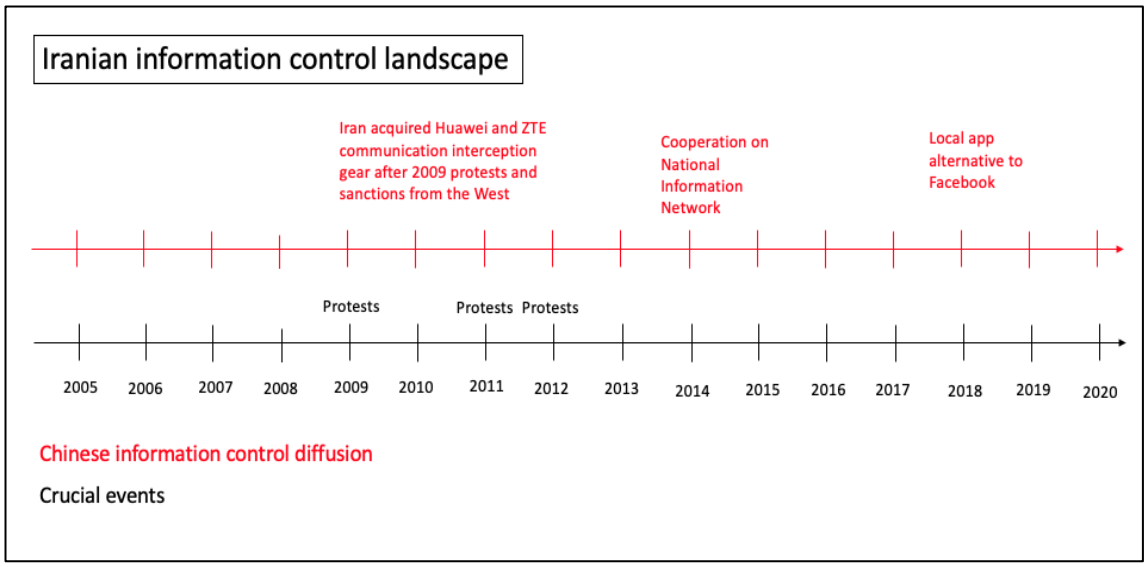


Figure 7: Iranian information control landscape

Tanzania

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 the years 2011, 2012, and 2013, Tanzania experienced major riots and protests.[64] Shortly after the political upheaval, collaboration with China was initiated. In 2014, Huawei announced that it had implemented a safe city in Tanzania.[65] The following year, Dahua Technology, a Hangzhou-based company, equipped the Zanzibar Presidential Office (note that Zanzibar is where Islamist riots

[63] Ministry of Communications and Information Technology of Iran, "مهندس جهانگرد در دیدار با مقام های شورای اطلاعات 'چین' China-Iran ICT Cooperationتبادل: خبرداد."

[64] BBC News, "Police Kill Tanzania Protesters," January 6, 2011, sec. Africa, https://www.bbc.com/news/world-africa-12126861; BBC News, "'Tanzanian Shot' in Gas Crackdown," May 24, 2013, sec. Africa, https://www.bbc.com/news/world-africa-22652809; Fumbuka Ng'wanakilala, "Zanzibar Islamists Burn Churches, Riot - Police," *Reuters*, May 27, 2012, https://www.reuters.com/article/zanzibar-protest-idUSL5E8GR1HB20120527.

[65] Cozzi, "Smart Cities: Envisioning a Sustainable Future."

occurred in 2012) with smart cameras that are capable of recognising faces and audio.[66] One year later, the People's Daily reported that Tanzanian journalists participated in a media fellowship programme organised by the China Public Diplomacy Association.[67] In turn, the exposure to Chinese information control technology and techniques has resulted in the Tanzanian government working to imitate the Chinese concept of censorship. In 2017, Tanzania's former Deputy Minister for Transport and Communication, Edwin Ngonyani, summed it up well. At a China-Tanzania New Media Roundtable, co-organised 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."[68]

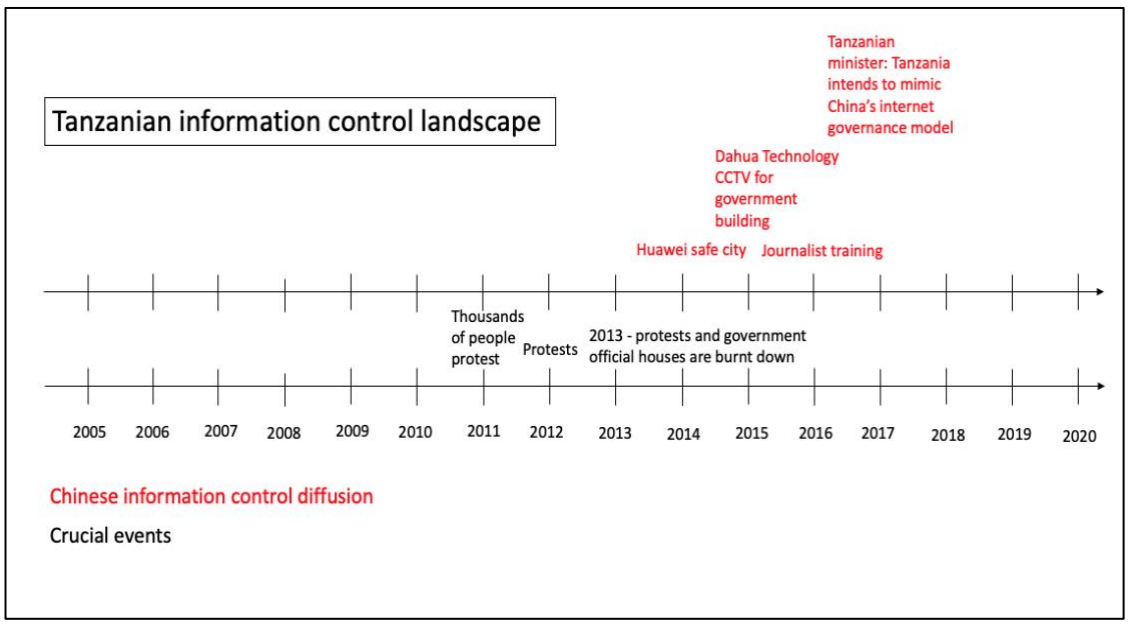


Figure 8: Tanzanian information control landscape

[66] Dahua Technology, "Dahua IP Megapixel Solution Secures Government Office in Tanzania," April 3, 2015, https://www.dahuasecurity.com/newsEvents/successStories/51/30.
[67] Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
[68] Interview with Daniel Mwesigwa (Ugandan internet researcher) on 20 March 2020; Banzi, "Tanzania."

Thailand

From March to May 2010, Thailand experienced the most brutal showdown between government forces and citizens since the 1992 uprising against the military dictatorship. 2,000 people were wounded and 90 died.[69] Only one month later, in June 2010, Hikvision took on the task of providing CCTV monitoring for the Thai Ministry of Commerce.[70] Then, in 2012, Hikvison supplied Thai police with portable video recorders, which help with real-time recording and remote monitoring.[71] Despite surveillance technology provided by Chinese companies, large-scale protests shook Thailand again in 2013-14. The protests ended in prime minister Yingluck Shinawatra being ousted and replaced by a military junta.[72] While the Shinawatra government bought technology from China, they did not engage in emulation. The new military leaders, however, decided that more drastic measures had to be put in place to prevent further unrest. Former Thai Foreign Minister Kasit Piromya stated in an interview that concerns as regards to cybersecurity were present for a long time in Thailand's conservative government/bureaucracy, but the feeling has intensified under General Prayut [who has been in power since 2014].[73]

[69] Human Rights Watch, "Descent into Chaos | Thailand's 2010 Red Shirt Protests and the Government Crackdown," *Human Rights Watch*, May 3, 2011, https://www.hrw.org/report/2011/05/03/descent-chaos/thailands-2010-red-shirt-protests-and-government-crackdown.

[70] Hikvision, "Hikvision Protects Ministry of Commerce (MOC) Thailand," June 24, 2010, https://webcache.googleusercontent.com/search?q=cache:QlraCG2ayrkJ:https://www.hikvision.com/europe/News--Events/Success-Stories/Government/305528969213861+&cd=1&hl=en&ct=clnk&gl=uk.

[71] Hikvision, "Hikvision Helping Bangkok's Police Force Stay Ahead of the Curve-Hikvision," July 11, 2012, https://webcache.googleusercontent.com/search?q=cache:05fh0kJfhrIJ:https://www.hikvision.com/uk/Press/Success-Stories/Government/305528970582113+&cd=1&hl=en&ct=clnk&gl=uk.

[72] BBC News, "Thai Military Seizes Power in Coup," May 22, 2014, sec. Asia, https://www.bbc.com/news/world-asia-27517591.

[73] Interview with Kasit Piromya on 25 June 2020, Thai Minister of Foreign Affairs from 2008-11; Member of the House of Representatives until the coup d'état of 2014.

In 2015, the prime minister's military junta ordered various government agencies to create Thailand's own Great Firewall in the image of China's.[74] 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, and allowing for invasive government on-site inspections at companies and individuals' properties in Thailand.[75] The Thai government has also been inspired by China's deployment of information controls in the Xinjiang province – Thai authorities started to collect DNA data and facial identification of its citizens without informing them how it will be used.[76] Akin to Xinjiang in China, which is a testbed for security policies that are later rolled out throughout the country, Thai political leaders see the deep south of Thailand as such a test bed for more stringent cybersecurity policies.[77] Further technology and technique transfer also took place from China. Starting in 2017, in cooperation with the Thai police, Huawei has been implementing its eLTE [Long-Term Evolution] Trunking Joint Innovation Project surveillance solution.[78] 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.[79] In short,

---

[74] Thai Government Public Relations Department, "Prime Minister's Orders," September 4, 2015, https://pr.prd.go.th/chaiyaphum/ewt_news.php?nid=9060.

[75] 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/; Thai Ministry of Digital Economy and Society, "Cybersecurity Act," 2019, https://www.mdes.go.th/law/detail/1904-Cybersecurity-Act--B-E--2562--2019-.

[76] Interview with Ida on 29 June 2020, former Thai parliamentarian.

[77] Interview with Ida.

[78] Allows the police to communicate more effectively within the smart city framework. 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.

[79] Meiya Pico, "Training"; 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.

Thailand is a crucial case to empirically illustrate this thesis' causal mechanisms. In the early 2010s, Thailand was a flawed democracy. As such, it bought information control technology from China. But only after serious protest movements and a regime change in 2014 did Thailand engage in imitation, which showcases norm diffusion.

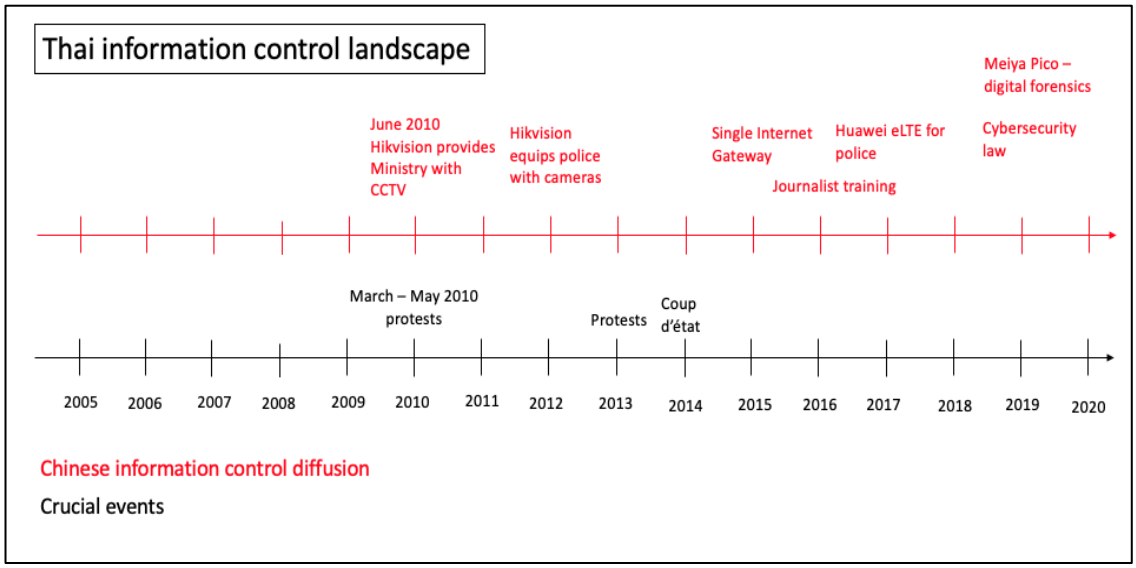


Figure 9: Thai information control landscape

Uganda

China's influence on Ugandan information control strategies has become apparent after major protests shook the country in the mid 2010s. In 2016, severe unrest took place in Uganda. On 16 February 2016, clashes between police forces and supporters of the opposition ended deadly.[80] The government responded with the crude method of social media shutdown, which affected platforms such as Facebook, Twitter, and WhatsApp for 24 hours on 18 February.[81] Uganda sought for help in China and its pleas were heard.

[80] Tendai Marima, "Violence Erupts Days Ahead of Uganda Elections," February 16, 2016, https://www.aljazeera.com/news/2016/02/uganda-opposition-leader-arrested-days-elections-160215132155444.html.
[81] Nshira Turkson, "A Social-Media Shutdown in Uganda's Presidential Election," *The Atlantic*, February 18, 2016, https://www.theatlantic.com/international/archive/2016/02/uganda-election-social-media-shutdown/463407/.

That same year, Ugandan journalists completed a ten-month-long propaganda training at the China Africa Press Center in Beijing, organised by the China Public Diplomacy Association.[82] 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.[83] "Cybercrime in this case is…widening the government's powers to surveil…[while at the same time] less focus is put on protecting users from cybercrime."[84] The following year, Huawei delivered surveillance cameras to facilitate the Ugandan government's safe policing programme.[85] President Museveni mentioned that he is using these cameras to enforce social distancing lockdown measures during the coronavirus pandemic: "I have my eyes now, all around Uganda."[86] The Shenzhen-based company also assisted the government with gaining access to the encrypted communications of opposition figures.[87] In June 2019, the Uganda Communications Commission revealed a draft internet regulation. The measure is intended to centralise control over the international information flows that enter and exit the country.[88] 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

[82] Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
[83] 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.
[84] Interview with Daniel Mwesigwa.
[85] Interviews with Neil Blazevic on 8 April 2020, Technology Advisor at DefendDefenders, a Ugandan human rights organisation; and Daniel Mwesigwa; Tom Wilson and Madhumita Murgia, "Uganda Confirms Use of Huawei Facial Recognition Cameras," August 20, 2019, https://www.ft.com/content/e20580de-c35f-11e9-a8e9-296ca66511c9.
[86] Interview with Neil Blazevic.
[87] Interview with Daniel Mwesigwa; Parkinson, Bariyo, and Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents."
[88]Interview with Daniel Mwesigwa.

it is centrally controlled and you can put one system at the centre of it all to control everything."[89] Daniel Mwesigwa, a Ugandan internet researcher, states that this is a "useful analogy. It shows the [Ugandan] government's stance towards internet governance. We [Uganda] are increasingly looking East to get inspiration."[90]

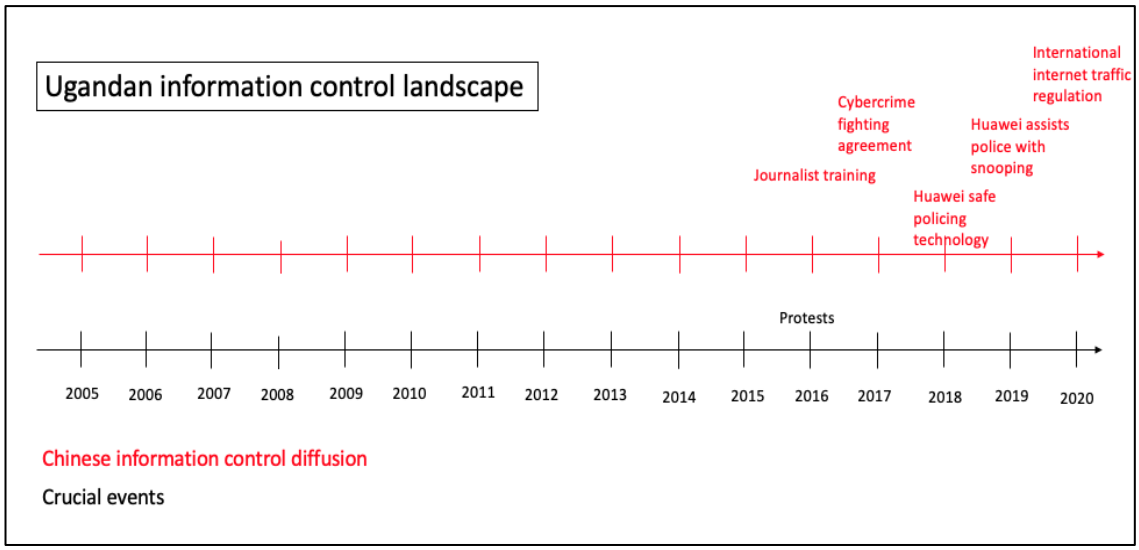


Figure 10: Ugandan information control landscape

Vietnam

In 2015, rare protests occurred in Vietnam. In April, thousands of workers in Ho Chi Minh City protested in the streets against the government's insurance law that was going into effect soon.[91] On 1, 8, and 15 May, people took to the streets in multiple Vietnamese cities and asked the government to investigate the mass fish deaths surrounding the coast of Vietnam.[92] The government cracked down on the environmental activists and blocked

[89] 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/.
[90] Interview with Daniel Mwesigwa.
[91] BBC News, "Thousands on Strike in Vietnam Over Insurance Law," April 1, 2015, sec. Asia, https://www.bbc.com/news/world-asia-32142635.
[92] Human Rights Watch, "Vietnam: Crackdown on Peaceful Environmental Protesters," May 18, 2016, https://www.hrw.org/news/2016/05/19/vietnam-crackdown-peaceful-environmental-protesters.

Facebook temporarily.[93] On 5 November 2015, activists gathered in Hanoi and Ho Chi Minh City to protest Chinese president Xi Jinping's visit to Vietnam and China's claims in the South China Sea.[94] The protesters were beaten by the police.[95]

Following these challenges against the regime, Vietnam mimicked provisions from China's 2017 cybersecurity law, which has been effective as of 1 June 2017.[96] Only a few days later, first drafts of a Vietnamese Cybersecurity Law were sent from Vietnam's Ministry of Public Security to the Vietnamese authorities.[97] Vietnamese political entities said that they were influenced by cybersecurity laws from several countries, including one from China.[98] Trinh Huu Long, a Vietnamese democracy activist, lists several overlaps between the Chinese and Vietnamese laws.[99] Both use the term "critical information system regarding national security". The Chinese and Vietnamese provisions both identify that any information endangering the ruling elite will not be tolerated. Furthermore, just like China, Vietnam now requires real-name registration for its internet users and demands domestic and international companies to localise data pertaining to Vietnamese users within Vietnam.

---

[93] Ibid.; Sarah Perez, "Facebook Blocked in Vietnam Over the Weekend Due to Citizen Protests," *TechCrunch*, May 17, 2016, https://social.techcrunch.com/2016/05/17/facebook-blocked-in-vietnam-over-the-weekend-due-to-citizen-protests/.

[94] Radio Free Asia, "Vietnamese Authorities Crack Down on Rare Protests Targeting Xi Visit," accessed January 6, 2021, https://www.rfa.org/english/news/vietnam/protests-11052015153610.html.

[95] Ibid.

[96] Rogier Creemers, Paul Triolo, and Graham Webster, "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," *New America*, June 29, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

[97] Long, "Vietnam's Cybersecurity Draft Law"; Government of Vietnam, "Cybersecurity Law," June 12, 2018, http://tulieuvankien.dangcongsan.vn/he-thong-van-ban/van-ban-quy-pham-phap-luat/luat-an-ninh-mang-so-242018qh14-ngay-1262018-hieu-luc-thi-hanh-tu-ngay-01012019-4474.

[98] Long, "Vietnam's Cybersecurity Draft Law."

[99] Ibid.

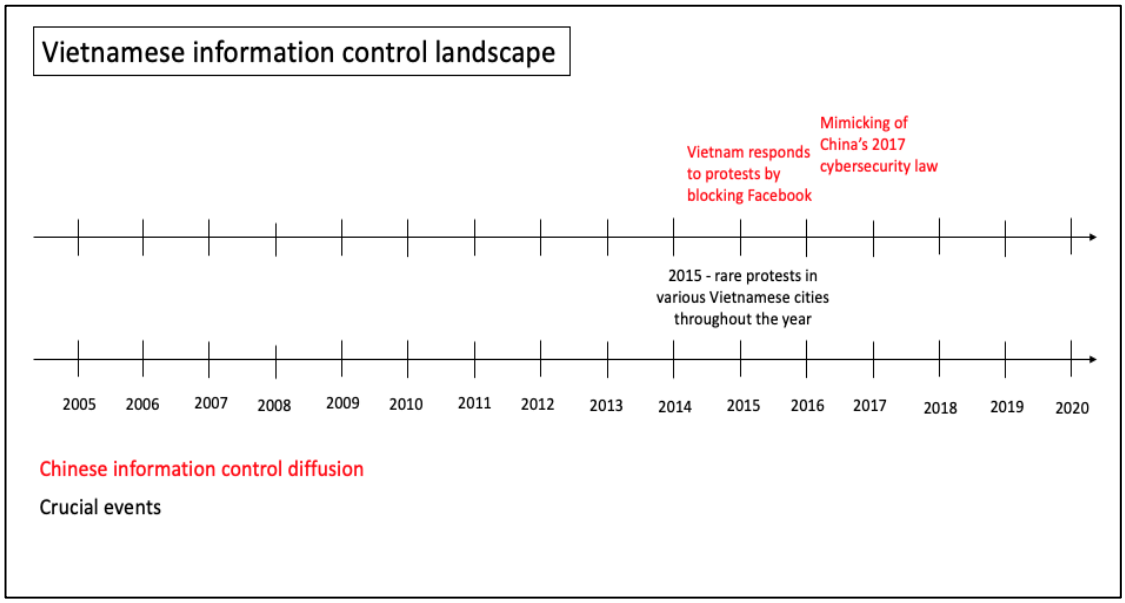


Figure 11: Vietnamese information control landscape

Zambia

The social unrest in the early 2010s explains partially why Zambia sought assistance from China and started to adopt its norm. In September 2011 and November 2014, major anti-government riots took place in the country.[100] Only a few months later, in 2015, Zambian president Edgar Lungu travelled to Beijing to finalise a $440 million project that would establish an information and communication trainings hub in Zambia.[101] It turned out that this training centre housed Huawei employees that allegedly aided the Zambian government intercept the digital communications of journalists and opposition groups.[102] Huawei also implemented a smart city to increase Zambia's physical surveillance

[100] France 24, "Riots Erupt Amid Claims of Vote-Rigging," September 22, 2011, 24, https://www.france24.com/en/20110922-zambia-presidential-election-rupiah-banda-michael-sata-riots-erupt-rumours-vote-rigging; Robyn Dixon, "After Rioting, Zambia's Acting President Reinstates Official," *Los Angeles Times*, November 4, 2014, https://www.latimes.com/world/africa/la-fg-riots-zambia-20141104-story.html.

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

[102] Ibid; Interview with Kuda Hove (Zimbabwean internet researcher at Privacy International focussing on Sub-Saharan Africa) on 10 April 2020.

capabilities.[103] In addition, the media landscape of the country has been influenced by Zambian journalists who have attended propaganda trainings during 2016 in China.[104] In the words of a Zambian minister, voiced in December 2018, Zambia is now following "the China way" of managing the internet.[105]

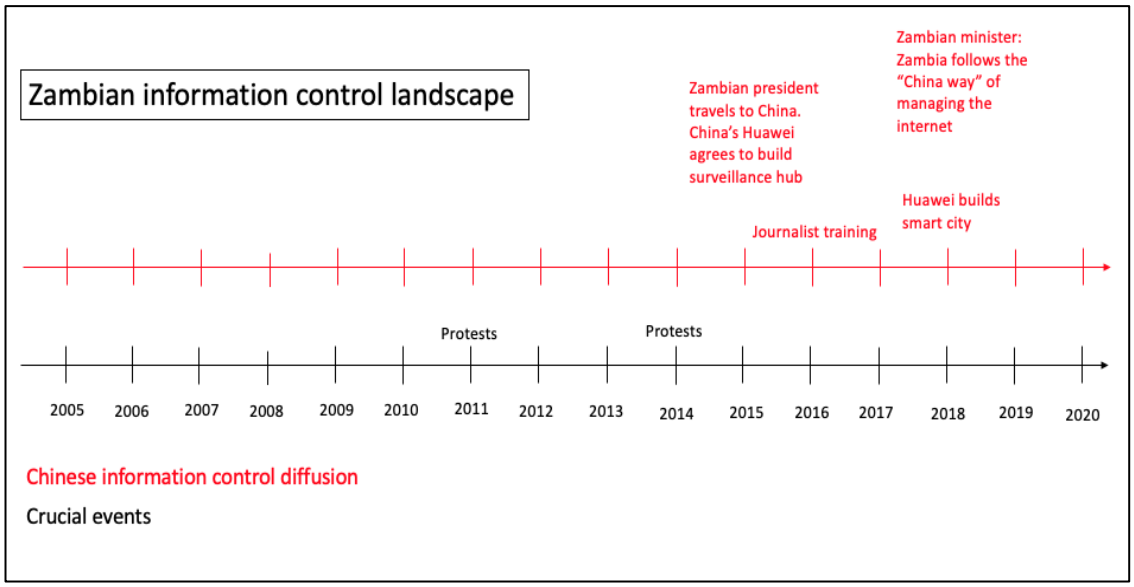


Figure 12: Zambian information control landscape

Zimbabwe

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.[106] These instances were some of the first examples of China exporting censorship technology, which China has refined since then.

[103] Huawei, "Huawei Smart City Overview Presentation," *Huawei Enterprise*, 2018, https://e.huawei.com/en/material/onLineView?MaterialID=02ad4d5ab608492ea24659ec667f04bd.
[104] Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
[105] 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.
[106] 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.

2007 was another milestone in Zimbabwean information control history. During this year, the economy was deteriorating at a fast pace.[107] The ruling ZANU-PF party passed the Interception of Communications Act.[108] According to a former Zimbabwean government official it was done as a response to the growing effectiveness of social media:

"This has been a country that has had for 60 years its public media tightly controlled by the government to the day both during Rhodesian times and since 1985… We only have one television station in the country and it's very tightly controlled by government and there is not a single independent radio station. And so social media was a major problem for ZANU-PF, because it allowed civilians to disseminate and receive information without constriction and it was their response to try clamp down on that."[109]

Then, the 2010 Arab Spring was consequential for Zimbabwean information control policies.[110] In February 2011, Zimbabwean police voiced that it was afraid of Egypt-style protests and arrested dozens of people who watched ongoing protests in Egypt.[111] Senator Coltart recalls:

"Between 2009 and 2013 … Mugabe and ZANU-PF controlled the coercive ministries and still were very intent on keeping a lid on any possible uprising, so yes there was deep concern about what had happened in Egypt and a concern that that might spill over and give people ideas."[112]

Since 2011, Zimbabwean journalists have been trained in Chinese information dissemination techniques in order to learn how to steer conversations and manage media

[107] Michael Wines, "As Inflation Soars, Zimbabwe Economy Plunges," *The New York Times*, February 7, 2007, https://www.nytimes.com/2007/02/07/world/africa/07zimbabwe.html.
[108] Government of Zimbabwe, "Interception of Communications Act [Chapter 11:20]," *Veritaszim*, 2007, http://www.veritaszim.net/node/252.
[109] Interview with Senator David Coltart on 22 May 2020, Member of Parliament in Zimbabwe's National Assembly from 2000-2008; since 2008 a Member of the Senate; Minister of Education, Sport, and Culture from February 2009 – August 2013.
[110] Interview with Kuda Hove.
[111] Cris Chinaka, "Zimbabwe Tense Over Anti-Mugabe Protests Call," *Reuters*, March 1, 2011, https://www.reuters.com/article/ozatp-zimbabwe-protests-20110301-idAFJOE7200B320110301.
[112] Interview with Senator David Coltart.

in an authoritarian environment.[113] In 2016 again, Zimbabweans protested against the dismal economic situation in the country and used social media platforms to organise themselves.[114] At that point, Zimbabwean leaders "became really aware of the internet's power to … spread freedom in the country… and that the internet was essential to their survival" and, as a consequence, responded by shutting down large parts of the internet.[115] The shocks of the 2010-12 Arab Spring, just as well as the more recent Ukrainian Revolution (2014) and the Umbrella protests in Hong Kong (2014) still reverberated in Zimbabwean leaders' perceptions.[116]

"[The concern] was far more heightened post the unity government [post 2013]. In recent years, we have now the cybersecurity bill that is going through with much increased powers of surveillance and the like. And I think it's in response not just to Egypt but what's been [happening in] Sudan, and even Hong Kong, you know the regime understands the importance of social media and of course in January last year [2019] you may recall that they shut down the internet completely at the height of these demonstrations."[117]

Member of Parliament Prince Sibanda confirms Senator Coltart's statement:

"The current government wants to remain in power in perpetuity… The potential of social media [that gives] citizens the capacity to organise themselves against the government that is the major fear that they have."[118]

---

[113] 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.

[114] Max Bearak, "'Shut Down Zimbabwe' Protests Are Met With Internet Blackouts and Arrests," *Washington Post*, July 6, 2016, https://www.washingtonpost.com/news/worldviews/wp/2016/07/06/shut-down-zimbabwe-protests-are-met-with-internet-blackouts-and-arrests/.

[115] Interview with Arthur Gwagwa on 28 March 2020, Zimbabwean internet researcher.

[116] Interview with Arthur Gwagwa.

[117] Interview with Senator David Coltart.

[118] Interview with Prince Sibanda on 17 June 2020, Member of Parliament since 2013 and is the Chairperson of the Parliamentary Portfolio Committee on Information Media and Broadcasting Service in the Zimbabwean National Assembly. In this role he oversees, monitors, and scrutinises Zimbabwe's Ministry of Information, Media and Publicity. He is a Member of the largest opposition party, the Movement for Democratic Change Alliance.

President Robert Mugabe responded to renewed protests that occurred first on 14 April 2016 and continued throughout the year by saying that there would be no "Arab Spring" in Zimbabwe.[119] He would prevent another Arab Spring by imitating China. In 2016, it was reported that Zimbabwe was developing local app equivalents of social media platforms in order to enhance control (an approach championed by China).[120] However, it lacks the technical capabilities for developing such apps.[121] 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."[122]

Senator Coltart responded to Supa Mandiwanzira's statement by maintaining:

"[T]hat [it] was an expression of desire rather than something that they [can] carry through. They don't have the capacity to do that and there has been no further development. My interpretation of this government and the former government under Mugabe is that they would love to have a Chinese situation [where] Facebook and Twitter are sealed off and banned and there are local alternatives that are tightly controlled by government, but this particular horse has already bolted in Zimbabwe. It will be very difficult for any government to now try to crack down on Facebook and Twitter. They are widespread and particularly [amongst] people in the young generation and having allowed people to lose those social media platforms will be very difficult to shut them down and they literally don't have the capacity to replace them with anything that would be used by the public."[123]

---

[119] MacDonald Dzirutwe, "No 'Arab Spring' in Zimbabwe, Mugabe Warns Protesters," *Reuters*, August 26, 2016, https://www.reuters.com/article/us-zimbabwe-protest-idUSKCN1110Q6; Associated Press in Harare, "Thousands March in Harare in Rare Mass Protest Against Robert Mugabe," *The Guardian*, April 14, 2016, http://www.theguardian.com/world/2016/apr/14/thousands-march-harare-rare-mass-protest-against-robert-mugabe.

[120] Lincoln Towindo, "Government to Regulate Social Media," April 10, 2016, http://www.sundaymail.co.zw/social-media-regulation-is-nigh/.

[121] Interview with Arthur Gwagwa.

[122] Towindo, "Government to Regulate Social Media."

[123] Interview with Senator David Coltart.

Kuda Hove, for his part, mentions that:

"[I]n 2017, one of president Mugabe's last acts was to set up a Cyber Security Ministry … and the presidential spokesperson said that the Zimbabwean government had in that particular instance looked up the model used in China...as an inspiration."[124]

Recent governments have indeed tried to:

"[E]nforce a Chinese style of governance in the country and particularly with regard to cyber security, but it's a very inefficient government and so I think that they will find it exceptionally difficult…China is a massive country, huge population, very powerful and efficient government, which the ZANU-PF government simply isn't."[125]

In 2018, Zimbabwe's government doubled down on technological cooperation with China. Zimbabwe's Nations Hardware and Electrical partnered with Hangzhou-based Hikvision to implement broader CCTV coverage in the country.[126] Government officials claim that "these cameras are for traffic enforcement, but when you look at them, they are not only for traffic control. The bottom part of it is for traffic", but the upper part may be used for other surveillance purposes.[127] Despite the technique and technology transfer from China, Zimbabwe has had difficulties to implement the model on its territory. This is also because it is surrounded by liberal countries.

"We are surrounded by South Africa and Botswana which has a relatively liberal environment and there is a lot of interaction between people in Zimbabwe and Botswana and South Africa and so because of that environment it will be very difficult for the government to impose its will in this regard in that way it stands in marked contrast with China."[128]

---

[124] Interview with Kuda Hove.
[125] Interview with Senator David Coltart.
[126] Interview with Kuda Hove; Hongpei Zhang, "Chinese Facial ID Tech to Land in Africa," *Global Times*, May 17, 2018, http://www.globaltimes.cn/content/1102797.shtml.
[127] Interview with Arthur Gwagwa.
[128] Interview with Senator David Coltart.

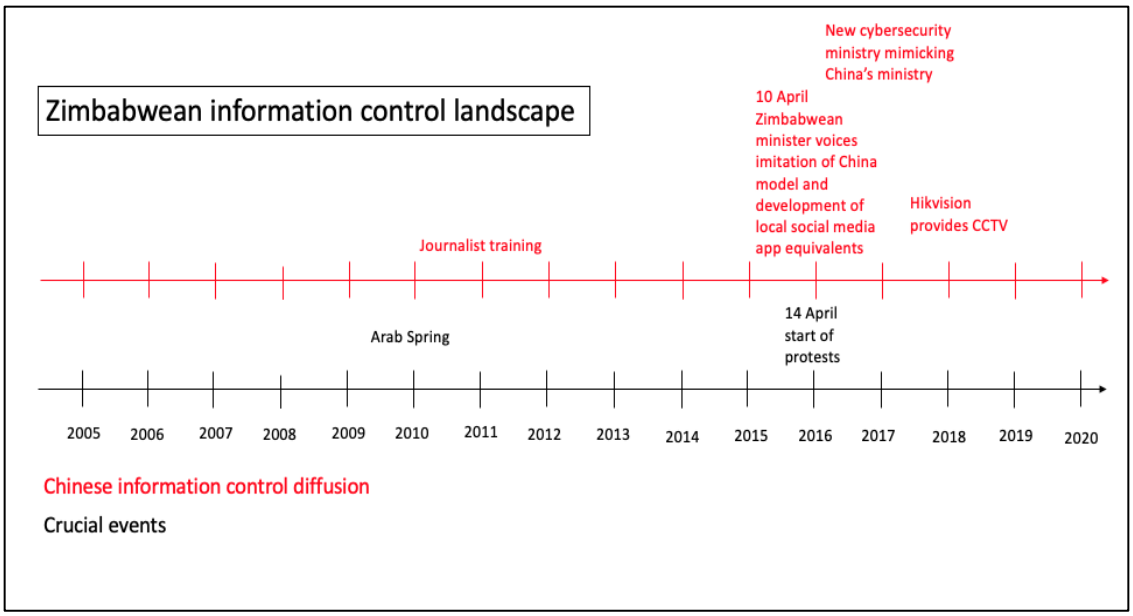


Figure 13: Zimbabwean information control landscape

6.3. Variation in the dependent variable

This section of the chapter is looking at certain countries that I would have, in theory, expected diffusion to occur but where, in practice, no technology/technique transfer has occurred. In particular, it is exploring the cases of Syria and Bahrain, as well as Nicaragua. A variation in the dependent variable means here that China's norm did not diffuse to those countries, as opposed to the above examined countries, such as, Egypt and Iran, where the Chinese norm diffused.

All the countries analysed below (Syria, Bahrain, and Nicaragua) have high regime survival concerns and, in addition to this, are countries where China seeks influence – Syria and Bahrain because they are located on the BRI trade routes, and Nicaragua because it is a Taiwan ally. With regards to the latter two countries, China has been

seeking influence in Nicaragua and the Gambia, because it wants to discourage them from being Taiwan allies.[129]

Syria

Why has the Chinese norm not diffused to Syria, a seemingly obvious place for it to take root? Syria would have had more than enough reasons to import technology from China. Its leader Bashar al-Assad has been cracking down on civil liberties at least since 2001 and ruled through emergency rule for the next decade.[130] Then, in March 2011, first Arab Spring protests erupted in the country, starting a serious and enduring challenge to the regime of president al-Assad.[131] During his years in power, al-Assad relied strongly on Western surveillance providers to keep track of dissent in the country. This long-held surveillance relationship with Western providers made it unnecessary to import gear or techniques from China. Already starting in 2004, German companies Ultimaco and Siemens provided interception management systems in what was a million-dollar deal with the Syrian government.[132] In 2007, engineers of RCS (an Italian company) travelled to Syria to prepare the monitoring of real-time Syrian targets. However, despite their efforts, Italian competitor AREA outdid RCS in their bid and won the bid for the project.[133] In 2009, however, RCS managed to win a contract to surveil communications that went through Syrian satellite providers (this type of communications is used predominantly in more rural Syrian areas).[134] Another company, South African

[129] Ben Blanchard Wu J. R., "With Gambia Move, China Ends Diplomatic Truce With Taiwan," *Reuters*, March 17, 2016, https://www.reuters.com/article/us-china-gambia-idUSKCN0WJ1DT.
[130] BBC News, "Syrian President Bashar Al-Assad: Facing Down Rebellion," August 31, 2020, sec. Middle East, https://www.bbc.com/news/10338256.
[131] Mona Yacoubian, "Syria Timeline: Since the Uprising Against Assad," United States Institute of Peace, accessed December 14, 2020, https://www.usip.org/syria-timeline-uprising-against-assad.
[132] Privacy International, "Open Season: Building Syria's Surveillance State," December 12, 2016, http://privacyinternational.org/report/1016/open-season-building-syrias-surveillance-state.
[133] Ibid.
[134] Ibid.

VASTech, has provided surveillance gear to Syria since 2002.[135] In June 2009, the company responded to a call by the Syrian government to build interception capabilities for the Damascus and Aleppo international exchanges, through which all traffic in and out of Syria was flowing.[136] Then, in 2011, it was revealed that the Syrian government also used US-based Blue Coat System's censorship equipment to monitor its citizens.[137] In 2015, it was reported that al-Assad used British-based Gamma Group to spy on the Syrian population.[138]

Bahrain

Another case where no diffusion of Chinese technology occurred, even though my hypothesis would have expected it, is authoritarian Bahrain. In February 2011, Bahrain experienced a large-scale uprising of the Shia majority population against the minority Sunni-led government.[139] Protesters gathered in the capital's (Manama) roundabout.[140] The Bahraini king declared a state of emergency and brought in 2,000 troops from Sunni-majority populated Saudi Arabia and the United Arab Emirates.[141] 30 civilians died, and 3,000 people were arrested as a consequence.[142]

---

[135] Ibid.
[136] Ibid.
[137] Dave Maass and Cindy Cohn, "A Warning to Know Your Customer: Computerlinks Fined for Dealing Blue Coat Surveillance Technology to Syria," *Electronic Frontier Foundation*, May 28, 2013, https://www.eff.org/deeplinks/2013/05/blue-coat-syria-scandal-next-shoe-drops-computerlinks-fzco.
[138] Nick Hopkins and Jake Morris, "UK Firm's Surveillance Kit 'Used to Crush Uganda Opposition,'" *BBC News*, October 15, 2015, sec. UK, https://www.bbc.com/news/uk-34529237.
[139] BBC News, "Arab Uprising: Country by Country - Bahrain," December 16, 2013, //www.bbc.co.uk/news/world-12482295.
[140] Ibid.
[141] Ethan Bronner and Michael Slackman, "Saudi Troops Enter Bahrain to Help Put Down Unrest," *The New York Times*, March 14, 2011, https://www.nytimes.com/2011/03/15/world/middleeast/15bahrain.html.
[142] BBC News, "Arab Uprising."

Bahrain relied on Saudi Arabia and the United Arab Emirates for maintaining regime stability in 2011. However, Western countries had their fair share too in security provisions to Bahrain. Bahrain hosts, for instance, the US Navy's Fifth Fleet, the US Naval Forces Central Command, the Combined Maritime Force, and the US Marine Central Command.[143] In addition, the US has sold military equipment worth billions of dollars to Bahrain.[144] Similarly, large military equipment sales were provided by the UK, and other European countries to Bahrain.[145]

Perhaps this long-standing "offline" security relation made Bahrain rely on Western technology companies to preserve stability "online" too and may explain why Bahrain did not have to rely on China. It already had working alternatives and partners that would help it to stay in power.

In the year following the 2011 uprising, Bahrain asked UK-based Gamma Group for support relating to Gamma Group products at least five times.[146] In the letters exchanged between Gamma Group and Bahrain, a list of 77 surveillance targets was exchanged.[147] The company's software was used to spy on Bahraini dissidents in the UK.[148] Italian Hacking Team's software, which can infect target devices remotely, record conversations

[143] Joe Gould, "US Senate Upholds Arms Sales to Bahrain, Qatar," *Defense News*, June 13, 2019, https://www.defensenews.com/congress/2019/06/13/us-senate-upholds-arms-sales-to-bahrain-qatar/.
[144] Reuters Staff, "State Department OKs Nearly $6 Billion in Weapons Sales to Gulf Allies," *Reuters*, May 3, 2019, https://www.reuters.com/article/us-usa-defense-arms-idUSKCN1S924P.
[145] Action on Armed Violence, "UK Arms Exports to Bahrain," November 29, 2018, https://aoav.org.uk/2018/uk-arms-exports-to-bahrain/; Central Intelligence Agency, "Middle East: Bahrain — The World Factbook," 2020, https://www.cia.gov/library/publications/the-world-factbook/geos/ba.html.
[146] David Pegg, "Bahraini Arab Spring Dissidents Sue UK Spyware Maker," *The Guardian*, October 11, 2018, sec. World news, https://www.theguardian.com/world/2018/oct/11/bahraini-arab-spring-dissidents-sue-uk-spyware-maker.
[147] Ibid.
[148] Privacy International, "Bahraini Government, With Help From FinFisher, Tracks Activists Living In The United Kingdom," accessed December 15, 2020, http://privacyinternational.org/blog/1231/bahraini-government-help-finfisher-tracks-activists-living-united-kingdom.

and take photos, as well as allows access to emails, has been sold to Bahrain at least since 2011.[149] Yet another spyware, Pegasus, produced by the Israeli company NSO Group, was also found to be used in Bahrain in 2018. Once installed without the knowledge of the user, Pegasus can be used to exfiltrate passwords, calendar events, contact lists, and real-time voice calls from mainstream messaging applications.[150]

In addition to Syria and Bahrain, this thesis would have assumed diffusion from China to Taiwan allies, since China seeks to poach them from Taiwan. Why then, do all 15 countries, even authoritarian-leaning ones (Nicaragua), that recognise Taiwan, have no information control interaction with China?[151]

It might be that China has no incentive to supply technology and techniques to Taiwan allies. This is because China might only have an incentive to help these countries once they switch over to its side, renouncing their relationship with Taiwan. If it helped them while being allies of Taiwan, they would have no reason to cut all diplomatic ties with Taiwan. In other words, China seeks influence in these countries by withholding economic and political cooperation until those countries renounce Taiwan as an ally. At the same time, Taiwan allies do rationally calculate the cost of not cooperating with

[149] Cora Currier and Morgan Marquis-Boire, "A Detailed Look at Hacking Team's Emails About Its Repressive Clients," *The Intercept*, July 7, 2015, https://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/.

[150] Marczak et al., "HIDE AND SEEK."

[151] Those are: Marshall Islands, Republic of Nauru, Palau, Tuvalu, Eswatini, Holy See, Belize, Republic of Guatemala, Haiti, Republic of Honduras, Nicaragua, Republic of Paraguay, St. Kitts and Nevis, Saint Lucia, St. Vincent & the Grenadines. Ministry of Foreign Affairs, Republic of China, "Diplomatic Allies," *(Taiwan) 中華民國外交部 - 全球資訊網英文網*, accessed March 13, 2020, https%3a%2f%2fwww.mofa.gov.tw%2fen%2fAlliesIndex.aspx%3fn%3dDF6F8F246049F8D6%26sms%3dA76B7230ADF29736.

China.[152] China and Paraguay, for instance, do not have any economic, political or information control interaction. In contrast, the regional annual average value for other countries of interacting with China amounts to 1 percent of their GDP between 2005 and 2014.[153] Taiwan offered Paraguay only around US$20 million in benefits per year.[154] According to an article by Long and Urdinez, Paraguay foregoes Chinese monetary incentives, which would largely exceed the US$20 million given by Taiwan, because it prefers the attention given to it by Taiwan and because it appreciates Taiwan's recognition of Paraguay as an important country.[155]

One might interject and say that Paraguay is a democratic country, which may have less interest in importing surveillance technology from China than an authoritarian-leaning country. Therefore, it might be helpful to look at an authoritarian Taiwan ally – Nicaragua.

Nicaragua

Daniel Ortega has ruled Nicaragua since 2007 and continuously moved to concentrate powers in his hands.[156] He has, for instance, amended the constitution to allow him to re-stand for election as many times as he wishes.[157] Since entering office, he has been challenged by massive anti-government protests in 2014, 2015, 2018, and 2020.[158] In

[152] Tom Long and Francisco Urdinez, "Status at the Margins: Why Paraguay Recognizes Taiwan and Shuns China," *Foreign Policy Analysis*, 2020, https://academic.oup.com/fpa/advance-article-abstract/doi/10.1093/fpa/oraa002/5825378?redirectedFrom=fulltext.
[153] Ibid.
[154] Ibid.
[155] Ibid.
[156] El País, "Nicaragua's Daniel Ortega Shows His True Colors," August 8, 2016, https://english.elpais.com/elpais/2016/08/08/inenglish/1470656537_002840.html.
[157] Ibid.
[158] BBC News, "Nicaraguans Protest Against Canal Plans," December 10, 2014, sec. Latin America & Caribbean, https://www.bbc.com/news/world-latin-america-30426100; BBC News, "Nicaragua Canal Protest: Thousands Oppose Atlantic-Pacific Plan," June 14, 2015, sec. Latin America & Caribbean,

2014 and 2015, thousands of people took to the streets and protested the Nicaraguan canal project that would connect the Atlantic with the Pacific.[159] In 2018, citizens protested and demanded the resignation of both president Ortega and his wife, who served as vice-president of Nicaragua.[160] During the 2018 protests, 300 people died, 2,000 were injured, and since then, 100,000 people have fled Nicaragua to seek asylum elsewhere.[161] Considering all these challenges to regime survival, it would only be natural for Nicaragua to seek surveillance assistance from China. However, Nicaragua was either unwilling or unable to get equipment from China. Instead, it acquired deep packet inspection internet surveillance gear from the Russian company VAS Experts, sometime between 2013 and 2018.[162]

6.4. Why geographical proximity and constructivist challenges fail to explain Chinese cyber norm diffusion

The examples above show how material incentives of Chinese seeking of influence (along the BRI and amongst Taiwan allies) and regime survival drive diffusion.

Geographical proximity theory claims that interconnectedness explains successful norm proliferation. So do Levitsky and Way, who look at norm diffusion taking place from

https://www.bbc.com/news/world-latin-america-33125526; BBC News, "Nicaragua Unrest: Thousands Join Renewed Anti-Government Rallies," May 27, 2018, sec. Latin America & Caribbean, https://www.bbc.com/news/world-latin-america-44269498; Karen McVeigh, "Over 100,000 Have Fled Nicaragua Since Brutal 2018 Crackdown, Says UN," *The Guardian*, March 11, 2020, sec. Global development, 00, https://www.theguardian.com/global-development/2020/mar/11/over-100000-have-fled-nicaragua-since-brutal-2018-crackdown-says-un.

[159] BBC News, "Nicaragua Canal Protest"; BBC News, "Nicaraguans Protest Against Canal Plans."

[160] BBC News, "Nicaragua Unrest."

[161] McVeigh, "Over 100,000 Have Fled Nicaragua Since Brutal 2018 Crackdown, Says UN," 00.

[162] VAS Experts, "About Us," *VAS Experts*, 2019, https://vasexpertsdpi.com/about-us/.

Western powers to countries that they have strong linkages with.[163] Levitsky and Way purport that geographic closeness matters in diffusion. According to them, it is the single most important factor, because geography is a proxy for strong economic and political interdependence. According to this theory, China's norm would diffuse to Southeast Asia, Central Asia and Russia, but it would less likely diffuse to Zimbabwe, which is thousands of miles away and linkages are not that strong. As such, geographical proximity theory disregards the strategic calculus of China, which is focussed on geographical areas way beyond its immediate surroundings and which explains why China's norm has diffused globally (including to Zimbabwe) and not only regionally.

Constructivists would see the BRI as an ideal organisational platform for China to promote the concept of internet sovereignty, since the Initiative builds on historic ties (Ancient Silk Roads) that China can more easily revive and use to socialise countries into a certain like-mindedness. And China does indeed use the BRI as a forum to persuade countries of the usefulness of its information control technology and techniques. It organises propaganda and cybersecurity trainings for BRI countries to make them more like-minded. In Chinese bureaucracy lingo, "like-mindedness" stands for a group of nations that share certain norms of acceptable state behaviour.[164] It is the view of this thesis that, while it is true that China "socialises" countries into its understanding of internet sovereignty through trainings, this thesis diverges with constructivism on "why" China organises these trainings and why receiving countries partake in them. Constructivists would purport that China tries to convince other countries out of pure

[163] Steven Levitsky and Lucan Way, *Competitive Authoritarianism: Hybrid Regimes After the Cold War*, Problems of International Politics (New York: Cambridge University Press, 2010): 43.
[164] Alice Ekman, Sinikukka Saari, and Stanislav Secrieru, "STAND BY ME!: The Sino-Russian Normative Partnership in Action," August 2020, https://www.iss.europa.eu/content/stand-me-sino-russian-normative-partnership-action.

ideational reasons, which may contradict and sometimes coincide with its material interests. But as it is exposed in this chapter, China's attempts to socialise countries into how to manage information is predominantly based on material interests of seeking influence, and countries that start to adopt China's norm do so out of regime survival concerns.

The example of Iran shows this very clearly. Iran may mimic China because it admires China and feels a certain "like-mindedness", but that is purely based on materialistic reasons of regime survival concerns. Before the large-scale Iranian protests of 2009, Iran received surveillance assistance from Western countries (see Iran observation above). Once those countries stopped providing products, China stepped in. This shows how opportunistic surveillance imports are. Whoever provides them is welcome. China, on the other hand, may feel compelled to help Iran to quell dissent, but again, the material benefits for China in doing so are clear – economic and political influence over Iran (due to the vacuum left by Western powers) and potentially also more influence over Iran based on intelligence from backdoors in equipment installed in Iran.

In short, constructivism fails to accurately assess the motivation underlying Chinese exports and countries' import behaviour. In contrast, neoclassical realism can provide a satisfying answer in this regard. It states that the material interests of seeking of influence and regime survival concerns underly the diffusion of the Chinese cyber sovereignty norm. This chapter has provided empirical evidence for this argument.

6.5. The Chinese technosphere and sovereignty

The process of information control diffusion creates a Chinese technosphere. While countries of a technosphere are strengthened in their position against their domestic populations, the process of technology and technique diffusion gives China political and economic influence over importing states. This means that the Westphalian sovereignty of importing states is being weakened vis-à-vis China.

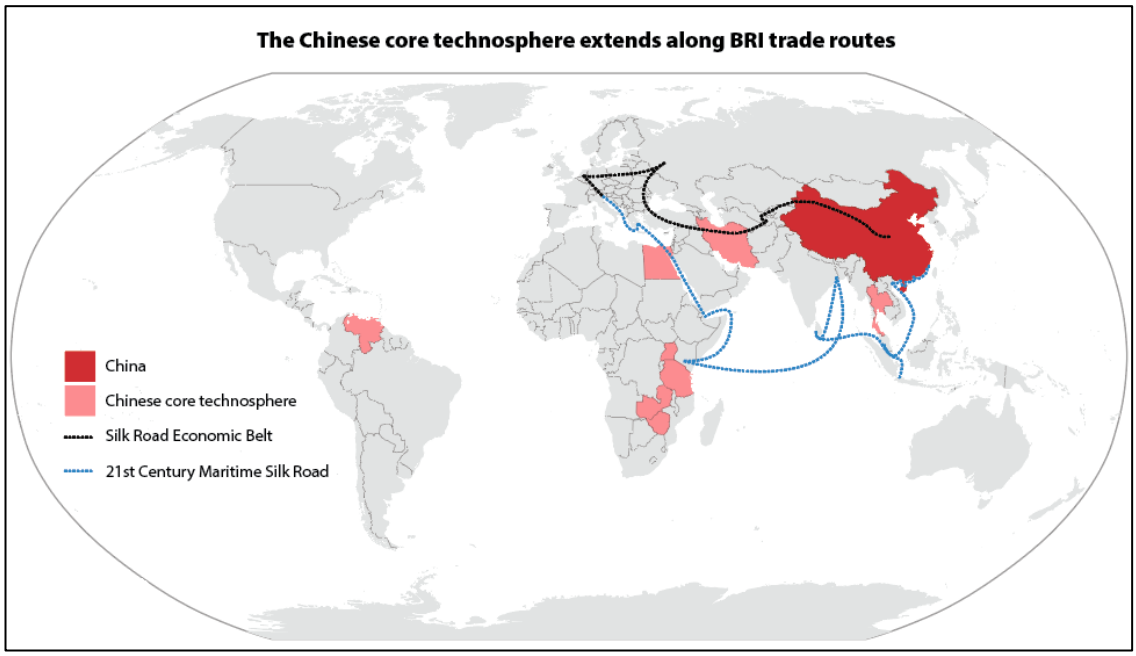


Figure 14: The Chinese core technosphere (primarily) extends along BRI trade routes.

6.5.1. China bolsters domestic and interdependence sovereignty

The case of Zimbabwe

China increases the domestic sovereignty of countries in two ways: options and use. Taking Zimbabwe as an example, this thesis shows that censorship and surveillance technology, as well as training in propaganda, were the primary exports from China to Zimbabwe. This diffusion increases Zimbabwe's options to induce fear through

surveillance technology as well as its ability to censor and manipulate its population. 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 Chinese diffusion, making the exertion of information controls more efficient. Zimbabwe may have chosen to rely on censorship and strategic information dissemination no matter what, but interacting with China has brought the African country closer to adopting that approach in full. This means that China has changed how Zimbabwean authorities exert authority and how effectively they do so. 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.

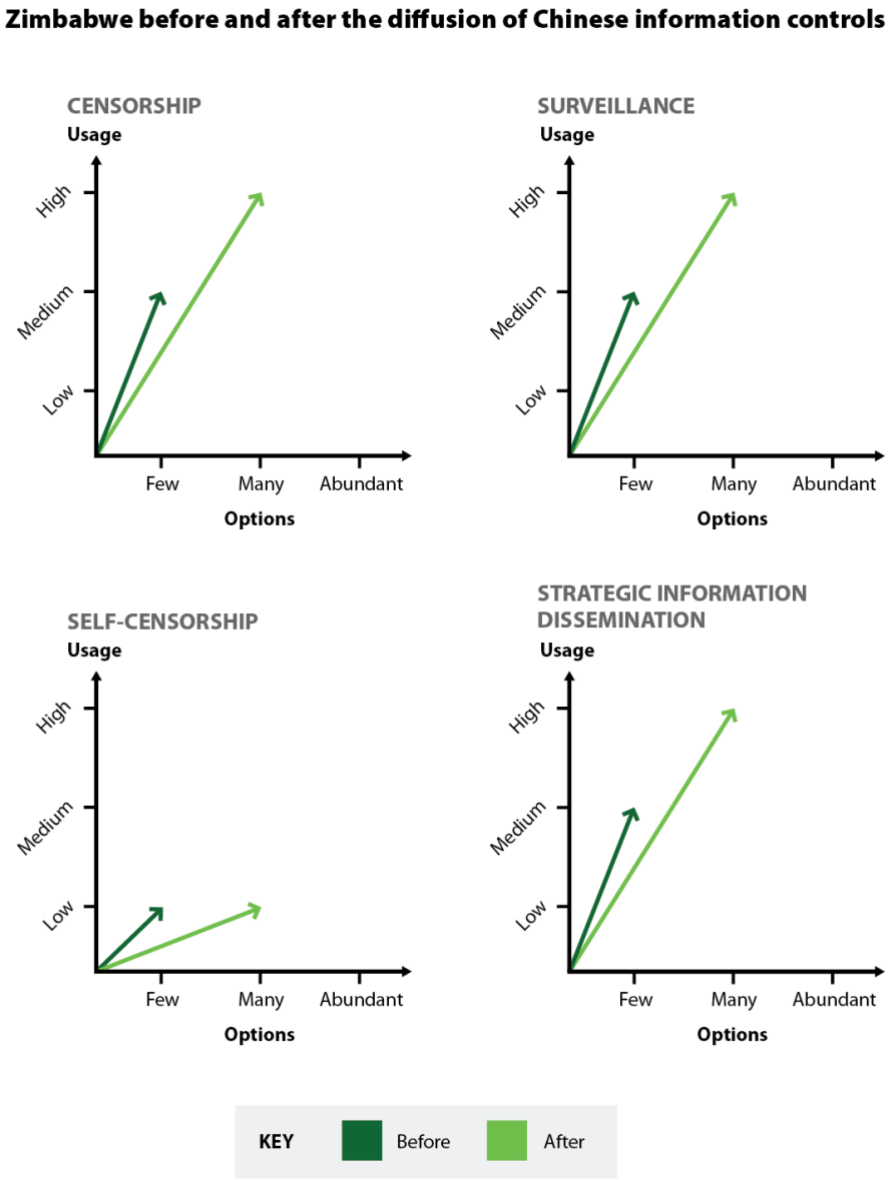


Figure 15: The impact of Chinese information control diffusion on Zimbabwe[165]

[165] The in-depth study of Zimbabwe's information control landscape is outside the scope of this thesis; 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 thesis.

Going beyond Zimbabwe

Powerful surveillance tools from China increase the surveillance options of countries and how they use technology and techniques to control their populations. Similarly, as in Zimbabwe, Beijing thereby increases their domestic and interdependence sovereignty.

The newly imported surveillance technology is often used to crack down on countries' own populations. The New York Times revealed that Ecuadorian authorities use an imported safe city from China to monitor a former Ecuadorian intelligence official.[166] The former official explained to the New York Times that the surveillance camera, which is part of the Chinese-built safe city project, is pointing directly at his house with no identifiable public security benefit. Hence, it is reasonable to argue that the Ecuadorian government uses the pretext of public security to monitor individuals that may be endangering its regime's stability.

In Uganda, Huawei has helped law enforcement personnel with the hacking of opposition figures' phones.[167] This strengthens Ugandan elites' domestic internet sovereignty vis-à-vis opposition figures and media. Ugandan authorities have already targeted a prominent opposition figure for the 2021 Ugandan presidential elections, Bobi Wine. Mr Wine, who is also a popular singer, carries with him several phones to evade surveillance. This case shows that assistance from China, that enables Ugandan authorities to better control a political opposition figure, could potentially tilt the balance in foreign elections in favour of the political incumbents. One might argue and say that Ugandan authorities would have

[166] 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.
[167] Parkinson, Bariyo, and Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents."

intercepted Wine's communications in any case, but a Wall Street Journal article claims otherwise:

"According to [Ugandan] officials, the team, based on the third floor of the capital's police headquarters, spent days trying to penetrate Mr. Wine's WhatsApp and Skype communications using spyware, but failed. Then they asked for help from the staff working in their offices from Huawei, Uganda's top digital supplier."[168]

It took Huawei technicians only two days to penetrate Mr Wine's communications.[169]

In Southeast Asia, the diffusion of the Chinese cybersecurity law has strengthened internal sovereignty too. Thailand, for its part, has passed a Cybersecurity Act in 2019 that will give Thailand's National Cybersecurity Committee (NCSC) unchecked powers.[170] Under the law, the NCSC can seize equipment and data without a court order in what authorities designate "emergency cases."[171] The law also stipulates that social media platforms must delete content that is "against public order or good morals of the people."[172] Just like in China, the Thai Cybersecurity Act remains intentionally vague to have flexibility when filing charges against dissidents or opposition voices.[173]

Furthermore, several countries aim to increase their interdependence sovereignty by imitating China. Iran, Thailand, and Uganda have all attempted to implement their own Great Firewalls, to better control information that crosses their borders. Moreover, in

[168] Ibid.
[169] Ibid.
[170] Coca, "Tourism from China Provokes an Internet Crackdown in Thailand."
[171] Ibid.
[172] Ibid.
[173] Coca, "Tourism from China Provokes an Internet Crackdown in Thailand."

order to monitor WhatsApp and the internet infrastructure, China supplies countries with tools to better manage cross-border information flows.

6.5.2. China erodes Westphalian sovereignty

The export of information controls gives China the opportunity to intervene into importing countries' internal affairs – thereby eroding their Westphalian sovereignty. Beijing acquires the means to intervene in a technosphere in political, intelligence, and economic terms.

Politically, Beijing influences how countries control information domestically. Beijing is creating a community of like-minded authoritarian-leaning countries. Through extensive socialisation of overseas entities into Chinese information control practices, China moulds the international space to look a lot like its domestic information environment. The more countries overseas identify with China's environment, the easier it is for China to exert influence. The example of Huawei in Uganda and Zambia is illustrative. Huawei's employees have helped those two countries to spy on opposition candidates and critical journalists.[174] Huawei employees sit alongside Ugandan and Zambian law enforcement officials and share their techniques first-hand with them. This creates a bond between China and those countries but, more importantly, it creates reliance on China to control their domestic populations. This gives China a considerable amount of influence over these countries.

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

Another way China is interfering into importing countries' internal affairs is by redrawing their media landscapes through the invitation of foreign journalists to China for the purpose of "training" in propaganda. As described by Cardenal, however, "training" means something slightly different to China:

> "'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."[175]

During the training, journalists visit media outlets, such as the People's Daily, a Chinese Communist Party mouthpiece. A biased view is seen in the trainees' reporting, which is uncritical of Chinese infrastructure projects within their own countries. Interestingly, China invites countries specifically from the BRI. It is no coincidence that those are the countries where China has most infrastructure projects running and where it wants to increase positive coverage of those projects. One instance of such a biased view is the reporting of a Pakistani journalist. In 2018, Abdul Wajid Khan, a Pakistani citizen, has spent 10 months in China attending a media fellowship.[176] During his fellowship, in October 2018, he published a piece in China Daily, a newspaper owned by the Communist Party of China. The article is titled "Anti-CPEC [China-Pakistan Economic Corridor]

---

[175] 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.: 31.

[176] 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.

propaganda and reality."[177] The article presents a one-sided view of the CPEC project and while the journalist's views might have already been pro-China before the training, they became even more so during the fellowship. He writes: "Pakistan should take benefits from China's experience of industrialization."[178]

Another case is Frederick P. W. Gaye, an African journalist, who was a media fellow of the China Public Diplomacy Association in 2016.[179] Having concluded the fellowship, he continued on numerous occasions to report on Chinese projects in Liberia, omitting any critical comments on the projects.[180] It may be assumed that in this case the sponsoring of journalists from BRI countries, and the tying of them into Chinese news reporting overseas after the fellowship, has clear benefits to China, because it raises its legitimacy abroad through uncritical local reporting about Chinese involvement overseas.

China's influence in a given country also depends on how big the country is. If a handful of journalists from Antigua and Barbuda (population size: 97,000) is trained in China, this has a much larger impact on the media landscape in Antigua and Barbuda, as compared to whether journalists from Thailand (population size: 70,000 000) attend trainings.[181] The ratio of journalist per citizen is much greater in the latter case. It might also be important who participates in trainings. It makes a difference if a media executive

---

[177] Abdul Wajid Khan, "Anti-CPEC Propaganda and Reality," *China Daily*, October 30, 2018, http://www.chinadaily.com.cn/a/201810/30/WS5bd7fda5a310eff3032857a2.html.
[178] Ibid.
[179] Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
[180] Fredrick Gaye, "China Completes Hand Pumps Project In Many Liberian Schools," Inprofiledaily, (December 4, 2018), http://inprofiledaily.com/index.php/2018/12/04/china-completes-hand-pumps-project-in-many-liberian-schools/; Frederick P. W. Gaye, "China's $60M Ministerial Complex Project in Liberia Finally Begins," *People's Daily*, September 16, 2016, http://en.people.cn/n3/2016/0916/c90000-9115672.html; Frederick P. W. Gaye, "Chinese Medical Team Expands Services in Liberia," *People's Daily Online*, August 22, 2016, http://en.people.cn/n3/2016/0822/c90000-9103618.html.
[181] The World Bank, "Population, Total," 2019, https://data.worldbank.org/indicator/SP.POP.TOTL?locations=AG.

takes part in trainings, who has greater influence on the domestic media landscape, rather than a young journalist. Judging from the source material collected in this thesis, it seems that China is targeting both media executives, who have influence, and young journalists, who can be seen as an investment into future reporting on China abroad. It may also make a difference how strongly developed the media landscape is in a given country. Chinese training in information controls of journalists from the US may have a lesser impact than similar trainings of journalists from Zimbabwe, since the latter country has only few quality media outlets and journalism schools compared to the former. It can be reasonably assumed, therefore, that the US media landscape can more easily counterbalance any Chinese information control techniques shared with US journalists.

China also undermines Westphalian sovereignty in terms of intelligence, by exporting hardware and software which can be used to exert political influence. To give an example, in a hypothetical trade deal discussion between Zimbabwe and China, the exported hardware and software by China might enable China to eavesdrop on the negotiation tactics of Zimbabwe.

Surveillance and censorship hardware are often, if not always, installed at critical points of countries. Safe cities, for instance, have cameras installed in most places that are important for public security. Surveillance middleboxes are installed in all important chokepoints of a country's internet infrastructure, because their purpose is to capture all important traffic that flows through internet cables.

Furthermore, Chinese companies have been constructing and equipping government offices and military bases around the world. This gives them the option to spy more easily

on countries if they wish to do so. Such snooping is possible, since most surveillance equipment is connected to the internet. For China it is easier to build in backdoors in such gear because it controls the supply chain of the product.[182] Backdoors are very difficult to detect, since they are designed not to look like backdoors.[183] This security concern led the US to ban major Chinese companies that produce surveillance products from supplying US government and military facilities with gear. In this vein, the US Congress passed the National Defense Authorization Act for Fiscal Year 2018, which prohibits the procurement of Huawei and ZTE technology for US military purposes.[184]

Cases where espionage undertaken by Chinese companies was revealed are rare, but in 2018, Le Monde reported that Huawei was involved in snooping around the African Union's (AU) headquarters in Addis Ababa. The building was financed by the Chinese government and the telecommunications equipment was provided by Huawei.[185] The gist of the story is that data was flowing from Addis Ababa to unknown servers in Shanghai for five years (2012-2017). Once Le Monde broke the story, the African Union changed its servers and declined help from the Chinese government to configure them.[186] In 2020, Japan's Computer Emergency Response Team discovered that an infrastructure associated with a Chinese hacking group dubbed "Bronze President" has exfiltrated

[182] Bruce Schneier, "Every Part of the Supply Chain Can Be Attacked," *The New York Times*, September 25, 2019, sec. Opinion, https://www.nytimes.com/2019/09/25/opinion/huawei-internet-security.html.
[183] UK Parliament, "Suppliers, Network Operators and Academics Questioned on UK Telecommunications Infrastructure - News from Parliament," *UK Parliament*, accessed October 8, 2019, https://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/news-parliament-2017/uk-telecommunications-infrastructure-evidence-17-19/.
[184] Mac Thornberry, "Text - H.R.2810 - 115th Congress (2017-2018): National Defense Authorization Act for Fiscal Year 2018," webpage, (December 12, 2017), doi:/bill/115th-congress/house-bill/2810/text.
[185] Danielle Cave, "The African Union Headquarters Hack and Australia's 5G Network," *The Strategist*, July 12, 2018, https://www.aspistrategist.org.au/the-african-union-headquarters-hack-and-australias-5g-network/.
[186] Tilouine and Kadiri, "A Addis-Abeba, le Siège de l'Union Africaine Espionné par Pékin."

surveillance footage from the AU buildings.[187] An AU official who spoke to Reuters mentioned that protest from the AU is unlikely since China helps running the building, as exemplified by a recent power outage when Chinese engineers helped to repair the fault.[188]

Another spying incident occurred at Bangkok airport. Chinese espionage services have put in place an advanced travel intelligence operation, compiling databases that traced passenger lists.[189] In the words of a former US official: "The Chinese have consistently extracted data from all the major transit hubs in the world", which may be done in order to track the movement of foreign spies.[190] As part of this effort, China has hacked into the Bangkok airport network to access passenger biometric data (e.g. CCTV data of faces and fingerprints).[191] This shows how important such data is for China and that it is actively seeking it from abroad. In this vein, it is fitting to note that China has, e.g., equipped the Thai Ministry of Commerce with CCTV gear, which may make it easier for China to access biometric data from these cameras.[192]

The smaller the country that imports technology, the larger will be the immediate influence of China. A safe city project in Mauritius gives China much more power over the Mauritian population than a safe city exported to Germany. This is because Germany has more resources to devote to cyber security risk mitigation to fend off cyber intrusions,

---

[187] Raphael Satter, "Exclusive-Suspected Chinese Hackers Stole Camera Footage From African Union - Memo," *Reuters*, December 16, 2020, https://www.reuters.com/article/us-ethiopia-african-union-cyber-exclusiv-idUSKBN28Q1DB.
[188] Ibid.
[189] Jenna McLaughlin and Zach Dorfman, "'Shattered': Inside the Secret Battle to Save America's Undercover Spies in the Digital Age," December 30, 2019, https://news.yahoo.com/shattered-inside-the-secret-battle-to-save-americas-undercover-spies-in-the-digital-age-100029026.html.
[190] Ibid.
[191] Ibid.
[192] Hikvision, "Hikvision Protects Ministry of Commerce (MOC) Thailand."

due to its larger economy. This was recently seen in Germany instituting a review board for Huawei's provision of 5G equipment into national critical infrastructure.[193]

Economically, China further undermines countries' sovereignty. Kai Fu-Lee, previously president of Google China, likens the export of Chinese advanced technology, which includes surveillance equipment, to extractive colonial practices of the past:

> "[I]f most countries will not be able to tax ultra-profitable AI companies to subsidize their workers, what options will they have? I foresee only one: Unless they wish to plunge their people into poverty, they will be forced to negotiate with whichever country supplies most of their AI software— China or the United States—to essentially become that country's economic dependent, taking in welfare subsidies in exchange for letting the 'parent' nation's AI companies continue to profit from the dependent country's users. Such economic arrangements would reshape today's geopolitical alliances."[194]

As another example, Venezuela is a highly indebted country and it is still buying Chinese security gear worth millions of dollars. So does Ecuador, which exchanged oil for equipment, thereby maintaining workplaces in high-tech industries within China. In a nutshell, some information control interactions between China and importing countries are extractive in nature and create an economic dependency on China.

On the other hand, China has largely benefitted from the exports of surveillance technology and increased its dominance over the surveillance industry. China's domestic artificial intelligence (AI) surveillance market is estimated at US$2 billion and is expected to rise to around US$19 billion in 2023.[195] The domestic industry is not bound to borders

---

[193] Douglas Busvine, "Exclusive: China's Huawei Opens up to German Scrutiny Ahead of 5G Auctions," *Reuters*, October 23, 2018, https://www.reuters.com/article/us-germany-telecoms-huawei-exclusive-idUSKCN1MX1VB.

[194] Kai-Fu Lee, "The Real Threat of Artificial Intelligence," *The New York Times*, June 24, 2017, https://www.nytimes.com/2017/06/24/opinion/sunday/artificial-intelligence-economic-inequality.html.

[195] Charles Rollet, "China Enforces Barriers Against Foreign AI and VSaaS Providers," *IPVM*, 02:06 400AD, https://ipvm.com/reports/vats.

and has exported strongly abroad. Dahua Technology and Hikvision are, for instance, the world's two largest video surveillance manufacturers.[196] Exporting facial recognition to Zimbabwe to capture darker faces, for instance, may give the Chinese AI sector a crucial advantage against its competitors such as Google and Facebook in targeting the African market in the future, because Western companies do not have yet accurate facial recognition systems trained on darker faces.[197] Thus, exporting now rather than later has additional benefits for China's surveillance industry and reinforces its exports. The Chinese government has recognised the potential for increasing exports and has facilitated annual exhibitions to pair up Chinese security companies with law enforcement officials from countries along the BRI trade routes. At a security exhibition that took place within the frame of the Lianyungang Forum on law enforcement, China's Ministry of Public Security stated that the Forum is intended to "…promote domestic [p]olice equipment and security companies and products…[to] go abroad."[198]

6.6. Conclusion

This chapter has filled the norm diffusion framework, presented in Chapter 4, with data and shown that the Chinese norm is much more likely to diffuse to authoritarian-leaning countries that have experienced large scale protests (increase in regime threat perception) and countries that are targeted by China's export initiative (whose aim is to increase influence abroad).

[196] IPVM, "First US State, Vermont, Bans Dahua and Hikvision," 01:31 500, https://ipvm.com/reports/vermont-hikua.
[197] 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/.
[198] Lianyungang Forum, "即使不露脸，照样知道你是谁," November 23, 2018, http://www.lygforum.gov.cn/english.php?m=news&a=details&content_id=535.

By empirically illustrating these causal mechanisms of supply and demand, this chapter demonstrated that other explanations of norm diffusion as supplied by geographical proximity theory and constructivist theory are less suited to shedding light on Chinese internet sovereignty diffusion.

Finally, this chapter showed that countries that receive information controls from China are enabled to keep a better lid on dissent because of an increase in information control capabilities (strengthening of domestic and interdependence sovereignty). At the same time, their Westphalian sovereignty vis-à-vis China weakens because of China's growing ability to spy on and economically exploit importing countries through Chinese surveillance equipment and extractive deals.

The analysis of China's internet sovereignty norm diffusion only gives a partial answer to this thesis' research question of why Chinese and Russian internet sovereignty norms diffused successfully. In order to answer the research question in full, this thesis now turns towards examining why Russia's internet sovereignty norm proliferated successfully across its borders.

Chapter 7: The regional web of Russian information controls

Chapter 7 defines the Russian cyber sovereignty norm (emphasis on self-censorship) and argues that it diffused predominantly to the CIS, because Russia has promoted exports to this geographical area in order to maintain or extend influence there. At the same time, CIS governments turned to Moscow in buying surveillance technology and imitating Russian laws on data because protest movements and news about the Arab Spring, powered by social media, seriously challenged their regimes. The cases examined in this thesis are: Belarus, Kazakhstan, Kyrgyzstan, Ukraine, and Uzbekistan. In short, the exchange is in both Moscow and the CIS elites' interest. It is a *quid* (Russia helps to maintain regime stability) *pro quo* (regimes depend on Russia for their stability). The case of Ukraine shows that information control diffusion can come to a halt when this *quid pro quo* and this acquiescence of being in a sphere of influence is being terminated by the influenced state (Ukraine). While Russia was still seeking influence in Ukraine post-Maidan protests (supply side), Ukraine itself turned to China (alternative supplier) to maintain stability. This is because the threat perception within the Ukrainian elite has changed. The primary challenge for the Ukrainian elite to stay in power was no longer the Ukrainian people, but Russia. Hence, a change in threat perception in the demand side of diffusion explains the halt in Russian information control diffusion to Ukraine after 2014.

The chapter continues by examining two alternative theories to explain the diffusion of Russian information controls: geographical proximity theory and constructivism. Geographical proximity theory purports that geographical, historic, societal and economic interlinkages between two countries explain the diffusion of norms. It may

sound reasonable to say that CIS countries have strong interlinkages with neighbouring Russia, and thus, geographic proximity theory may, to some extent, be an appropriate explanatory theory. However, geographical closeness fails to provide a rationale for why Ukraine did not import any Russian information controls after the Maidan protests of 2014. Geography was a crucial factor for geographic proximity theory to explain diffusion *before* 2014, but in 2015, Ukraine's geographical closeness to Russia did not translate anymore into information control diffusion.

Constructivist theory, for its part, claims that Russian information control diffusion is more than a *quid pro quo* – bolstering of regime survival capabilities in exchange for Russian influence. However, as all the below cases will show, information control diffusion is precisely that, a *quid pro quo*, and nothing more.

Russia gains influence in these countries by providing technology that is suspected to be riddled with backdoors (see below the concerns of a Kyrgyz adviser to the government). Through spying, Russia knows the political decision-making in CIS countries in and out, which may give it an information advantage, for instance, in economic or political negotiations with these countries (weakening of their external sovereignty).

7.1. Russia's internet sovereignty norm

Most Russian information control technology has its roots in the late Soviet era, when it was developed in government-funded research laboratories. Many engineers from those laboratories lost their work after the fall of the Soviet Union and founded their own companies that provide interception services.[1] The financial crisis of 1998-99 and the US

[1] Borogan and Soldatov, "Just Business."

intervention in Kosovo in the late 1990s heightened the threat perception in Moscow.[2] As a result, the Kremlin drafted its "Foreign Policy Concept" and the "Information Security Doctrine" in 2000.[3] Both documents emphasise the need to protect sovereignty online and offline in light of such events. The colour revolutions of the 2000s added further to the perception that sovereignty was being undermined. These events led Vladislav Surkov, former chief ideologist of the Kremlin, to conceptualise the term "sovereign democracy" in 2006.[4] The concept is the Kremlin's response to both pressures from below (populist) and above (international pressure).[5] In order to manage these pressures, a nationalisation of the economy, strengthening of the defence forces, and restriction of media freedom was seen necessary.[6] Tomas Janeliūnas, professor at Vilnius University, claims that sovereign democracy does not only entail the nationalisation of the economy, but also the nationalisation of information.[7] This likely translates into the Kremlin wishing to extend its ability to control information.

This sovereignty discourse of Russian elites persisted in the 2010s. In the words of president Putin:

"The very concept of state sovereignty is being eroded. Undesirable regimes, countries that pursue an independent policy or simply stand in the way of someone's interests, are destabilized. To do this, the so-called color revolutions are used…"[8]

---

[2] Giles, *Moscow Rules: What Drives Russia to Confront the West*.
[3] Ibid.; Russian Federation, Information Security Doctrine of the Russian Federation.
[4] Vladislav Surkov, "Nationalization of the Future," *Expert Online 2.0*, November 20, 2006, https://web.archive.org/web/20101110050502/http://expert.ru:80/printissues/expert/2006/43/nacionalizaciya_buduschego/.
[5] Ivan Krastev, "'Sovereign Democracy', Russian-Style," *Insight Turkey* 8, no. 4 (December 2006): 113–17.
[6] Tomas Janeliūnas, "'Sovereign Democracy' - Yet Another Attempt to Define Russia's Regime," *Lithuanian Foreign Policy Review*, no. 18 (2006): 117–32.
[7] Ibid.
[8] This is the author's translation of President of Russia, "Заседание Совета Безопасности," *Президент России*, July 22, 2014, http://kremlin.ru/events/president/news/46305.

In 2014, Sergei Lavrov, the Russian foreign minister, framed colour revolutions as foreign operations that spread democracy and instigate regime change.[9] Defence minister Sergei Shoigu complemented Lavrov's statement by saying that information warfare is a central aspect of those revolutions.[10]

Any such revolution would have dire consequences for the political elite in Russia. Recent history has shown that emperors as well as Soviet leaders did not transit peacefully into retirement. Often, they were murdered and toppled by a coup d'état.[11] President Putin echoes this troubled history by discussing the potential of digital technologies to cause instability. In a 2012 article, he noted that the Arab Spring showed how information technologies have become an important factor for domestic and international politics. He continued by saying that these events "require reflection… to reduce the risk of its use by terrorists and criminals."[12] In 2012, Sergey Smirnov, then first deputy director of the FSB (Federal Security Service, which is Russia's main security agency) declared that: "New technologies are used by Western secret services to create and maintain a level of continual tension in society with serious intentions extending even to regime change."[13] In 2017, large protests shook Russia. During March of the same year, Putin claimed that these unrests could lead to an Arab Spring style event within Russia.[14]

---

[9] Однако, "Лавров, Шойгу и Генштаб: О «цветных Революциях», Украине, Сирии и Роли России," May 23, 2014, http://www.odnako.org/blogs/konferenciya-po-mezhdunarodnoy-bezopasnosti-o-cvetnih-revolyuciyah-ukraine-sirii-i-roli-rossii/.

[10] Corey Flintoff, "Are 'Color Revolutions' A New Front In U.S.-Russia Tensions?," accessed July 3, 2020, https://text.npr.org/s.php?sId=321392873.

[11] Giles, *Moscow Rules: What Drives Russia to Confront the West*.

[12] Vladimir Putin, "Russia and the Changing World," *Moskovskie Novosti*, March 28, 2020, http://web.archive.org/web/20200328133258/https://www.mn.ru/politics/78738.

[13] Ronald. Deibert, *Black Code: Inside the Battle for Cyberspace* (Toronto: Signal, 2013).

[14] Neil MacFarquhar, "Vladimir Putin, in First Remarks on Russian Protests, Warns of Potential Chaos," *The New York Times*, March 30, 2017, sec. World, https://www.nytimes.com/2017/03/30/world/europe/putin-russia-protests.html.

This historic context of perception of insecurity and instability within the Russian ruling elite is also seen within its information control policies and practices that were often a result of periods of heightened insecurity, such as in 2000 (financial crisis 1998-99), 2012 (large protests), and 2017 (large protests). The following paragraphs give concrete examples of such policies and practices.

Surveillance

Russia started laying the legal foundations for its extensive surveillance framework in 1995, with the "Law on Operational Investigations", which allowed the FSB to operationalise its online surveillance system — also known as SORM, the System for Operative Investigative Activities.[15] SORM-1 focused on intercepting landline 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.[16] Here, it is important to underline the difference of SORM to European or American interception systems. While agencies in the latter countries have to operate according to court orders and have to ask for access to the data gathered by Internet Service Providers (ISPs), no such safeguards are present in the SORM system.[17] Russian internet service providers had to install SORM equipment in order to obtain licenses to operate.[18] This equipment gives law enforcement agencies direct access to the data of individuals.[19] Furthermore, it is the ISPs' duty to maintain the

[15] Kerr, "The Russian Model of Internet Control and Its Significance."
[16] Privacy International, "Lawful Interception: The Russian Approach," March 4, 2013, https://privacyinternational.org/blog/1296/lawful-interception-russian-approach.
[17] Human Rights Watch, "The Right to Privacy in Uzbekistan," June 2015, https://privacyinternational.org/sites/default/files/2017-12/PI%20submission%20Uzbekistan.pdf.
[18] Ibid.
[19] Ibid.

equipment and make sure that law enforcement have continued access to data. If they fail to do so, they face pecuniary sanctions, or their licenses may be revoked.[20]

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.[21] 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.[22] These laws were intended to showcase Russia's pervasive surveillance over its citizens and induce self-censorship.[23]

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.[24] More subtle measures of intimidation have far-

[20] Ibid.

[21] Russian Federation, Information Security Doctrine of the Russian Federation.

[22] Kerr, "The Russian Model of Internet Control and Its Significance."

[23] 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.

[24] 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.

reaching effects, too. Russia's state-led discourse, emphasising the dangers of the internet, has been found to increase self-censorship.[25]

Strategic information dissemination

In Russia, the emphasis of propaganda and disinformation is on spreading pro-regime messages.[26] 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.[27] 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.[28] Some of them work full-time, spending twelve-hour shifts at their offices.[29]

Censorship

[25] 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.
[26] 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).
[27] Ibid.; BBC, "Russia Profile - Media," April 25, 2017, sec. Europe, https://www.bbc.com/news/world-europe-17840134.
[28] 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.
[29] Walker, "The Russian Troll Factory at the Heart of the Meddling Allegations."

Russia maintains a national blacklist of websites and uses advanced surveillance capabilities, such as deep packet inspection technology, to enforce the blacklist.[30] However, filtering in Russia is less pervasive than in China. Alexei Navalny's YouTube channel, for instance, is allowed to operate despite his critical stance on the Kremlin.[31] One potential explanation for the relatively lax approach to filtering information is, that unlike China, Russia has not been able to create domestic substitutes for foreign media platforms. Russian technology companies fail to reach a sufficient domestic market share. This includes Russian companies that run app stores, search engines, or social media platforms.[32] In contrast, if Russia were able to exclude foreign social media companies and replace them with national champions it would more likely be able to enforce stringent censorship.

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.[33] Telegram Messenger is still available in mobile 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

[30] Jakub Dałek, *Russian Blacklist*, Python, (2014; repr., 2018), https://github.com/jakubd/russian-blacklist; Seddon and Foy, "Russian Technology."
[31] Алексей Навальный, "Алексей Навальный," *YouTube*, accessed March 19, 2019, https://www.youtube.com/channel/UCsAw3WynQJMm7tMy093y37A.
[32] 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.
[33] 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.

plethora of circumvention apps are still available at the Apple Store and Google Play Store in Russia.[34]

7.2. The diffusion of Russia's internet sovereignty norm

7.2.1. Understanding the supply side of diffusion

The following section demonstrates how cyber norm exports were driven by an underlying wish to maintain or extend Russia's influence in the post-Soviet space. Russian security assistance to countries of the former Soviet Union is not new. Dmitry Gorenburg, a Senior Research Scientist at Harvard University, writes, for instance, that:

> "Russian military assistance to the weaker Central Asian states can be described as a quid pro quo arrangement, wherein Russia provides political and military support for the ruling regimes in exchange for … a certain level of acquiescence on Russian foreign policy priorities in the region."[35]

Mark Galeotti, for his part, maintains that Russia shares intelligence with authoritarian-leaning regimes in its so-called "near abroad", a term used by political Moscow to describe republics of the former Soviet Union, which the Kremlin does not recognise as fully sovereign.[36] Galeotti continues by claiming that:

---

[34] 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.

[35] Dmitry Gorenburg, "External Support for Central Asian Military and Security Forces" (SIPRI, January 2014), https://www.sipri.org/sites/default/files/SIPRI-OSFno1WP.pdf.

[36] Mark Galeotti, "'RepressIntern': Russian Security Cooperation with Fellow Authoritarians," in *No Shelter: The Harassment of Activists Abroad by Intelligence Services from the Former Soviet Union*, ed. Adam Hug (London: The Foreign Policy Centre (FPC), 2016), https://fpc.org.uk/wp-content/uploads/2016/11/1786.pdf; William Safire, "ON LANGUAGE; The Near Abroad," *The New York Times*, May 22, 1994, https://www.nytimes.com/1994/05/22/magazine/on-language-the-near-abroad.html.

"[G]iven Moscow's evident and overwhelming superiority in the intelligence field, this inevitably becomes one more instrument in its campaign to dominate post-Soviet Eurasia through a mix of coercion and assistance."[37]

Russia has funnelled its influence seeking in countries of the CIS. Similarly, as China's BRI, the CIS is where Russian strategic priorities lie. 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.[38]

Research for this paper found that the while Russian information controls diffused to 28 countries – that are as geographically varied as Palestine and Mexico – countries from the CIS account for a disproportionately large share of Russian information control exports (25 percent or 7 out of 28 countries).[39] This thesis argues that a large share of exports goes to CIS countries because Russia is actively seeking to change the information control environment in these countries into an image of its own and with the aim to better exert influence abroad.

Russia's seeking of influence in Crimea, Luhansk, and Donetsk

[37] Ibid.: 13.

[38] 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.

[39] This number represents the breadth of diffusion (number of countries exported to) and not the depth (how much was exported to a given country).

Russian actions in Crimea, and separatist regions Luhansk and Donetsk People's Republics show how information control abroad changes according to Russian strategic interests, i.e., how the supply side of information controls changed. Ukraine (post-2014) is a unique example, because the actions and their effects are more easily identified. Russian information control measures were blatant and had great effects on the Ukrainian occupied territory. It shows how Russia would like the information environment abroad to look like. It highlights how this landscape would look like if it had complete control over it – it is an information environment that reflects its strategic interests. It is Russian information controls (abroad) at its extremes. It is interesting that pre-2014, Russia did have some control over major Internet Service Providers in Ukraine. For instance, Russian entities operated major ISPs in Ukraine, such as Kyivstar (which was in the hands of Russian oligarch Mikhail Fridman) or Vodafone Ukraine, which was a daughter company of Russian MTS corporation until 2019.[40] Such ownership and provision of internet services was in Russia's economic advantage i.e., it created business profits for Russian companies.

The following lines are intended to show how Moscow seeks influence in Ukraine. They show how Russia actively exported technology, laws, and practices to Crimea, Donetsk, and Luhansk, to bring the information space under its control and to consequently exert influence.

Crimea

[40] Alfa Bank, "Mikhail Fridman," 2020, https://alfabank.com/members/mikhail-fridman/; Max Seddon, "MTS Sells Ukrainian Unit as It Focuses on Russia," November 25, 2019, https://www.ft.com/content/4a5a21ee-0f9b-11ea-a7e6-62bf4f9e548a.

The major events that triggered Russian action occurred in February 2014. After days of anti-government protests, Ukrainian president Yanukovych fled Kiev in the night-time of 21 February 2014.[41] Only a few days later, on 27-28 February pro-Russian forces took over critical buildings in Crimea's capital, Simferopol.[42] On 2 March 2014, Vladimir Putin stated that "… in the eastern regions of Ukraine and Crimea, Russia reserves the right to protect its interests and the Russian-speaking population living there."[43] In information control terms, Russia defended its interests by seizing key telecommunications buildings in Crimea and started to interfere in communications of Ukrainian members of parliament on 3 and 4 March. Then head of Ukraine's SBU security service [Ukraine's main government counterintelligence agency] Valentyn Nalivaichenko, witnessed the effects of the Russian seizure:

> "I confirm that an IP [Internet Protocol]-telephonic attack is under way on mobile phones of members of Ukrainian parliament for the second day in row…At the entrance to (telecoms firm) Ukrtelecom in Crimea, illegally and in violation of all commercial contracts, was installed equipment that blocks my phone as well as the phones of other deputies, regardless of their political affiliation."[44]

In other words, Russia started to actively disrupt information that it saw could hurt its strategic interests – information of high-ranking Ukrainian officials. This applied to Ukrainian websites too. Digital Security Lab Ukraine, an NGO, found through network measurements in Sevastopol and Simferopol, that websites that are accessible in Russia have been blocked in Crimea, which could indicate that censorship in Crimea is even

---

[41] Tim Judah, *In Wartime: Stories from Ukraine* (Great Britain: Penguin Random House UK, 2015).
[42] BBC News, "Ukraine Crisis: Timeline," November 13, 2014, sec. Europe, https://www.bbc.com/news/world-middle-east-26248275.
[43] The President of Russia, "Телефонный Разговор с Президентом США Бараком Обамой," March 2, 2014, http://kremlin.ru/events/president/news/20355.
[44] Pavel Polityuk and Finkle Jim, "Ukraine Says Communications Hit, MPs Phones Blocked," *Reuters*, March 4, 2014, https://www.reuters.com/article/us-ukraine-crisis-cybersecurity-idUSBREA231R220140304.

more stringent than in Russia, reflecting the tense strategic environment in the region.[45] Censorship is tailored towards Ukrainian news websites that provide a different viewpoint from Russian state media.[46]

At the same time Russia started laying internet cables to Crimea to increase the amount of data routed through Russia. Then Prime Minister Dmitry Medvedev underlined the important role that would fall onto Rostelecom, a Russian state-owned telecommunications company, in providing these services and building submarine cables to connect Russia and Crimea.[47] On 24 March 2014, he tweeted that: "It is necessary to ensure the early entry of Rostelecom in # Crimea. The transfer of important information to foreign companies is unacceptable."[48] About a week later, on 2 April, Roskomnadzor, Russia's chief agency tasked with censorship, established its office in Crimea employing 11 personnel.[49] On 25 April, Russia's Ministry of Communications declared that it had tasked Rostelecom to construct and operate a fibre optic cable on the bottom of the Kerch Strait.[50] On the same day, Rostelecom announced that it had completed the cables and that they are fully operational.[51] The corresponding Minister stated that this will allow

[45] Digital Security Lab Ukraine, "Crimea Has a Website Ban List Additional to Russia-Wide List, a Research Proves," *Medium*, September 20, 2018, https://medium.com/@cyberlabukraine/crimea-has-a-website-ban-list-additional-to-russia-wide-list-a-research-proves-4f20fa6fc762.
[46] Ibid.
[47] KM.RU, "Rostelecom Launches Cable Laid to Crimea," October 28, 2018, https://web.archive.org/web/20181028002313/http://www.km.ru/economics/2014/04/28/ministerstvo-svyazi-i-massovykh-kommunikatsii-rf/738619-rostelekom-zapustil-v-e.
[48] Dmitry Medvedev, "Дмитрий Медведев on Twitter," *Twitter*, March 24, 2014, https://twitter.com/MedvedevRussia/status/448048962474225664.
[49] Russian Ministry of Communications and Mass Media, "The Ministry of Communications of Russia Has Created the Territorial Administration of Roskomnadzor in Crimea," *Министерство Цифрового Развития, Связи и Массовых Коммуникаций Российской Федерации*, April 2, 2014, /ru/events/30092/.
[50] Russian Ministry of Communications and Mass Media, "Nikolai Nikiforov: 'FOCL Through the Kerch Strait Will Cover the Current Needs of Crimea in Communication Services,'" *Министерство Цифрового Развития, Связи и Массовых Коммуникаций Российской Федерации*, April 25, 2014, /ru/events/30028/.
[51] telecompaper, "Rostelecom Launches Fibre Link to Crimea," April 25, 2014, https://www.telecompaper.com/news/rostelecom-launches-fibre-link-to-crimea--1010208.

the peninsula to further integrate with Russia and allow for secure communications on the territory.[52] The Ministry also claimed that further cables are planned in the future to enhance connection with Russia.[53] However, according to Dyn, an internet infrastructure company, it took until 24 July that actual traffic flowed through the newly built Kerch Strait Cable.[54] What is more, since Crimea's annexation in 2014, all Russian information control laws apply directly in Crimea, making the supply of Russian norms direct and immediate. To give an example, Russia's internet sovereignty law, which went into effect on 1 May 2019, allows Russia to disconnect its domestic internet from the global network. In Russia's view, this applies to network operators in Moscow, St. Petersburg, just as it does to those in Crimea.[55]

In addition to the integration of the internet infrastructure and immediate applicability of laws, the Russian Ministry of Communications maintained that it would aid Crimea to switch to Russian internet domains, as well as encourage trainings to merge the Russian and Crimean IT [Information Technology] communities.[56] Alexei Volin, Deputy Minister of Telecom and Mass Communications, stated that common internet standards should be adopted to further allow for a seaming integration between the two entities.[57]

---

[52] Russian Ministry of Communications and Mass Media, "Nikolay Nikiforov."
[53] Ibid.
[54] Doug Madory, "No Turning Back: Russia Activates Crimean Cable," July 31, 2014, https://dyn.com/blog/no-turning-back-russia-crimea/.
[55] Russian Federation, "On Amendments to the Federal Law 'on Communications' and the Federal Law 'on Information, Information Technologies and the Protection of Information,'" May 1, 2019, https://sozd.duma.gov.ru/bill/608767-7.
[56] Russian Ministry of Communications and Mass Media, "Alexey Volin: 'Internet Security and Reliability Issues Are Now Key,'" *Министерство Цифрового Развития, Связи и Массовых Коммуникаций Российской Федерации*, April 7, 2014, https://digital.gov.ru/ru/events/30084/.
[57] Ibid.

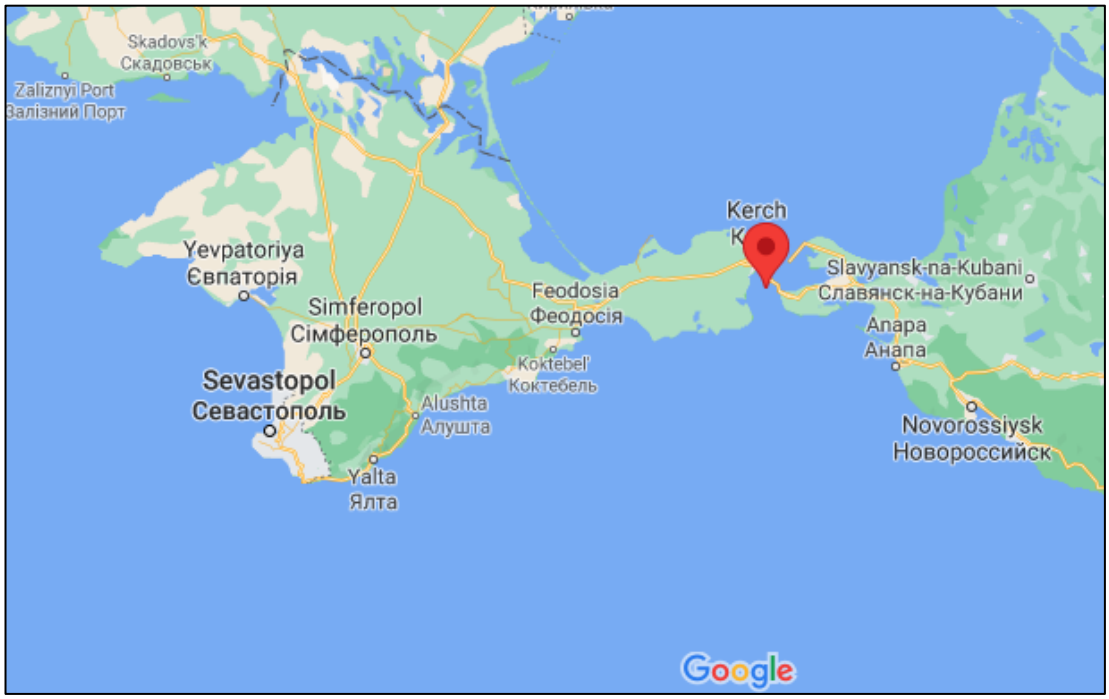


Figure 16: A map of Crimea and the Kerch Strait (highlighted with a red pin).[58]

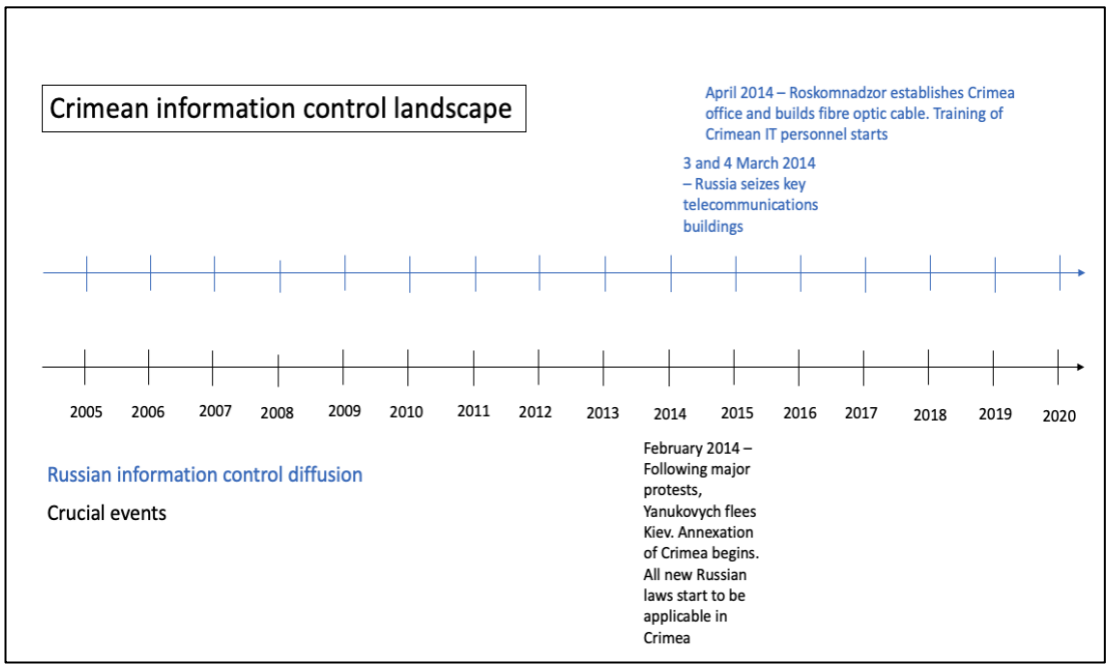


Figure 17: Crimean information control landscape

[58] Russian Ministry of Communications and Mass Media, "Alexey Volin: 'Internet Security and Reliability Issues Are Now Key,'" *Министерство Цифрового Развития, Связи и Массовых Коммуникаций Российской Федерации*, April 7, 2014, /ru/events/30084/.

Donetsk and Luhansk

In Donetsk and Luhansk, the information control integration with Russia has been less pronounced, since the two territories have not been formally annexed by Russia.[59] Keir Giles, a Russia expert, suggests that Donetsk and Luhansk may be even returned to Ukraine, if Kiev accepts Russia's annexation of Crimea.[60] Despite no formal annexation process, Russian troops are stationed in both entities and Russian experts exert key positions in the local governments.[61] As a consequence, many international experts believe that Donetsk and Luhansk are Russian puppet states.[62] In a similar vein, one could argue that the information control actions exerted in the two breakaway republics are in many ways Russian information controls that have diffused there.

On 11 May 2014, pro-Russian separatists in Donetsk declared independence after an internationally unrecognised referendum.[63] In September 2014, the Donetsk local government sent a letter to ISPs serving the territory to block specific Ukrainian websites from local subscribers in order to shield subscribers from "the spread of knowingly false information and slander."[64] The following year the Donetsk parliament established a blacklist, which mostly targets Ukrainian news websites.[65] On 30 May 2015, it passed the

[59] Sofia Cavandoli, "The Unresolved Dilemma of Self-Determination: Crimea, Donetsk and Luhansk," *The International Journal of Human Rights* 20, no. 7 (2016): 875–92.
[60] Giles, *Moscow Rules: What Drives Russia to Confront the West*.
[61] Wiliam H. Hill, "Unrecognized Actors from Unrecognized States: Moscow's Puppets or Inevitable Interlocutors" (European Leadership Network, November 2017), https://www.europeanleadershipnetwork.org/wp-content/uploads/2017/11/171117-William-H.-Hill-Unrecognized-Actors-from-Unrecognized-States.pdf.
[62] Ibid.
[63] BBC News, "Ukraine Crisis."
[64] The government letter was leaked to a journalist who scanned it and published it on social media. ZN.ua, "В Донбассе Заблокированы Сайты Ряда Проукраинских СМИ," *ZN.Ua*, September 30, 2014, https://zn.ua/TECHNOLOGIES/v-donbasse-zablokirovany-sayty-ryada-proukrainskih-smi-154664_.html.
[65] Global Voices, "Self-Proclaimed 'Donetsk People's Republic' Now Has an Internet Blacklist," June 17, 2015, https://globalvoices.org/2015/06/17/self-proclaimed-donetsk-peoples-republic-now-has-an-internet-blacklist/.

"Law On Information and Information Technologies" that calls for the establishment of a registry of URLs [Uniform Resource Locator] that are deemed undesirable and consequently are blocked.[66] The Donetsk parliament also passed a "Law on Mass Media", identical in name to the Russian Law on Mass Media.[67]

Censorship was not enough to control information in Donetsk. The territory has harboured a group posting anti-Ukrainian propaganda videos. Interestingly, the propaganda machine in Donetsk collaborates with the Internet Research Agency (IRA), a Russian troll factory in St. Petersburg. In particular, the IRA helps the Donetsk entity to produce fake videos and images.[68] On 1 March 2017, Donetsk and Luhansk separatist leaders declared that they would seize control over enterprises that are within Ukrainian jurisdiction.[69] On the same day Ukrtelecom, a major Ukrainian ISP, stated that it was impossible to provide further internet services in the future, due to illegal actions against its premises in Donetsk. It maintains that armed individuals have seized their offices and intervened in the operations of the ISP.[70] The Russian presidential spokesperson Dmitry Peskov commented on the seizure of premises in the Donbass by saying that the steps

---

[66] Government and the People's Council of the DPR, "The Next Meeting of the People's Council of the DPR," May 30, 2015, https://web.archive.org/web/20150530084135/http://dnr-online.ru/news/sostoyalos-ocherednoe-zasedanie-narodnogo-soveta-dnr-2/; Global Voices, "Self-Proclaimed 'Donetsk People's Republic' Now Has an Internet Blacklist."

[67] Government and the People's Council of the DPR, "The Next Meeting of the People's Council of the DPR"; Russian Federation, "The Law of the Russian Federation of 12.27.1991 N 2124-1 (as Amended on 01.03.2020) 'On the Mass Media,'" March 1, 2020, https://www.consultant.ru/document/cons_doc_LAW_1511/285787630b41d4963964c4c89fada1196a65cf3e/.

[68] Andrei Soshnikov, "Inside a Pro-Russia Propaganda Machine in Ukraine," *BBC News*, November 13, 2017, sec. BBC Trending, https://www.bbc.com/news/blogs-trending-41915295.

[69] Interfax - Ukraine, "Боевики ОРДЛО Вводят Внешнее Управление На Предприятиях Под Украинской Юрисдикцией На Временно Оккупированных Территориях - Источник," *Интерфакс-Украина*, March 1, 2017, https://interfax.com.ua/news/general/406251.html.

[70] СКМ, "ПАТ «Укртелеком» Повідомляє Про Неможливість Надання Абонентам Послуг Зв'язку На Непідконтрольній Частині Донецької Області Через Протиправні Дії Щодо Його Об'єктів На Цій Території," March 1, 2017, https://web.archive.org/web/20170309052617/https://www.scm.com.ua/uk/media-centre/news/view/2589/.

taken are reasonable.[71] Despite the seizure in 2017, it took until January 2019 for the process of full internet routing through Russia to take place.[72] In an interview with CNews, Minister of Communications of Donetsk Viktor Yatsenko stated that internet traffic now [January 2019] runs independently of Ukraine.[73]

The Luhansk governmental bodies have also avidly implemented Russian information control techniques. On 7 November 2014, the Luhansk parliament passed a law that is a copy paste of Russia's Law on Mass Media.[74] Section 4, for instance, is titled both in the Russian and in the Luhansk versions as "Inadmissibility of Abuse of Freedom of the Media".[75] The Ministry of Communications of Luhansk website has a section entitled "List of prohibited websites", which is password protected.[76] It had been reported previously that dozens of Ukrainian news websites are blocked by the ministry in order to shield citizens in the area from "destabilising information" published by these media.[77] Digital Security Lab Ukraine established, through network measurements of the internet

[71] РИА Новости, "В Кремле Заявили, Что Национализацию Заводов в ДНР и ЛНР Можно Понять," March 3, 2017, https://ria.ru/20170301/1489002715.html.
[72] Igor Korolev, "ДНР и ЛНР Полностью Переключили Магистральный Трафик На Россию," *CNews.Ru*, January 9, 2019, https://www.cnews.ru/news/top/2019-01-08_dnr_i_lnr_polnostyu_pereklyuchili_magistralnyj.
[73] Ibid.
[74] СКМ, "ПАТ «Укртелеком» Повідомляє Про Неможливість Надання Абонентам Послуг Зв'язку На Непідконтрольній Частині Донецької Області Через Протиправні Дії Щодо Його Об'єктів На Цій Території," March 1, 2017, https://web.archive.org/web/20170309052617/https://www.scm.com.ua/uk/media-centre/news/view/2589/.
[75] Luhansk People's Republic, "Luhan People's Republic of Law About the Media"; Russian Federation, "The Law of the Russian Federation of 12.27.1991 N 2124-1 (as Amended on 01.03.2020) 'On the Mass Media.'"
[76] Luhansk People's Republic, "Госкомнадзор Минкомсвязи ЛНР," *Министерство Связи и Массовых Коммуникаций Луганской Народной Республики*, 2020, https://mslnr.su/goskomnadzor.html.
[77] Tetyana Lokot, "Ukrainian Separatists Block 100+ News Websites in 'Lugansk People's Republic' · Global Voices," *Global Voices*, January 14, 2016, https://globalvoices.org/2016/01/14/ukrainian-separatists-block-100-news-websites-in-lugansk-peoples-republic/.

infrastructure, that 56 Ukrainian websites, mostly pertaining to human rights groups, NGOs, and local media were blocked in Luhansk.[78]

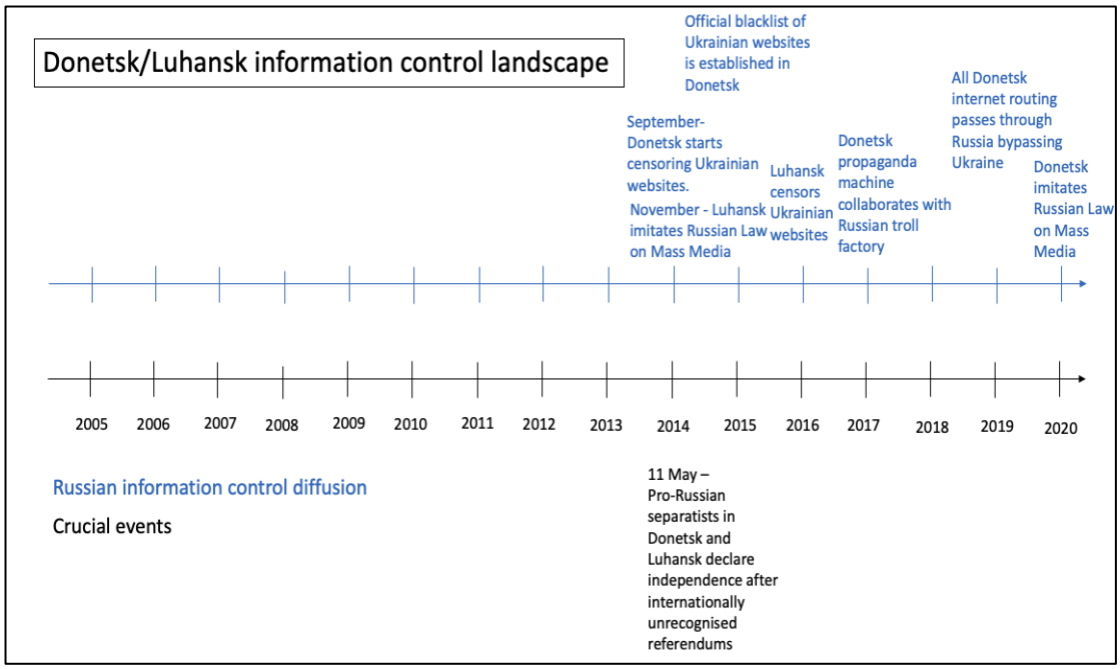


Figure 18: Donetsk/Luhansk information control landscape

7.2.2. Understanding the demand side of diffusion

By examining the cases of Belarus, Kazakhstan, Kyrgyzstan, Ukraine (pre-2014), and Uzbekistan – all CIS countries – this thesis sheds a light on the demand side of Russian internet sovereignty diffusion. Many surveillance laws in those countries copy paste the wording of Russian laws. Those are laws, that create an atmosphere of doubt and allow room for the intimidation of dissidents. The above-listed CIS countries thereby replicate Russia's emphasis on self-censorship, which makes this cyber norm distinct from the Chinese and American norms.

[78] Digital Security Lab Ukraine, "At Least 56 Ukrainian Websites Are Blocked in Luhansk, and Almost Nothing in Donetsk, Research Proves," *Medium*, September 21, 2018, 56, https://medium.com/@cyberlabukraine/at-least-56-ukrainian-websites-are-blocked-in-luhansk-and-almost-nothing-in-donetsk-a-research-c01577830b8e.

Belarus

For decades, Belarus has been a part of the Former Soviet Union, so it is natural that some surveillance practices mirroring Russia's have persisted into the 1990s and even until today. Belarus' closeness to the Russian surveillance apparatus can be seen within its surveillance bureaucracy. After the end of the Soviet Union, the Russian FSB renamed its surveillance department from OTU (Operativno-Technicheskoye Upravlenie, or Operative Technical Department) to UOTM (M stand for Measures).[79] However, Belarus retained the acronym OTU for its surveillance department.[80] Belarus also retained the FSB's term ORM to designate snooping operations (it stands for Operativno-Rozisknie Meropriatiya, or Operative-Search Measures.[81] Moreover, in 2002, Belarus modelled its cyber-crime fighting department within its Ministry of Interior after Russia's Department "K", which had been created in 1998.[82] These events above are just to show that Belarus had had information control cooperation with Russia pre-2010. The following lines show how, around major protests in 2010, the Russo-Belarusian cooperation has intensified. This highlights how information controls diffusion is propelled when threat perception increases.

In 2006, presidential elections took place in Belarus. These were followed by gatherings in Minsk of between 10,000-30,000 citizens that were displeased with the election

[79] Privacy International, "Lawful Interception: The Russian Approach."
[80] Ibid.
[81] President of the Republic of Belarus, "On Approval of the Regulation on the Procedure for the Interaction of Telecommunication Operators With Agencies Engaged in Operational-Search Activities," March 3, 2010, https://web.archive.org/web/20190104143950/http://oac.gov.by:80/files/files/pravo/ukazi/Ukaz_129.htm.
[82] ECPAT International, "REGIONAL OVERVIEW on Child Sexual Abuse Images through the Use of Information and Communication Technologies in Belarus, Moldova, Russia and Ukraine," September 2008, https://www.ecpat.org/wp-content/uploads/2016/04/regional_overview.pdf.

results.[83] These protests, dubbed the Denim Revolution, did not bring about any major political change (Lukashenko remains in power), but they did express dissatisfaction with the current regime. President Alexander Lukashenko took lessons from the 2006 election/protest year and issued the Decree No. 129 on 3 March 2010, just a few months before crucial presidential elections would take place on 19 December 2010.[84] The March decree, which closely imitates Russia's SORM surveillance regulations, may be seen as preparing the ground to expand surveillance in the election year.[85] Similarly to Russia, the law stated that from now on internet and mobile operators had to give direct and non-stop access to customer data to authorities, as well as acquire and maintain SORM equipment at their own cost.[86]

Resembling the events from 2006, in 2010, large-scale protests broke out, following the disputed elections, to which the government responded with a violent crackdown.[87] Amnesty International, a non-profit organisation, concluded 50 interviews with Belarusian activists and concluded that "[t]he use of surveillance of mobile phone and internet data to track the identities of protestors and to prosecute opposition political leaders and others was a significant feature of this crackdown."[88] Authorities, for instance, used data gained from surveillance of private communications to incriminate

[83] Margot Letain, "The 'Denim Revolution': A Glass Half Full," *OpenDemocracy*, April 10, 2006, https://www.opendemocracy.net/en/denim_3441jsp/.
[84] President of the Republic of Belarus, "On Approval of the Regulation on the Procedure for the Interaction of Telecommunication Operators With Agencies Engaged in Operational-Search Activities"; Miriam Elder, "Clashes in Belarus After Thousands Turn out in Protest at Alleged Vote-Rigging," *The Guardian*, December 20, 2010, sec. World news, https://www.theguardian.com/world/2010/dec/20/belarus-protest-alleged-vote-rigging.
[85] Amnesty International, "'It's Enough for People to Feel It Exists,'" 2016, https://www.amnesty.org/en/documents/eur49/4306/2016/en/.
[86] President of the Republic of Belarus, "On Approval of the Regulation on the Procedure for the Interaction of Telecommunication Operators With Agencies Engaged in Operational-Search Activities."
[87] Amnesty International, "'It's Enough for People to Feel It Exists.'"
[88] Ibid.

political candidates and activists in the months following the 2010 elections.[89] In 2011, president Lukashenko summed up his view on the intersection of protests and digital technologies. At a Collective Security Treaty Organization meeting (CSTO) he said:

"Many new goals have appeared in light of recent world events, including those in the Arab states and in North Africa…We [CSTO] have agreed that our countries will work out measures to fight potential threats, primarily in the information sphere and cyber space."[90]

To comply with government laws, Belarusian operators have acquired DPI technology (Deep Packet Inspection technology; used for online filtering and surveillance) since at least 2011.[91] They have purchased, for instance, DPI tools from VAS Experts, which has been deployed in the cities of Brest, Grodno, Ivanava, Minsk, and Vitebsk.[92] For its part, the Belarusian Ministry of Internal Affairs purchased technology from Analytical Business Solutions, a Russian firm that specialises in increasing the efficiency of online monitoring.[93]

Furthermore, the Russian Academy of Information Systems (AIS) hosts Belarusian cyber security professionals for regular training in this field.[94] According to Tatyana Halyavina,

[89] Ibid.
[90] Joshua Kucera, "With Eye To Arab Spring, CSTO Strengthens Cyber, Military Powers," *Eurasianet*, August 15, 2011, https://eurasianet.org/with-eye-to-arab-spring-csto-strengthens-cyber-military-powers.
[91] Mikhail Doroshevich and Maria Sokolova, "Internet Development and Usage," in *Belarusian Yearbook 2012*, ed. Anatoly Pankovsky and Valeria Kostyugova (Minsk: Belarusian Institute for Strategic Studies, 2013).
[92] VAS Experts, "About Us."
[93] 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.
[94] Daniyar Moldabekov, "Евразийский Киберсоюз - Аналитический Интернет-Журнал Власть," *VLAST*, December 19, 2019, https://vlast.kz/obsshestvo/31791-evrazijskij-kibersouz.html.

head of the AIS, around two to three people from Belarus attend the courses at the academy every two months.[95]

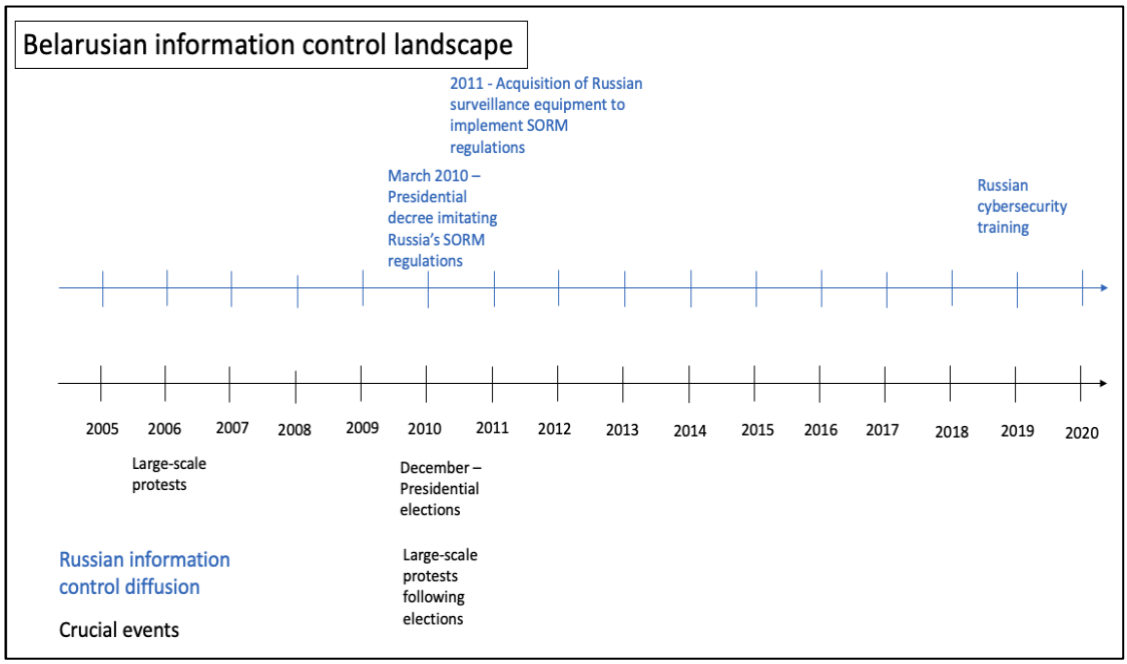


Figure 19: Belarusian information control landscape

Kazakhstan

Kazakhstan has one of the most effective collaborations with the Russian Federal Security Service, according to its former Director Nikolai Patrushev.[96] What is more, for years after the fall of the Soviet Union, the republic's KGB officers (KGB stands in English for Committee for State Security and was the Soviet Union's principal security agency) continued to staff Kazakhstan's intelligence agency, the KNB (also known as National Security Committee of the Republic of Kazakhstan).[97] As a consequence, the behaviours

[95] Ibid.
[96] Stéphane Lefebvre and Roger N Mcdermott, "Russia and the Intelligence Services of Central Asia," *International Journal of Intelligence and CounterIntelligence* 21, no. 2 (2008): 251–301.
[97] Ibid.

and customs of the KGB continued to linger within Kazakh security services[98] and maybe also because of this, Kazakhstan's information controls now continue to resemble those of Russia.

Kazakhstan's surveillance laws have some resemblance with the Russian SORM model. Article 15 of the country's 2004 Communication Law, for instance, states that telecommunication network operators ought to provide assistance to special investigative authorities and access to service subscribers' information.[99] Similarly to SORM, Investigation of authorities and communication interception may be carried out without the knowledge of network operators.[100]

The Arab Spring resonated with Kazakh leaders. In 2011, at a CSTO meeting, Kazakhstan's former president Nursultan Nazarbaev mentioned the need to establish an "impregnable wall", i.e., tighter control of the information environment, to avoid revolutions – such as those that shook the Middle East – in Central Asia. Nazarbaev stated that an unregulated cyberspace translated into "threats to regional security and stability in the CSTO member states, especially in light of the latest developments in the world."[101] In 2012, Nazarbaev also enshrined national security and domestic political stability as the number one and two priorities in the long term within its "Kazakhstan 2030" strategy.[102]

---

[98] Roger McDermott, "Central Asian Security Post - 2014" (Danish Institute for International Studies, 2013), https://www.diis.dk/files/media/publications/import/extra/rp2013-12-mcdermott-kazakhstan_web.jpg_1.pdf.

[99] Ministry of Justice of the Republic of Kazakhstan, "Law on Communications," July 5, 2004, http://adilet.zan.kz/eng/docs/Z040000567_.

[100] Telecommunications Industry Dialogue, "Provision of Real-Time Lawful Interception Assistance," June 2015, https://www.telecomindustrydialogue.org/resources/kazakhstan/.

[101] Roger McDermott, "CSTO Moves Into The Information Age," *RadioFreeEurope/RadioLiberty*, September 4, 2011, https://www.rferl.org/a/commentary_csto_moves_into_information_age/24317363.html.

[102] The General Prosecutor's Office of the Republic of Kazakhstan, "The Strategy «Kazakhstan 2030»," April 9, 2012, http://prokuror.gov.kz/eng/state/acts-president/strategy-kazakhstan-2030.

Kazakhstan mimicked Russia when it comes to personal data laws. On 21 July 2014, Russia passed the Amendments to the Personal Data Law, also known as Federal Law No. 242 "On Amending Certain Legislative Acts of the Russian Federation with regard to clarifying the processing of personal data in information and telecommunication networks".[103] The law stipulates that:

"When collecting personal data, including through the information and telecommunication network Internet, the operator is obliged to record, organize, accumulate, store, clarify (update, change), extract personal data of citizens of the Russian Federation using databases located on the territory of the Russian Federation."

Only a year later, on 26 November 2015, Kazakhstan published its own amendments to the law "On Personal Data and Protection Thereof", titled "On Amendments to Certain Legislative Acts of the Republic of Kazakhstan on Informatization".[104] Article 12 of the law states that any personal data on Kazakh citizens must be stored within Kazakhstan:

"Storage of personal data is carried out by the owner and (or) operator, as well as by a third party in the database, which is stored on the territory of the Republic of Kazakhstan."

Then in 2018, updated SORM regulations allegedly went into effect, which considerably increased the surveillance powers of Kazakhstan.[105] Telia, a Swedish network operator, had to comply with the regulations and warned of its effects on digital human rights, since the new regulations "allow government authorities real-time access to the networks of

[103] Russian Ministry of Communications and Mass Media, "Обработка и хранение персональных данных в РФ. Изменения с 1 сентября 2015 года :," *Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации*, September 2015, https://digital.gov.ru/ru/personaldata/.
[104] DAC Beachcroft, "Kazakhstan - Localization of Personal Data," January 12, 2016, https://www.lexology.com/library/detail.aspx?g=303621d9-e5b7-4115-9d8c-2a5d1d40ed2c.
[105] President of the Republic of Belarus, "On Approval of the Regulation on the Procedure for the Interaction of Telecommunication Operators With Agencies Engaged in Operational-Search Activities."

telecommunications operators without making specific or periodic demands to the operator."[106]

Kazakhstan bought deep packet inspection technology from VAS Experts, a company based in St. Petersburg.[107] 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.[108] The Kazakh Ministry of Emergency Situations also acquired Semantic Archive, an information analysis platform provided by Analytical Business Solutions.[109] In 2017, Kazakhtelecom, Kazakhstan's largest telecommunications company, and Solar Security, a Russian cyber security company, signed a memorandum in which they vow to establish a centre to monitor and respond to cyberattacks.[110] In 2018, the BBC reported that Digital Revolution, a Russian hacker group, claimed to have hacked into Quantum Research Institute, a supplier of the Russian FSB.[111] The documents published by Digital Revolution group show that the Russian Quantum Research Institute has provided a "monitoring system for social networks, the main purpose of which is the analysis of protest moods", to Kazakhstan.[112] In a further sign of reliance on Russia, Kazakhstan's technical standard with regards to

---

[106] Telia, "Respecting Freedom of Expression - Telia Company's View on New Surveillance Regulation ('Direct Access') in Kazakhstan," May 10, 2017, https://www.teliacompany.com/en/news/news-articles/2017/freedom-of-expression-kazakhstan/.

[107] VAS Experts, "About Us."

[108] 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."

[109] Analytical Business Solutions, "Semantic Archive."

[110] Бауржан Муканов, "Центр Мониторинга и Реагирования На Кибератаки Создадут Казахстан и Россия," April 27, 2017, https://informburo.kz/novosti/centr-monitoringa-i-reagirovaniya-na-kiberataki-sozdadut-kazahstan-i-rossiya.html.

[111] Андрей Сошников and Андрей Захаров, "'Стоп-слово' - Навальный. Хакеры разоблачили 'проект ФСБ' в соцсетях," *BBC News Русская служба*, December 20, 2018, sec. Подробности, https://www.bbc.com/russian/features-46621322.

[112] Ibid.

cryptographic information security (GOST R 34.11-2015) was initially developed by the FSB's Information Security and Special Communications Centre as well as the InfoTex OJSC, a large Russian company, that focusses on the production of information security software.[113] Moreover, the Russian Academy of Information Systems trains Kazakh cyber security professionals.[114] In 2018, another Russian company Positive Technologies, signed a memorandum with the KNB to exchange knowledge in the field of information security.[115]

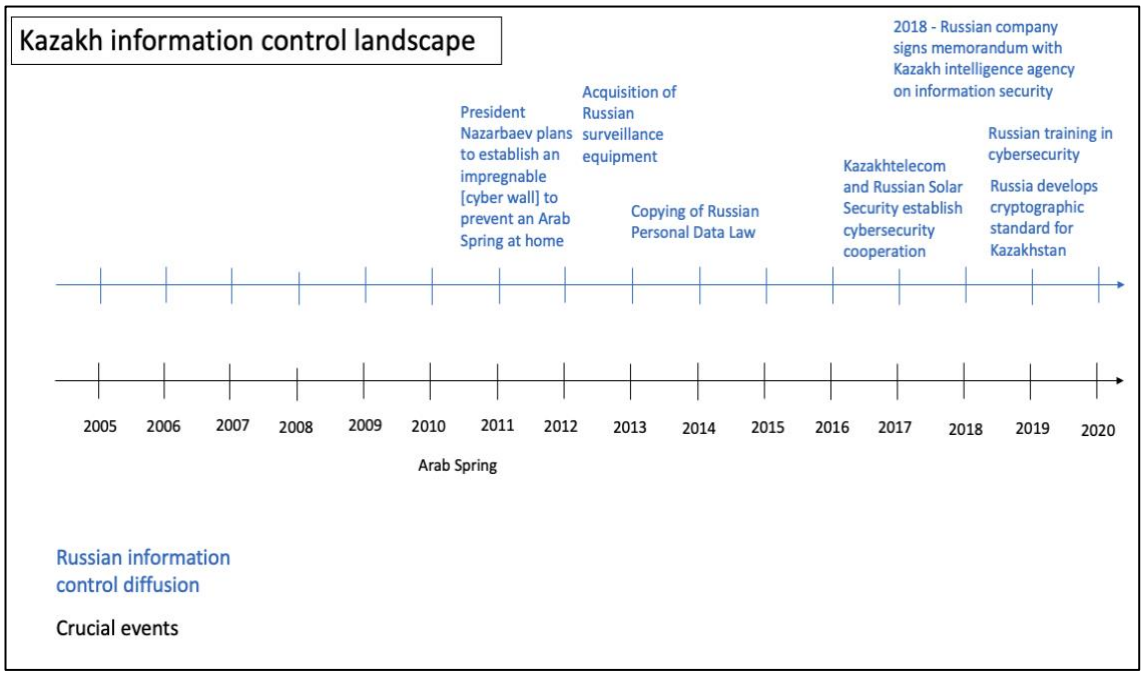


Figure 20: Kazakh information control landscape

Kyrgyzstan

According to Dmitry Gorenburg: "Internal instability is the greatest threat to Kyrgyzstan."[116] A major uprising took place in 2007 against the regime of former

[113] Moldabekov, "Евразийский Киберсоюз - Аналитический Интернет-Журнал Власть."
[114] Ibid.
[115] Ibid.
[116] Gorenburg, "External Support for Central Asian Military and Security Forces."

president Kurmanbek Bakiyev.[117] Only one year later, in 2008, Kyrgyzstan's main intelligence agency, the GKNB (State Committee on National Security) started to install Russian SORM equipment.[118] SORM equipment was acquired from Russian companies, such as Oniks-Line and Signatek.[119] In 2010, protests, organised also via social media, shook Kyrgyzstan. The government started to feel the pressure emanating from the internet (e.g., videos were being posted online of government violence) and as a result began to bully online news discussion forums, such as Diesel Forum, into censoring content. However, the authorities' measures were unsuccessful. The protests lead to an overthrow of the government in 2010.[120] In a research paper, Neil Melvin and Tolkun Umaraliev state that "new media made a significant contribution to the protests that were eventually to topple President Bakiyev…"[121] They further claim that the Bakiyev regime has had difficulties to "track and disrupt the rapidly changing information environment."[122] In 2012, the Defense and Security Committee of the Kyrgyz parliament stated that Russian equipment should be given priority in connecting the country's monitoring centres and Internet Service Provider networks.[123] In August of the same year, the State Committee for National Security of the Kyrgyz Republic published a draft of a

[117] Ibid.
[118] Eurasianet, "Kyrgyzstan: Bishkek Snoops Relying on Russian Spyware," November 7, 2012, https://eurasianet.org/kyrgyzstan-bishkek-snoops-relying-on-russian-spyware.
[119] 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/.
[120] Neil Melvin and Tolkun Umaraliev, "New Social Media and Conflict in Kyrgyzstan," SIPRI Insights on Peace and Security (Stockholm: SIPRI, August 2011), https://www.sipri.org/sites/default/files/files/insight/SIPRIInsight1101.pdf.
[121] Neil Melvin and Tolkun Umaraliev, "New Social Media and Conflict in Kyrgyzstan," SIPRI Insights on Peace and Security (Stockholm: SIPRI, August 2011), https://www.sipri.org/sites/default/files/files/insight/SIPRIInsight1101.pdf: 22.
[122] Ibid: 19.
[123] Soldatov and Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You."

regulation on its website that is practically a copy-paste of the Russian communication interception regulations.[124]

In 2014, an anti-LGBT [Lesbian, Gay, Bisexual, and Transgender] propaganda law was proposed in the Kyrgyz parliament, which followed the example of Russia's "gay propaganda law" signed by president Putin in June 2013.[125] The Russian law, which covers traditional newspapers just as modern social media, stipulates that it is forbidden to provide children with insight into the life of LGBT people.[126] Also in 2014, a new resolution was issued that urged Internet Service Providers to comply with an updated SORM system. Under the resolution, ISPs ought to store customer data for up to three years, with direct access and no judiciary oversight.[127]

Vega Radio Engineering Corporation, a Moscow-based entity, built a smart city in Bishkek.[128] It provided the city with traffic surveillance cameras that are able to check, for example, number plates against databases. According to the Ministry of Internal Affairs of the Kyrgyz Republic, the plan is to install 110 hardware and software systems in mobile complexes, at roads in Bishkek, on border crossings and roads that lead to

---

[124] Kyrgyz Republic's State Committee for National Security, "Об Утверждении Правил Внутреннего Распорядка Изоляторов Временного Содержания Органов Национальной Безопасности Кыргызской Республики," August 17, 2012, https://web.archive.org/web/20130902225513/http://www.gknb.kg/index.php?option=com_content&view=category&layout=blog&id=29&Itemid=57.

[125] European Parliament, "JOINT MOTION FOR A RESOLUTION on Kyrgyzstan, Homosexual Propaganda Bill," January 14, 2015, https://www.europarl.europa.eu/doceo/document/RC-8-2015-0054_EN.html.

[126] Russian Federation, "Федеральный закон о защите детей от пропаганды гомосексуализма," *Российская газета*, June 29, 2013, https://rg.ru/2013/06/30/deti-site-dok.html.

[127] Kyrgyz Ministry of Justice, "Инструкция о Порядке Взаимодействия Операторов Электросвязи и Операторов Мобильной Сотовой Связи с Государственными Органами Кыргызской Республики, Осуществляющими Оперативно-Розыскную Деятельность," June 30, 2014, https://web.archive.org/web/20191026180458/http://cdb.minjust.gov.kg:80/act/view/ru-ru/96622.

[128] Vega, "The System of Photo-Video Recording of Traffic Violations 'Prism,'" accessed May 18, 2020, http://vega.su/production/detail.php?ID=2301.

Bishkek International Airport.[129] The system officially went into effect in February 2019.[130]

Regarding strategic information dissemination, the Kyrgyz landscape reminds fake news researchers of the one in Russia, rather than China. However, it is difficult to precisely pinpoint a resemblance of the Kyrgyz propaganda landscape to either Russia, where the Internet Research Agency is active, or China, which is known for its 50 Cent Army.[131]

Finally, some of Kyrgyzstan's international internet connections run through Kazakhstan, which is tied to Russian cables. This means that websites blocked in Russia are also intermittently blocked in Kazakhstan and Kyrgyzstan. Russian information control policies consequently have a reach beyond its borders, due to the technical infrastructure of the internet.[132] Russia also maintains a signals centre in Kara-Balt, northern Kyrgyzstan, which is used for electronic surveillance, amongst other activities.[133]

[129] Ministry of Interior of the Kyrgyz Republic, "Safe City," accessed May 18, 2020, http://www.guobdd.kg/safecity.
[130] Юлия КОСТЕНКО, "«Безопасный Город». Где Установлены Видеокамеры Для Фиксации Нарушений," *24.Kg*, May 14, 2019, https://24.kg/obschestvo/114794_bezopasnyiy_gorod_gde_ustanovlenyi_videokameryi_dlya_fiksatsii_narusheniy/.
[131] Interview with Christopher Schwartz, journalist based in Bishkek, and Rebekah Overdorf, internet researcher focussed on Central Asia, on 20 May 2020. We discussed their recent paper on Kyrgyzstan. Christopher Schwartz and Rebekah Overdorf, "Disinformation from the Inside: Combining Machine Learning and Journalism to Investigate Sockpuppet Campaigns," *Companion Proceedings of the Web Conference 2020*, Taipei, Taiwan, doi:https://doi.org/10.1145/3366424.3385777.
[132] Freedom House, "Kyrgyzstan," 2019, https://freedomhouse.org/country/kyrgyzstan/freedom-net/2019.
[133] Gorenburg, "External Support for Central Asian Military and Security Forces."

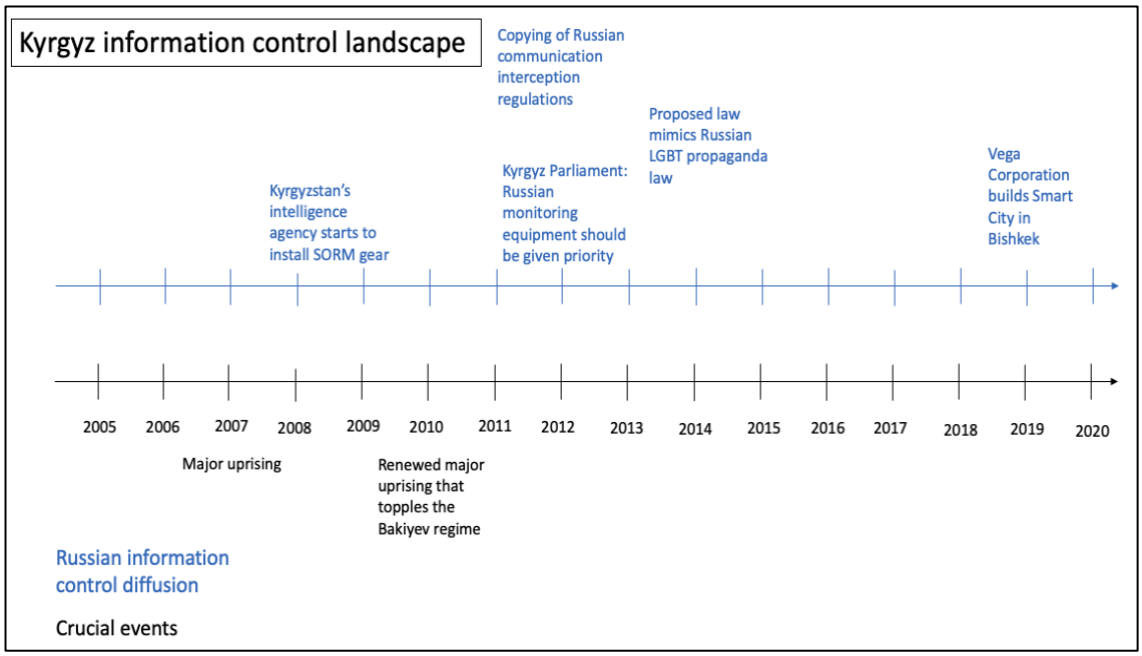


Figure 21: Kyrgyz information control landscape

Ukraine

Until its major spat with Russia in 2014, Ukraine had maintained close knit relations with the Russian security organs.[134] In addition to this, its intelligence agencies were infiltrated with hundreds of spies loyal to Moscow.[135] Even its former counterintelligence chief was arrested in 2014 for similar suspicions.[136] There was such close cooperation between the two countries' law enforcement/intelligence agencies that when Russia, for instance, instituted a Department "K" in 1998 within its Ministry of Internal Affairs to fight "computer crime", Ukraine established a similar specialised unit within its respective

[134] And except a short period after the Orange revolution between 2005-2010 where relations were sour. Christopher Miller, "Ukraine's Top Intelligence Agency Deeply Infiltrated by Russian Spies," *Mashable*, accessed June 2, 2020, https://mashable.com/2014/12/30/russian-vs-ukrainian-spies/; 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): 516.

[135] Miller, "Ukraine's Top Intelligence Agency Deeply Infiltrated by Russian Spies."

[136] Radio Free Europe/Radio Liberty, "Ukraine Arrests Ex-Chief of Counterintelligence," November 10, 2014, https://www.rferl.org/a/treason-ukraine-bik-arrest-counterintelligence/26683395.html.

ministry in 2002.[137] The establishment of this unit follows major protests that called for the stepping down of then president Leonid Kuchma in 2000-2001.[138] In 2004, major protests led to a peaceful regime change in Ukraine, bringing Viktor Yushchenko to power.[139] In 2009, then president Viktor Yushchenko passed a decree that aimed at implementing an information security doctrine within the country that is very similar to the Russian information security doctrine of the year 2000.[140]

Ukraine also acquired SORM equipment from the Russian company VAS Experts, whose DPI tools are deployed to monitor internet traffic in Kiev and Kharkov.[141] Victor Shlyapobersky, a leading figure in St. Petersburg's regional SORM testing facility of the Central Research Institute of Communications stated that "the Ukrainian SORM is tougher [than the Russian] – they have the right to interrupt the conversation and we have no such powers."[142] SORM compatible equipment became crucial in Ukrainian politics during the 2014 Maidan protests. It was allegedly used to intercept a call between Geoffrey Pyatt, former US ambassador to Ukraine and Victoria Nuland, the US Assistant Secretary of State for Europe.[143] The interception was possible because Pyatt had used an ordinary cell phone that established an unencrypted call to Nuland.[144] During the

[137] ECPAT International, "REGIONAL OVERVIEW on Child Sexual Abuse Images through the Use of Information and Communication Technologies in Belarus, Moldova, Russia and Ukraine"; Vladimir Golubev, "Fighting Cybercrime in CIS: Strategy and Tactics," *Computer Crime Research Center*, June 29, 2005, http://www.crime-research.org/articles/golubev_Jul/.
[138] Human Rights Watch, "Ukraine," 2003, https://www.hrw.org/reports/2003/ukraine0303/Ukraine0303.pdf.
[139] Council on Foreign Relations, "Ukraine's Post-Independence Struggles," 2020, https://www.cfr.org/timeline/ukraines-post-independence-struggles.
[140] President of Ukraine, "Про Доктрину інформаційної безпеки України," *Законодавство України*, July 8, 2009, https://zakon.rada.gov.ua/go/514/2009.
[141] VAS Experts, "About Us."
[142] Soldatov and Borogan, *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*: 516.
[143] 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): 512.
[144] Ibid.

conversation, which was later leaked mysteriously to several recipients that had uploaded it online, Nuland said "Fuck the EU", expressing her frustration over the EU's approach to managing the political situation in Ukraine.[145] In addition to this, she voiced her opinion on who should succeed the then disputed Ukrainian government.[146]

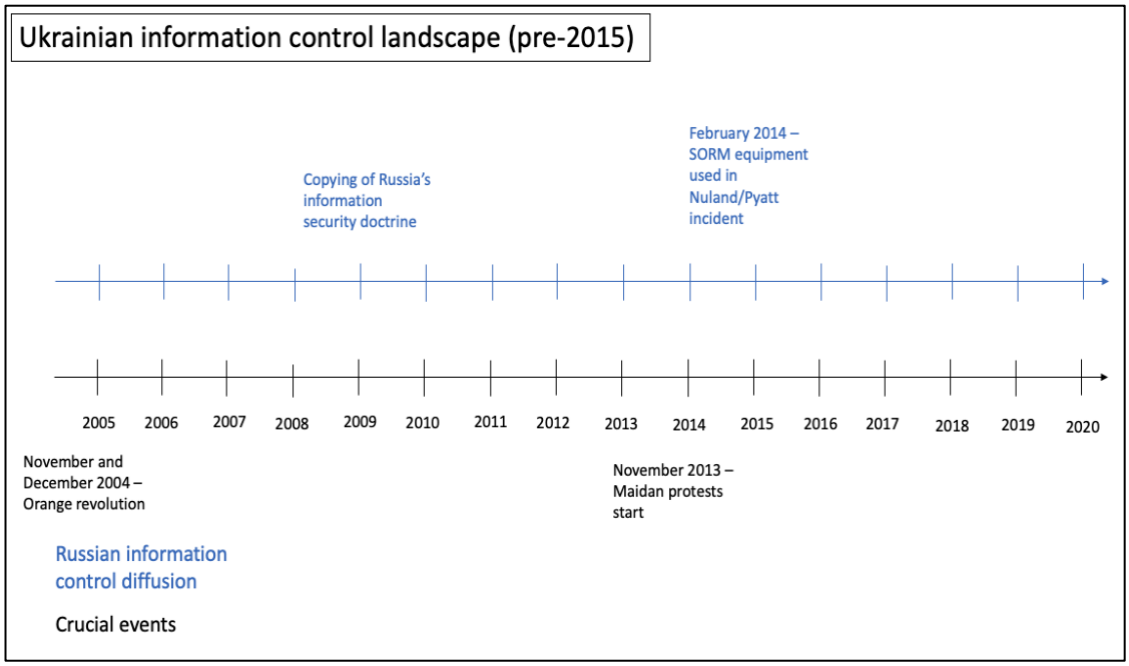


Figure 22: Ukrainian information control landscape (pre-2015)

Uzbekistan

Uzbekistan has long-rooted surveillance ties with Russia. It goes back as far as 1992, when the newly founded state entered an agreement of intelligence sharing and cooperation on operations and investigations with other intelligence agencies of the CIS countries.[147] Its intelligence agency, the National Security Service, is central to Uzbekistan's domestic surveillance programme. Since the end of the Soviet Union, it has

[145] BBC News, "Transcript of Leaked US Ukraine Call," February 7, 2014, sec. Europe, https://www.bbc.com/news/world-europe-26079957.
[146] Ibid.
[147] Lefebvre and Mcdermott, "Russia and the Intelligence Services of Central Asia."

not changed much and is still very similar to the former Uzbek Republic's KGB department.[148]

On the one hand, Uzbekistan was concerned by the Arab Spring, in which social media played a prominent role. Uzbekistan imposed a complete news blackout on the topic of the Arab Spring in 2011.[149] At the same time, Uzbekistan imported Russian technology and laws to implement surveillance. It acquired 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.[150] In 2012, the Uzbek government instituted the law on "Operational Investigative Activity", which mimics Russia's law on state surveillance.[151] Like in Russia, there is a lack of independent oversight to access citizen's data through the Russian provided SORM-technology and there is no need to obtain judicial authorisation for surveillance even on individuals that are not subject to a criminal investigation.[152]

Uzbekistan's domestic surveillance programme is at least partly a product of the ruling elite's regime survival concerns, since many of the surveillance campaigns are "targeted against individuals that are of political interest to Uzbekistan."[153] This can be seen in the

---

[148] Ibid.

[149] Muhammad Tahir, "Governments Move To Thwart 'Arab Spring' In Central Asia," *Radio Free Europe / Radio Liberty*, April 28, 2011, https://www.rferl.org/a/governments_move_to_thwart_arab_spring_in_central_asia/16796618.html.

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

[151] Borogan and Soldatov, "Just Business"; The Russian Federation (State Duma), "Федеральный Закон 'Об Оперативно-Розыскной Деятельности' От 12.08.1995 N 144-ФЗ (Последняя Редакция)," August 12, 1995, https://www.consultant.ru/document/cons_doc_LAW_7519/; Republic of Uzbekistan, "Об Оперативно-Розыскной Деятельности," December 2012, https://lex.uz/docs/2106527.

[152] Human Rights Watch, "The Right to Privacy in Uzbekistan"; Peter Roudik, "ECHR, Russian Federation: Breaches of Human Rights in Surveillance Legislation |," *Global Legal Monitor*, March 2, 2016, //www.loc.gov/law/foreign-news/article/echr-russian-federation-breaches-of-human-rights-in-surveillance-legislation/.

[153] Interview with Etienne, Threat Intelligence Analyst, on 10 April 2020.

lead intelligence agency (National Security Service) allegedly targeting important political figures, such as the daughter and potential successor to her father, the long-term dictator Islam Karimov, Gulnara Karimova.[154] The intelligence agency has also hacked several Uzbek human rights and political activists.[155]

At the same time, influential media figures became targets of cyberattacks. In 2014, Galima Bukharbaeva, a former journalist of government critical UzNews, discovered that she was hacked, and her e-mails released on Russian social networks. She suspects that it was a Russian actor who was upset about UzNews's coverage of the conflict in Ukraine.[156] The personal attack on her had reached its purpose – Galima went into exile, and UzNews ceased to exist. In 2016, another hacking campaign against critical voices in Uzbekistan was launched.[157] The start of the campaign coincided with a major political event – the death of former Uzbek president Karimov. A week before the Uzbek government announced the death of Karimov, the event had already been reported by Fergana News.[158] The publishing of this major political event without the government's approval made Fergana News an ideal target of the ensuing hacking campaign. Journalists and human rights defenders were targeted with "Bedep", a backdoor that has also been used in previous cybercrime campaigns.[159] Interestingly, many of the domains and tools used were Russian, such as Pochta.top (mimicking the Russian Post's domain), auth.yandex.ru.my-id.top (imitating Russian search engine Yandex), drw.sh (url

[154] Privacy International, "Private Interests: Monitoring Central Asia."
[155] Sean Lyngaas, "How Uzbekistan's Security Service (Allegedly) Began Developing Its Own Malware," *CyberScoop*, October 3, 2019, https://www.cyberscoop.com/uzbekistan-sandcat-kaspersky/.
[156] Amnesty International, "We Will Find You Anywhere," 2017, https://www.amnesty.org/download/Documents/EUR6259742017ENGLISH.PDF.
[157] Equalit.ie, "Deflect Labs Report #6: Phishing and Web Attacks Targeting," May 9, 2019, https://equalit.ie/deflect-labs-report-6/.
[158] Interview with Etienne.
[159] Cristopher Budd, "Angler: The Rise and Fall of an Exploit Kit," *Trend Micro*, September 14, 2016, https://blog.trendmicro.com/angler-rise-fall-exploit-kit/.

shortener tool, owned by a Russian security company Doctor Web).[160] Many e-mail addresses to register domains during this campaign were also used during previous Bedep campaigns, which indicates a nexus between previous cybercrime campaigns and this surveillance one.[161] One interviewee confirms this observation and mentions that they have "seen some attacks targeting activists and at the same time the attack servers were used for fake bank websites."[162] Interestingly, Bedep was also used in 2015 to inflate the number of views of pro-Russian propaganda videos on YouTube.[163]

Then in 2019, Kaspersky Lab, a Russian anti-virus company, reported that Uzbekistan's spy agency had attacked dissidents with commercially available hacking tools, which were used in other hacking campaigns on dissidents.[164] While it is uncertain who exactly was behind the various surveillance campaigns in Uzbekistan, they show a strong dependence on Russian internet services. And also, the nexus between (private) cybercrime campaigns and (potentially state-sponsored) surveillance campaigns is very reminding of the Russian information control landscape. In both Uzbekistan and Russia, criminal groups, have been "often close to the government during this kind of targeted attacks [on human rights groups]."[165]

[160] Equalit.ie, "Deflect Labs Report #6: Phishing and Web Attacks Targeting."
[161] Ibid.
[162] Interview with Etienne.
[163] Kogan Rami, "Bedep Trojan Malware Spread by the Angler Exploit Kit Gets Political," *Trustwave*, April 29, 2015, https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/bedep-trojan-malware-spread-by-the-angler-exploit-kit-gets-political/.
[164] Jack Stubbs, "Uzbek Spies Attacked Dissidents With Off-The-Shelf Hacking Tools," *Reuters*, October 3, 2019, https://www.reuters.com/article/us-uzbekistan-cyber-idUSKBN1WI0YL.
[165] Interview with Etienne.

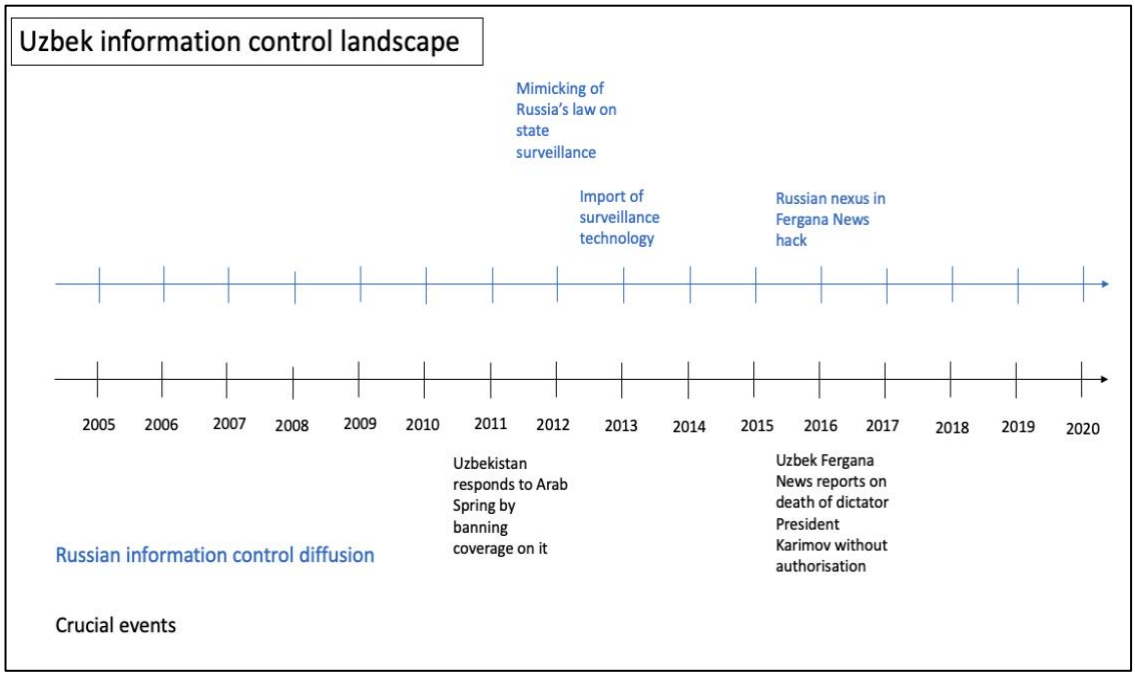


Figure 23: Uzbek information control landscape

7.3. Variation in the dependent variable

This thesis has previously looked at Ukraine pre-2015 and compares it now to Ukraine post-2014. Ukraine post-2014 is not that different from Ukraine pre-2015. Its geographical location has not changed, its culture, history, or structure of the economy did not change either. Why then, did the diffusion of Russian information control come to a halt?

The Maidan protests in 2014, and the ensuing Russian invasion of Ukraine changed the overarching threat priorities in Ukraine. A Russian invasion in Crimea and Russian backing of pro-Russian separatists in Luhansk and Donetsk threatened Ukraine's Westphalian sovereignty. Of course, the leaders in Kiev were still concerned about mass protests challenging their regime, but rather than seeking assistance from Russia, which

challenged Ukraine's territorial integrity, leaders sought surveillance help from China.[166] In 2017, for example, Hikvision and Huawei supplied 4,100 surveillance cameras to transform Kiev into a smart city.[167]

Russia's annexation of Ukrainian territory in 2014 induced a major split in Ukrainian-Russian information control landscapes. Several measures were put in place to make Ukrainian information control management more independent from Russia. In May 2017, former Ukrainian president Petro Poroshenko signed a decree that forbade mainstream Russian services and websites such as Mail.ru, VKontakte, Odnoklassniki, and Yandex.[168] He accompanied the decree by a post on VKontakte, a Russian social media platform urging all Ukrainians to switch away from Russian social media networks:

"Hybrid warfare requires adequate responses to challenges. Therefore, in order to influence opponents and counter-propaganda, my team used pages on some Russian social networks. But massive Russian cyberattacks around the world, including the recent interference in the French election campaign, indicate that it is time to act differently and more decisively. Ukrainian Internet providers should stop providing access to Vkontakte, Odnoklassniki, Yandex and other Russian services. All official pages of the President in these services will be closed. I urge all compatriots to leave Russian servers immediately for security reasons."[169]

In surveillance matters, a draft law on abolishing Department "K" has been presented to the public in mid-October 2019.[170] This seeking of independence was clearly expressed

[166] Liga.net, "Smart City - Города с Разумом," accessed May 1, 2019, http://www.liga.net/projects/smart_city/.
[167] Ibid.
[168] President of Ukraine, "УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №133/2017," *Офіційне інтернет-представництво Президента України*, May 15, 2017, https://www.president.gov.ua/documents/1332017-21850.
[169] Petro Poroshenko, "Post on VKontakte," *VKontakte*, May 16, 2017, https://vk.com/poroshenko.petro?w=wall-69234729_7815.
[170] Sergii Bondarchuk, "This Should Be Zelenskyy's Next Big Push," *Atlantic Council*, October 29, 2019, https://www.atlanticcouncil.org/blogs/ukrainealert/this-should-be-zelenskyys-next-big-push/; Security Service of Ukraine, "SBU Presents Draft Version of New Law 'on the Security Service of

by David Akhramia, previously leader of the ruling group in the Ukrainian parliament. Commenting on the exiting of Russian Internet Service Provider MST from the Ukrainian market, he said that the arrangement was: "The first in 90 days [since president Volodymyr Zelensky's party took power] — $734m and one less Russian operator in the country."[171]

However, Ukraine's yearning for independence also produced some paradoxes. Russia accompanied its intervention into Ukraine with a massive information campaign.[172] At least since February 2014, pro-Russian accounts surged in spreading disinformation, such as promoting stories of atrocities perpetrated by Ukrainian forces in the conflict.[173] In order to gain better control over Russian fake news, former president Poroshenko instituted several measures that targeted Russian services, but hurt internet freedom at the same time within the country.

To give some examples, in February 2015, Ukrainian legislators discussed the so-called "bloggers law", which requires website owners and bloggers to post their full names and addresses, so law enforcement personnel could easily reach out to them.[174] It also requires bloggers to fact check information that they publish, similarly to provisions that apply to

Ukraine' to the President," October 15, 2019, https://ssu.gov.ua/en/news/25/category/21/view/6613#.PdJ0jWrs.dpbs.

[171] Seddon, "MTS Sells Ukrainian Unit as It Focuses on Russia."

[172] NATO StratCom Centre of Excellence, "Analysis of Russia's Information Campaign Against Ukraine" (Riga, 2015).

[173] Todd C. Helmus et al., "Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe," Product Page (RAND Corporation, 2018), https://www.rand.org/pubs/research_reports/RR2237.html; NATO StratCom Centre of Excellence, "Analysis of Russia's Information Campaign Against Ukraine."

[174] Verkhovna Rada of Ukraine, "Draft Law on Amendments to the Law of Ukraine 'on Information' (Concerning the Dissemination of Mass Information on the Internet)," February 12, 2015, http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=54006; Lokot, "Ukrainian Separatists Block 100+ News Websites in 'Lugansk People's Republic' · Global Voices."

major news outlets.[175] The law was withdrawn after popular outcry from the public.[176] However, what is important is that the law would have been similar to Russia's law on bloggers which entered into force in August 2014, and whose main aim is to de-anonymise popular webpages.[177] The Russian law obliges operators of websites that have more than 3,000 readers a day to use their full name when they publish, as well as to register with the appropriate authorities.[178]

On 14 May 2018, president Poroshenko put into effect a decree that allowed for 192 predominantly Russian websites to be blocked.[179] Irina Chulivska from Digital Security Labs Ukraine condemned the action, since internet restrictions can usually only take place after public discussion and involvement of the judicial branch of the executive.[180] The Decree bypassed these democratic procedures, according to Chulivska.[181] In 2018, another presidential decree banned 200 Russian websites.[182] Then, in February 2019, just ahead of the Ukrainian presidential elections, the SBU proposed to ban 100 websites that

[175] Verkhovna Rada of Ukraine, "Draft Law on Amendments to the Law of Ukraine 'on Information' (Concerning the Dissemination of Mass Information on the Internet)."
[176] Tetyana Lokot, "Ukrainian MP Pushes for Carbon Copy Of Russian Blogger Law, Meets Resistance," *Global Voices*, February 16, 2015, https://globalvoices.org/2015/02/16/ukraine-russia-blogger-law/.
[177] Russian Federation, "Федеральный Закон От 05.05.2014 г. № 97-ФЗ," August 1, 2014, http://kremlin.ru/acts/bank/38409; Russian Federation, "В Законодательство Внесены Изменения, Устанавливающие Ответственность За Размещение Информации в Интернете," *Президент России*, May 5, 2014, http://kremlin.ru/acts/news/20929.
[178] Russian Federation, "Федеральный Закон От 05.05.2014 г. № 97-ФЗ"; Russian Federation, "В Законодательство Внесены Изменения, Устанавливающие Ответственность За Размещение Информации в Интернете."
[179] Verkhovna Rada of Ukraine, "Про Рішення Ради Національної Безпеки і Оборони України Від 2 Травня 2018 Року 'Про Застосування Та Скасування Персональних Спеціальних Економічних Та Інших Обмежувальних Заходів (Санкцій),'" *Офіційний Вебпортал Парламенту України*, May 14, 2018, https://zakon.rada.gov.ua/go/126/2018.
[180] Detektor Media, "Указом Про Санкції Президент Незаконно Зобов'язав Провайдерів Блокувати 192 Нових Сайти – «Лабораторія Цифрової Безпеки»," *Detector.Media*, May 25, 2018, https://detector.media/infospace/article/137834/2018-05-25-ukazom-pro-sanktsii-prezident-nezakonno-zobovyazav-provaideriv-blokuvati-192-novikh-saiti-laboratoriya-tsifrovoi-bezpeki/.
[181] Ibid.
[182] President of Ukraine, "УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №126/2018," *Офіційне інтернет-представництво Президента України*, 2018, https://www.president.gov.ua/documents/1262018-24150.

promote Russian propaganda, stating that the aim would be to defend the country from Russian "information influences."[183]

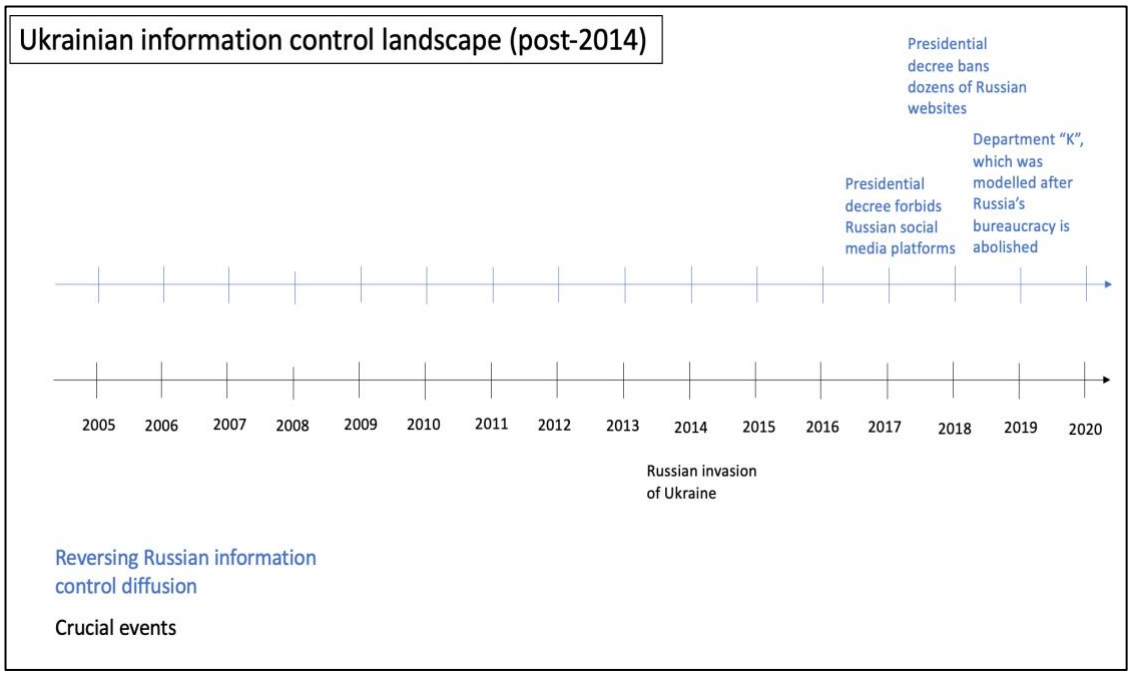


Figure 24: Ukrainian information control landscape (post-2014)

7.4. Why geographic proximity and constructivist challenges fail to explain Russian cyber norm diffusion

Constructivists purport that norm diffusion is about more than a *quid pro quo*. It is not only driven by material incentives of the norm promoter and the norm receiving countries. Fact is, however, that the Russian transfer of technology and techniques is precisely tailored to improve the power of the elite against its citizens. Elite reasoning for importing the norm and Russian exports is driven by political calculus. This is why Belarusian president Lukashenko imported SORM equipment in an election year. This is why

[183] Internet Svoboda, "Напередодні Українських Виборів СБУ Пропонує Заблокувати Нові 100 Інтернет-Сайтів," February 12, 2019, https://netfreedom.org.ua/article/naperedodni-ukrayinskih-viboriv-sbu-proponuye-zablokuvati-novi-100-internet-sajtiv.

Russian company Positive Technologies signed a memorandum on information security with a Kazakh intelligence agency. This is why Uzbekistan mimicked Russia's law on state surveillance. Russia's internet sovereignty norm is ultimately about regime survival and centralising power within the hands of a country's elite. And this is why Russia's norm has become so popular with authoritarian-leaning countries within the CIS. Considering all this it is difficult to argue that the norm transfer is much more than rational calculation driven by material interests of Russian and CIS elites.

Constructivists would foresee Russia's norm to diffuse within the Commonwealth of Independent States. The group of countries has a similar history as Russia and is therefore the perfect organisational platform for Russia as a norm promoter. However, Russia did not have to persuade these countries of its security assistance. The CIS elites' regime survival concern drove them to accept Russia as a security guarantor after the fall of the Soviet Union. It would only make sense that Russia would extend it being a guarantor into the digital realm. If Russia can send tanks to bolster regime security, why not also surveillance equipment?

Geographic proximity scholars would claim that strong economic and political interdependence between countries, which is reflected in geographical closeness, propels norm diffusion. This would explain much of the Russian sovereignty norm diffusion into CIS countries. Russia has had longstanding historical, economic and political linkage with these countries during the Soviet and ensuing post-Soviet period. However, geographic proximity scholars would have difficulties explaining the stop and even reversal of diffusion to Ukraine post-2014. They might look at data of economic interdependence with Russia for explanations. The economic ties started to diverge in

2012, when Ukrainian exports to and imports from Russia started to decrease.[184] The reduction of political interdependence (Ukraine left CIS in 2018) might be another indicator of the decreasing interlinkage between Russia and Ukraine – which would mean that diffusion of the Russian norm would be less likely.[185] But geographic proximity theorist scholars would have a hard time to explain a "reversal" of the norm diffusion process. They would have difficulties explaining Ukraine's wish and actions to root out the Russian cyber norm in its bureaucracy (abolishing of Department "K") and media landscape (banning of Russian websites). Moreover, geographic proximity theory as the prime factor for diffusion loses entirely its meaning post-2014. How did geography imply political, economic interdependence before 2014, but not thereafter? Why did geography matter for explaining norm diffusion in 2014, but not in 2015? Geographic proximity scholars fail to explain why.

As opposed to both geographic proximity theory and constructivist theory, empirical evidence provided in this chapter shows that the neoclassical realist explanation for diffusion holds. As long as there is a material demand and supply for information control technologies and techniques, norm diffusion is likely to take place. If there is no demand for Russian internet sovereignty anymore, such as in the case of Ukraine (due to a changing threat perception), diffusion stops, and a process reversing norm diffusion may take place.

[184] Marek Dabrowski, Marta Domínguez-Jiménez, and Georg Zachmann, "Six Years After Ukraine's Euromaidan: Reforms and Challenges Ahead," June 30, 2020, https://www.bruegel.org/2020/06/six-years-after-ukraines-euromaidan-reforms-and-challenges-ahead/.
[185] Radio Free Europe / Radio Liberty, "Ukraine Shuts Down Offices In CIS Member States."

7.5. The Russian technosphere and sovereignty

The first few ensuing paragraphs serve to illustrate Russia's conception of its right to influence its near abroad. This thesis will then show how this perception extends to cyberspace and how Moscow has built and is maintaining its technological sphere of influence and what this means for importing countries' sovereignty.

Russia has had a long history of embracing the concept of spheres of influence. The first time the concept was used is in the mid-19th century by the Russian foreign minister, in which he maintained that Afghanistan is within Russia's sphere of influence (SOI).[186] This SOI mainly extended to a number of countries that Russia perceived as buffers between itself and adversaries.[187] This sense of imperial rule over its neighbours was rediscovered after the fall of the Soviet Union.[188] During the Soviet era, organisations such as the Council for Mutual Economic Assistance (COMECON) were formed in order to legitimise Moscow's rule. It was easier to obtain orders from a multilateral organisation than directly from the Kremlin. In the post-Soviet Union era, the Soviet multilateral organisations were replaced by organisations such as the CIS. Even after the fall of the Soviet Union, it was clear what Moscow regarded as its SOI. Russian border policy in the 1990s attributed solely the CIS' external borders the full status of an international border, anything falling within these boundaries was seen as the internal administrative territory.[189] As Alina Polyakova, a senior Russia expert stated:

[186] Weber, "Making Sense of Technological Spheres of Influence."
[187] Giles, *Moscow Rules: What Drives Russia to Confront the West*.
[188] Ibid.
[189] Ibid: 15.

"The Kremlin does not believe that countries like Ukraine, [and] other countries it considers in its sphere of influence, that the people in those countries have the right to determine their own future."[190]

Former Russian officials have, for instance, argued that Russia is the only power that has the right to intervene in the former Republics of the Soviet Union and help maintain order, which led some observers to liken this stance to the US' Monroe doctrine.[191] In 2014, president Putin framed the annexation of Crimea in a similar discourse.[192] He defended Russian actions in Crimea as a legitimate way to protect Russian interests and tied Ukrainian sovereignty to these interests – meaning that there is no sovereignty, if Russian interests are not taken into consideration.[193]

Ruth Deyermond, a Senior Lecturer in Post-Soviet Security at King's College, sums it up well by claiming that the predominant significance of the sovereignty concept in Russian foreign policy is instrumental rather than ideational.[194]

[190] Alina Polyakova, "Russian Foreign Policy," *Council on Foreign Relations*, April 13, 2017, https://www.cfr.org/event/russian-foreign-policy.
[191] Bohuslav Litera, "The Kozyrev Doctrine - a Russian Variation on the Monroe Doctrine," *Perspectives*, no. 4 (1994): 45–52.
[192] President of Russia, "Address by President of the Russian Federation," *President of Russia*, March 18, 2014, http://en.kremlin.ru/events/president/news/20603.
[193] Ibid.
[194] Ruth Deyermond, "The Uses of Sovereignty in Twenty-First Century Russian Foreign Policy," *Europe-Asia Studies* 68, no. 6 (2016): 957–84.

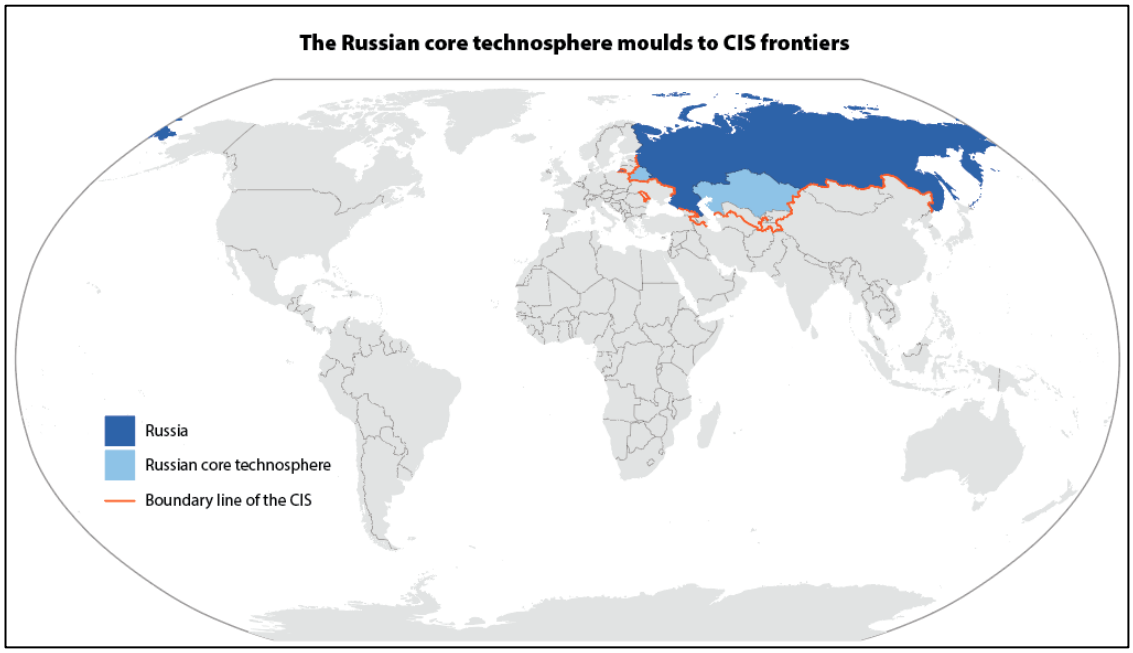


Figure 25: The Russian core technosphere moulds to CIS frontiers

7.5.1. Russia bolsters domestic and interdependence sovereignty

Russian regime survival assistance to elites of the CIS is nothing new. Traditionally Russia has bolstered regimes in the region by providing military equipment or by providing troops to appease conflicts.[195] This help comes with a tacit understanding that those regimes will take Russian interests into consideration when carrying out their domestic and foreign policies.[196] This tacit understanding has also been transferred into the digital age. Russia has been an avid supplier of surveillance technology to countries of the CIS and has served as a flagship example of how to govern cyberspace.

Thereby, it has bolstered domestic sovereignty of the elites (how authority is organised domestically and how effectively those structures exert authority). As the numerous

[195] Gorenburg, "External Support for Central Asian Military and Security Forces."
[196] Ibid.

examples above show, countries of the CIS have mimicked Russian state structures and laws when it comes to surveillance. In order to enforce surveillance laws, they have relied on Russian SORM technology, which is essentially a powerful tool that likely increases the effectiveness of authorities in controlling information.

At the same time, Russia has increased CIS countries' interdependence sovereignty (ability of states to control information, people, ideas across borders). One example is Kazakhstan's "Cyber Shield", which is intended to control cross-border information more effectively, introduce cybersecurity into national education, and create international cooperation on cybersecurity.[197] Much of the "Cyber Shield's" technology comes from Russia.[198] In this process of acquiring Russian technology and techniques, countries inevitably become more like Russia. As seen in Ukraine post-2014, this process can be stopped, and information control diffusion reversed.

This thesis proposed a framework to define information control models, depending on how ambitious a country is in controlling information as well as how much "options" it has to conduct information controls. In these terms, countries like Kazakhstan have become more like Russia, using Russian techniques and technology. Through receiving technology from Russia, their options to exert information controls increase. Kazakhstan may have already relied on surveillance, self-censorship, and strategic information dissemination and less so on censorship, but the diffusion from Russia strongly reinforced this tendency (e.g., copying of surveillance law).

[197] Government of the Republic of Kazakhstan, "Утвержден План Мероприятий По Реализации Концепции Кибербезопасности («Киберщит Казахстана») До 2022 Год (Аннотация к Документу От 28.10.2017)," *Zakon.Kz*, November 1, 2017, https://www.zakon.kz/4886464-utverzhden-plan-meropriyatiy-po.html.
[198] Moldabekov, "Евразийский Киберсоюз - Аналитический Интернет-Журнал Vласть."

At least since 2014, it has become clear what happens if a CIS country refuses Russian seeking of influence, and actively tries to become more independent: Russia immediately starts to undermine the elites of that country. But most countries acquiesce to be part of Russia's sphere of influence and enter the bargain of increasing domestic and interdependence sovereignty that comes at the expense of Westphalian sovereignty.

7.5.2. Russia erodes Westphalian sovereignty

China and the US do 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 in the system, allowing them to continue to obtain information after installation.[199] Deputy Director of Sygnatek (one of the companies that exported the gear to Kyrgyzstan), Sergei Pykhtunov said that "we shipped the interception equipment to Kyrgyzstan – it was an intergovernmental decision" but he denies the accusations that his equipment contained Russian backdoors.[200] The installation of backdoors would have coincided with heavy Russian influencing of Kyrgyz politics offline. In 2010, for instance, a combination of hard power (Russia removed its fuel subsidy for Kyrgyzstan) and soft power (Russia launched a propaganda campaign attacking the Kyrgyz president) moves helped topple Kyrgyz president Kurmanbek Bakiyev.[201] Russian meddling was due to Bakiyev's refusal to close the American military base in Manas in the country's north.[202] With Russia's influence in Kyrgyzstan

[199] Soldatov and Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You."
[200] Soldatov and Borogan, *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*: 640.
[201] Bruce Pannier, "Russia's Star On Rise Again In Kyrgyzstan," *RadioFreeEurope/RadioLiberty*, April 8, 2011, https://www.rferl.org/a/kyrgyzstan_back_in_russian_embrace/3551508.html.
[202] Ibid.

it is unsurprising that it would want to be informed on Kyrgyzstan's political affairs. In this vein, Tattu Mambetalieva, Adviser to the Prime Minister of Kyrgyzstan is concerned about possible backdoors in Russian supplied SORM equipment.[203]

Kazakhstan, for its part, is still relying strongly on foreign equipment makers, foremost among them Russia, in building its cyber capabilities.[204] The Director of Astana-based company CARCA, which was crucial in the building of Kazakhstan's "Cyber Shield" project, a cyber security system for Kazakhstan, mentioned that currently Kazakhstan is not yet there, but in the future the idea is to substitute imports domestically.[205] This is a security issue since the "Cyber Shield" project involves the building of a single data backup storage for critical information of state bodies.[206] It is very likely that the technology provided by Russia will be used to build this high security data storage, as well as other facilities, which are part of this cyber defence project.[207]

In Ukraine, Russian technology companies abroad were seen as potential tools of Russian spying. There are many possibilities for the FSB to spy on those companies' users, including Ukrainian citizens. Various Russian laws allow the FSB to monitor the users of these companies in real-time without notification.[208] As a consequence, the Ukrainian government prohibited Russian web companies Mail.Ru and Yandex. Those two

[203] Eurasianet, "Kyrgyzstan."
[204] Moldabekov, "Евразийский Киберсоюз - Аналитический Интернет-Журнал Vласть."
[205] Ibid.
[206] Government of the Republic of Kazakhstan, "Утвержден План Мероприятий По Реализации Концепции Кибербезопасности («Киберщит Казахстана») До 2022 Год (Аннотация к Документу От 28.10.2017)."
[207] Ibid.
[208] Russian Federation, "Федеральный Закон От 5 Мая 2014 г. N 97-ФЗ," *Российская Газета*, 2014, https://rg.ru/2014/05/07/informtech-dok.html; Russian Federation, "Об Информации, Информационных Технологиях и о Защите Информации," July 14, 2006, http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102108264.

companies had 25 million and 10.8 million Ukrainian users respectively before sanctions went into effect (total Ukrainian population around 40 million).[209]

According to an SBU investigation, Yandex had illegally stored and transferred data of Ukrainian citizens to Russia.[210] Amongst the citizens whose data was collected were military and law enforcement officials that were involved in combatting separatist groups in Eastern Ukraine.[211] This shows just how useful Russian social media sites can be for Russia in its attempt to gain intelligence on Ukraine and increase the power chasm between the two countries. The SBU continued by stating that:

"[T]he information was passed to the special services of the Russian Federation for planning, organizing and conducting intelligence, sabotage, information and subversive operations in our country to the detriment of **Ukraine's sovereignty** [emphasis added], territorial integrity and inviolability."[212]

With the banning of those Russian services Ukraine expects to reduce Russian influence and gain more Westphalian sovereignty. Interestingly, in June 2020, India recently imposed a similar step and blocked 59 Chinese mobile apps in reference to reclaiming its sovereignty by banning them.[213]

---

[209] Dmytro Borysov and Adam Lelonek, "Analysis: Yandex and Mail.RU Group Blocking in Ukraine in the Context of Information Warfare," *Centrum Analiz Propagandy i Dezinformacji*, accessed July 3, 2020, https://capd.pl/en/analyses/188-analysis-yandex-and-mail-ru-group-blocking-in-ukraine-in-the-context-of-information-warfare.

[210] SBU, "СБУ Провела Обшуки в Офісах Дочірньої Структури Російської Компанії «Яндекс» (Оновлено Відео) :: Служба Безпеки України," May 29, 2017, https://web.archive.org/web/20200608164106/https://ssu.gov.ua/ua/news/1/category/21/view/3431.

[211] Ibid.

[212] Ibid.

[213] Government of India - Press Information Bureau, "Government Bans 59 Mobile Apps Which Are Prejudicial to Sovereignty and Integrity of India, Defence of India, Security of State and Public Order," June 29, 2020, pib.gov.in/Pressreleaseshare.aspx?PRID=1635206.

7.6. Conclusion

This chapter has provided further evidence for the claims made in the theory chapter (see chapter 4 above). In particular, it shows how Russian information controls are much likelier to diffuse to countries where both the elite threat perception (IV2) has increased after major anti-government protests and the events of the Arab Spring, and in geographical areas where Russia is actively seeking influence in, i.e., CIS (IV1).

Through the provision and analysis of empirical data, this thesis has demonstrated that Russian information control diffusion is a question of demand and supply to satisfy material interests. The Russian norm does not diffuse because Russia persuaded CIS elites to import it. In contrast, they actively sought such assistance from Russia, and even imitated Russian laws that would help them strengthen their grip onto power.

This exchange between Russia and CIS countries comes as a sovereignty trade-off, where CIS countries' domestic and interdependence sovereignty is strengthened (bolstering of surveillance capabilities) and Westphalian sovereignty is diminished (e.g., Kyrgyzstan and Kazakhstan's dependence on Russia for regime survival).

The Russian internet sovereignty chapter completes the series of empirical chapters of this thesis, which provide extensive insights as to why Chinese and Russian internet sovereignty norms diffused successfully, thereby undermining the previously widespread internet freedom norm. This leads us to the concluding chapter of this thesis.

Chapter 8: Conclusion

This chapter first summarises the findings of the thesis and then turns to the contributions for IR. The thesis finally proposes recommendations for those who wish to defend internet freedom. It also examines future avenues for research with regards to the changing nature of surveillance, the future of internet freedom, as well as technospheres.

8.1. Findings and contributions

8.1.1. Findings

This thesis has sought to explain why the Chinese and Russian internet sovereignty norms diffused successfully to some countries – thereby undermining the dominant US norm of internet freedom. It also discussed some of the implications of successful international diffusion of internet sovereignty for understandings of sovereignty in IR.

The research questions treated in this thesis are important for both practice and theory. With regards to practice, Chinese and Russian digital authoritarianism have been on the rise internationally for the last decade. With the proliferation of the three cyber norms – internet freedom and Russian and Chinese internet sovereignty – a need to understand their proliferation has arisen. Without an understanding of why they have diffused successfully, it would be difficult to craft policies that could stall their diffusion. When it comes to theory, the concept of sovereignty is central. As this thesis has shown, the analysis of sovereignty has not yet extensively been applied to the topic of cyber norm diffusion. This thesis has sought to systematically address this gap in IR literature.

This thesis demonstrated that US, Russian and Chinese norm diffusion via technology and training has occurred across the world – but with important differences. Diffusion of

US, Chinese and Russian norms was more likely to occur in geographical areas where the norm promoters sought influence (IV1) and where high regime threat perception was present amongst a country's elite (IV2).

In chapter 5 (internet freedom case study), this thesis demonstrated that the internet freedom norm diffused to 192 countries through internet freedom technologies (e.g., TCP/IP is used all over the world; the Signal encryption protocol is used by 2 billion users). At first the US' internet freedom policies pushed for open markets, which allowed US technology companies to become global giants. Later on, the US funded internet freedom technologies, such as VPNs and the Tor Project in order to use those tools to increase its political influence abroad – e.g., US involvement in Iranian protests through Twitter in 2009 – and to increase freedoms worldwide (see Hillary Clinton's speech on internet freedom). This thesis argues that most countries imported the internet freedom norm unwittingly, especially authoritarian ones. They perceived the internet as an instrument to boost economic growth and not as a tool for political change that one could use for organising protests. In short, internet freedom diffused across the world because the US promoted its exports to gain economic and political influence abroad (IV1) and because, in the beginning, countries perceived the internet as a tool that would propel their economies, rather than an instrument that could threaten their regime stability (IV2).

Chapter 5 analysed the diffusion of internet freedom to the countries of the "Freedom Online Coalition+" in more detail. Only two countries worldwide did not import internet freedom: North Korea and China – they started building a national intranet instead. Early on, they recognised the revolutionary potential of the internet, and they consequently removed the freedom component from the internet.

Chapters 6 and 7 (Chinese and Russian internet sovereignty case studies) showed how around the year 2010, the Arab Spring and domestic protests changed the regime threat perception of elites in various countries (IV2), which led to the import of internet sovereignty. All countries that "imitated" China or Russia are either of a hybrid or authoritarian regime type and have experienced large-scale protests or made reference to the Arab Spring and social media as a threat to their regime before import occurred. The argument here is that regimes that have a heightened threat perception (hybrid/authoritarian regimes) are very likely to imitate Chinese and Russian sovereignty norms to ensure their own survival. This is because authoritarian-leaning leaders perceive that they have more to lose if they lose political power, e.g., exile, or capital punishment, compared to democratic leaders.[1] This observation is in line with the authoritarian diffusion literature, which claims that norms diffuse more easily between authoritarian regimes.[2]

To which countries has internet sovereignty not diffused and why? Some countries did not adopt internet sovereignty technology or techniques, because they already had alternative suppliers, as for instance, Bahrain and Syria. Others were likely not able to import Chinese equipment, because China withheld information control technology from them in order to influence their behaviour. Not exporting to Taiwan allies, for example, may make them more conducive to diplomatically recognise the People's Republic of China instead of Taiwan. Other countries, for their part, did not import sovereignty because the supplier (Russia) actually became a threat to their regime (Ukraine) through

[1] Kadercan, "Making Sense of Survival: Refining the Treatment of State Preferences in Neorealist Theory."
[2] Weyland, "Crafting Counterrevolution: How Reactionaries Learned to Combat Change in 1848."

invasion of the country and annexation of parts of its internet infrastructure (Crimea). As a result, Ukraine switched to an alternative supplier (China) to ensure the continued supply of vital surveillance equipment.

The theory deployed in this thesis of "why" and "where" diffusion occurred was tested against two rival theoretical approaches in IR: constructivist theory and geographic proximity theory. Constructivist theory challenges this thesis' theory as regards to "why" freedom/sovereignty diffusion occurred at all – why did the US, China, and Russia promote those norms and why did countries import it? Constructivism purports that internet freedom diffused because the US persuaded countries to adopt the norm with the underlying motive of increasing human rights.

US leaders have mentioned the increase of human rights as the goal of internet freedom, but its actions show that internet freedom is just as much motivated by the seeking of political and economic influence abroad. Furthermore, constructivism cannot explain why internet freedom diffused to authoritarian countries like Iran and Zimbabwe. It is unrealistic to believe that the US convinced authoritarian-leaning countries, such as Zimbabwe or Iran to import the internet, and with it, internet freedom in order to increase human rights.

As regards to internet sovereignty diffusion, China and Russia did not have to persuade authoritarian leaders of the utility of their surveillance technologies either. Countries did not import the internet sovereignty norm because China or Russia ideationally persuaded or materially forced them to do so, just like Gorbachev did not order glasnost and

perestroika due to external pressures from the West.[3] Rather, Gorbachev perceived the Soviet Union as relatively declining in power and in a state of overextension.[4] Consequently, he introduced reform measures.[5] And for countries adopting internet sovereignty policies, there is a perceived threat to regime survival, which explains these measures. Domestic protests organised through the internet were reason enough for countries to import surveillance technology.

Geographic proximity theory challenges my theory as regards to "where" diffusion should have occurred. It states that geographic closeness is the best indicator to explain diffusion. In this way, the US norm should have diffused to the rest of North America and South America. In reality, internet freedom diffused across the world – to every continent. In a similar way of thinking, the Chinese norm should have diffused to the rest of Asia. However, the empirical chapters show that Chinese tools have diffused to every continent, and even countries that showed advanced norm diffusion (imitation), were situated along the BRI (IV 1 – where Beijing is seeking influence) rather than in neighbouring geographical areas. As regards to Russia, advanced norm diffusion only occurred within the CIS countries. Here, geographic proximity theory was correct with its assumption that the norm is more likely to diffuse only regionally. However, geographic proximity theory fails to explain Ukraine's turn against Russian norm diffusion post-2014.

[3] Wohlforth, "Realism and the End of the Cold War."
[4] Ibid.
[5] Ibid.

8.1.2. Contributions

By answering the research question this thesis has sought to make several theoretical and empirical contributions. Firstly, this thesis has established a theoretical framework that allows for the distinction of different cyber norms (Chapter 4). This can be used by future scholars in their scholarly works. Secondly, this thesis has compiled and analysed large amounts of diffusion data, with regards to the internet freedom, Chinese, and Russian sovereignty norms. A portion of this data and analysis is already available online.[6] It has been used and cited by other researchers in their own works.[7] Thirdly, this thesis has argued that sovereignty trade-offs occur during the process of internet freedom/sovereignty norm diffusion. China and Russia bolster the domestic and interdependence sovereignty of countries and restrict their Westphalian sovereignty. Internet freedom diffusion, for its part, introduces checks and balances on the domestic and interdependence sovereignty of countries and weakens Westphalian sovereignty. The empirical evidence provided in this thesis (Chapters 5, 6, and 7) bolsters Stephen Krasner's view of sovereignty, who sees it as something divisible, which can be weakened or strengthened. This thesis thereby contributes to IR literature, which has been discussing what constitutes a weakening of sovereignty. Fourthly, this thesis has shown that norms and technology are inseparable. Internet freedom is inherent in the dominant internet protocols and standards of today or in messenger applications like Signal, which was funded through the US government's internet freedom fund and is designed to

[6] Weber, "The Worldwide Web of Chinese and Russian Information Controls."

[7] Andrew Imbrie et al., "Agile Alliances," February 2020, https://cset.georgetown.edu/research/agile-alliances/; Dahlia Peterson, "Foreign Technology and the Surveillance State," in *China's Quest for Foreign Technology: Beyond Espionage*, ed. William C. Hannas and Didi Kirsten Tatlow (London and New York: Routledge, 2021); Lydia Khalil, "Digital Authoritarianism, China and COVID," *Lowy Institute*, November 2, 2020, https://www.lowyinstitute.org/publications/digital-authoritarianism-china-and-covid.

provide a high level of privacy to users. Fifthly, this thesis highlighted the importance of material incentives as causes of internet freedom and sovereignty norm diffusion

8.2. Policy recommendations

8.2.1. Those interested in defending internet freedom should focus their norm promotion efforts on the most prized technosphere: The Technological Crescent

Many geostrategists have placed Eurasia at the centre of history's geopolitical pivot. Throughout history, this swath of land has harboured major geopolitical players, from the Romans to the Mongols to the Manchus.[8] Each empire used the area's abundant resources to acquire immense power — with the western, southern, and eastern fringes being especially vital, as Nicholas Spykman observed in the middle of the twentieth century.[9] This thesis, therefore, designates the combination of Europe, Middle East, South(east) Asia, and East Asia as the world's "Technological Crescent", the most prized territory. It contains states with important rare earth resources (China, India, Malaysia, Myanmar, Thailand, and Vietnam), which are used to produce high-tech products.[10] It also plays host to the world's technology supply chain and innovation hubs, spanning from China, Taiwan, South Korea, Japan, Thailand, through to Germany, France, and the UK. In addition, the territory houses companies such as ARM, BBK Electronics, Bosch, Foxconn, Fujitsu, Huawei, Infineon, Samsung, Siemens, as well as cyber powers like Iran and Israel.

The "Technological Crescent's" geopolitical importance also bears more traditional characteristics. It is here that two of the three largest economic, military, and technological political entities — China and the EU — interact. It is more critical of a geographical pivot

[8] Zbigniew Brzezinski, *The Grand Chessboard: American Primacy and Its Geostrategic Imperatives* (BasicBooks, 1997).
[9] This geographical space was designated by Halford Mackinder as the Inner or Marginal Crescent and by Nicholas Spykman as the Rimland.
[10] U.S. Geological Survey, "U.S. Geological Survey, Mineral Commodity Summaries - Rare Earths," February 2019, https://prd-wret.s3-us-west-2.amazonaws.com/assets/palladium/production/atoms/files/mcs-2019-raree.pdf.

than the Eurasian hinterland. Russia, the preeminent power there, while still important (especially regarding its cyber-attack and information warfare capabilities), is a waning power with an economy the size of Italy's and almost no companies that provide technology or services beyond its borders. It is thus increasingly apparent that Russia and the region at large — which includes states such as Kazakhstan, Mongolia, and Uzbekistan — do not represent the most vital technological area. In short, due to the vitality of the Eurasian Technological Crescent, those interested in promoting internet freedom should focus their efforts on countries present in this geographical area. The idea is that if one manages to increase internet freedom in countries where technology is being produced, designed and standards are being established, internet freedom may have a better chance in the rest of the world.

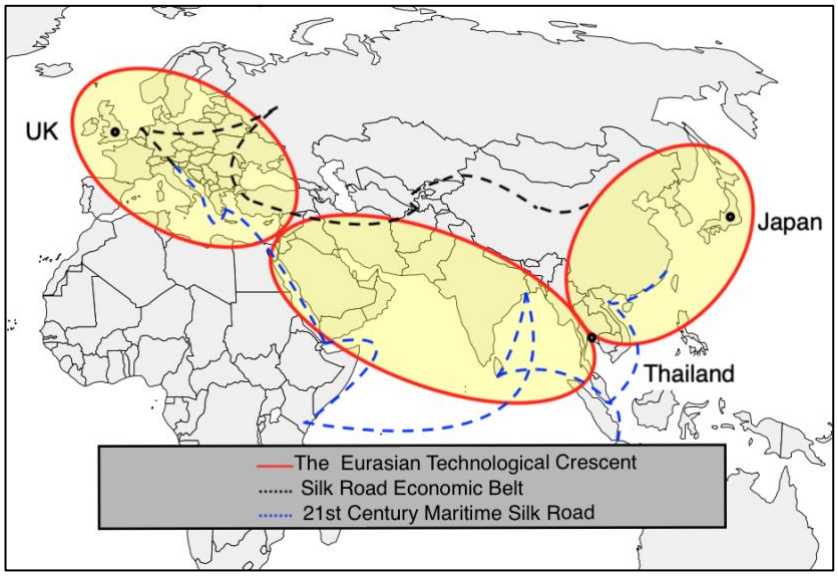


Figure 26: The Eurasian Technological Crescent

8.2.2. Those interested in defending internet freedom should embrace strategic thinking

The literature surrounding the intersection of strategy and human rights offers insights in the path of how to combat the decline of internet freedom. For now, strategic thinking is

confined to few sub-communities within the internet freedom community, such as funders (who pick projects they think are most effective in fighting information controls) and lawyers who conduct strategic litigation.[11] The following section highlights how strategic thinking could benefit the internet freedom community more broadly.

Strategy is one of the fields that has produced one of the most prolific bodies of literature, whether it is in the military, political, business, and more recently also in the human rights field.[12] A basic definition of strategy that is common across disciplines is that strategy is a plan to reach a goal and to overcome a challenge through certain means.[13] Strategists always have limited resources and hence need to balance ends and means. Johnson and Sikkink have conceptualised strategic thinking for human rights advocates in a book chapter titled "Strategizing for Human Rights: From Ideals to Practice".[14] In it, they mention that bringing strategy to the field raises certain suspicions amongst human rights activists, who are naturally averse to thinking associated with the military or cold-blooded power politics. Many activists fear that the normative element of human rights work gets lost if activists start engaging in cost-benefit calculations of how to reach their goals and prioritise their targets. However, Johnson and Sikkink mention that strategic thinking brings several benefits to human rights advocacy.[15] They argue that one needs to

[11] Digital Freedom Fund, "About."

[12] Robert J Art, *A Grand Strategy for America*, Cornell Studies in Security Affairs (Ithaca: Cornell University Press, 2003); Laurent Bernhard, *Campaign Strategy in Direct Democracy*, Challenges to Democracy in the 21st Century (Basingstoke: Palgrave Macmillan, 2012); Brian Tracy, *Business Strategy*, Brian Tracy Success Library (New York, New York: American Management Association, 2015); Bardo Fassbender et al., eds., "Strategizing for Human Rights: From Ideals to Practice," in *The Limits of Human Rights* (Oxford: Oxford University Press, 2019).

[13] Colin S. Gray, *The Future of Strategy* (Cambridge: Polity, 2015); Richard K. Betts, "Is Strategy an Illusion?," *International Security* 25, no. 02 (Fall 2000): 5–50; Fassbender et al., "Strategizing for Human Rights: From Ideals to Practice."

[14] Fassbender et al., "Strategizing for Human Rights: From Ideals to Practice."

[15] Some scholars have pointed to the lack of attention of Johnson and Sikkink to historical and social context of many movements and that in devising these strategies this context should be central, otherwise advocacy could have negative results. Micheline Ishay, "Historical Strategies for Human Rights," in *The*

understand how one's adversary thinks. Countries do think strategically, and a better understanding thereof within the internet freedom community may increase chances of success in one's struggle against powerful countries' human rights violations. The following paragraphs illustrate how strategic thinking could look like in practice.

Long-term thinking

Thinking in a strategic way helps understanding nation-states better, because threat actors think strategically, with a view of the long term. Digital rights defenders, on the other hand, face a question of survival every day. Often, there is no time to think into the long term, but it would be of value. Thinking of trends and nation-state motivations can be beneficial to devising information control defeating strategies. For instance, if the recent crackdown in Hong Kong had been actively expected, what measures could have been put in place by activists to mitigate current surveillance practices? As can be currently observed, Taiwan might suffer a similar fate as Hong Kong, if action is not taken immediately. It would thus certainly be beneficial to ask more future-oriented questions. This includes, for instance, how one could put structures in place *now* that would facilitate protests in a hypothetical future Taiwan under mainland-Chinese government rule, where information control abuse would be commonplace. Another long-term question is whether new techniques should be developed to divert censors' and surveillers' attention and thereby complement existing tools that are intended to foster anonymity and freedom of expression. How can the community divest the censors' resources in the long-term?

Limits of Human Rights, ed. Bardo Fassbender and Knut Traisbach (Oxford: Oxford University Press, 2019).

Creating synergies: Integrating anti-surveillance and anti-censorship techniques into an integrated approach

A crucial part of strategic thinking is to create synergies, i.e., encouraging that a variety of means become more than the simple sum of their individual parts. Governments across the world are already taking such an approach. They create synergies by integrating different surveillance technologies and centralising data. What combination of tools is needed to create synergies when it comes to anti-censorship/surveillance tools? How does a holistic information control mitigation toolbox look like?

Tying the tactical to the operational, and the operational to the strategic

Integrating the various levels of tactical (individual actions) and operational actions (series of related tactical actions) is necessary to achieve strategic outcomes. In the process of doing so, one obtains a clear idea of what tactical and operational actions can achieve in terms of strategic outcomes.[16]

In addition to the above measures, several strategic considerations help to increase the effectiveness of human rights advocacy: a clear definition of who exactly the most effective target of a campaign is (local police department, courts), what the consequence of applying pressure on a specific node is (e.g., demonstrations in front of parliament), what the alternative targets are, and what tactics are successful in a given situation (large concentrated or dispersed demonstrations).

[16] United States Air Force, "Three Levels of War," *Air and Space Power Mentoring Guide* 1 (1997).

8.2.3. Winning hearts and minds through a compelling strategic narrative

The current strategic narrative of liberal democracies is too narrow, and it offers no clear and tangible roadmap to a world where freedom can prevail.

The narrative focuses solely on two arguments. One, that digital authoritarianism is illegitimate due to its repressive nature. Two, that an open society will eventually outcompete dictators, since open societies innovate more readily and attract talent more easily. China's version of digital authoritarianism has successfully contested both arguments and thereby strengthened the legitimacy of its mode of government.

First, on the moral side of things, president Biden has continued arguments from previous US administrations that digital authoritarianism is illegitimate.[17] In contrast, China, and other authoritarian countries, have hijacked the term sovereignty and used it as a shield to ward off any criticism directed towards their repression and abuse of digital human rights.[18]

Second, the strategic narrative of democracies is built on a claim that open societies will prevail in the long run over closed ones.[19] However, China has continued to show that repression online does not necessarily translate into hampering the economy and damaging competitiveness too much. Meanwhile, many autocrats abroad have taken notice and attempt to replicate this model of building one's own intranet ecosystem while

[17] Joe Biden, "Remarks by President Biden at the 2021 Virtual Munich Security Conference," *The White House*, February 19, 2021, https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/02/19/remarks-by-president-biden-at-the-2021-virtual-munich-security-conference/.
[18] Qiu, "India's Internet Shutdown Shows Normal Practice for Sovereign Countries."
[19] Electronic Frontier Foundation, "Secretary of State Hillary Rodham Clinton Remarks on Internet Freedom," February 15, 2011, https://www.eff.org/files/filenode/clinton_internet_rights_wrongs_20110215.pdf.

staying plugged into the global digital economy. Even though they may not succeed, since they do not have the market size of China, there is still a belief among autocrats that it may be possible. One just needs to look at the development of local app equivalents to Facebook or WhatsApp in Russia, Iran, and Egypt as a proof of this belief.

Since the democratic narrative is being contested on both counts of legitimacy and performance, just insisting on these two assertions may be insufficient. In order to meet the authoritarian challenge, liberal democracies need to broaden the category of their arguments. Much more could be done to study digital authoritarianism and uncover weaknesses in its system and juxtapose it with the strengths of the democratic system. Previously, I have written about how detrimental China's control of information is for its cyber security and that it leaves it exposed to cyberattacks.[20] Democracies should highlight that, while China's model allows autocrats to monitor their populations more easily, it makes their cybersecurity landscape more vulnerable. Since the authoritarian model actively discourages encryption and privacy measures, countries that remake their cybersecurity landscapes in the image of China may be more vulnerable to cybercrime campaigns and competing states' cyber operations. On the other hand, a democratic model of digital governance (as exemplified particularly by Europe), where privacy is inherent in the system and encryption is ubiquitous, reduces such dangers.

At the same time, democracies cannot only call out the weaknesses of their opponents, but they have to continue to strengthen their own systems, bolster privacy and champion the digital rights of their citizens. In addition to broadening the scope of the argument, the strategic narrative also needs to have achievable goals. Few liberal democracies have

[20] Weber, "How China's Control of Information Is a Cyber Weakness."

yet laid out a quantifiable roadmap for enhancing digital freedoms, against which success of actions could be measured.

The US and other members of the democratic tech-alliance should set out an Internet Freedom 2030 Strategy, in which they present achievable internet freedom milestones. Quantifiable goals are already present in other areas of global relevance, such as climate change (limiting global warming to below 2°C) and should be extended to the digital rights agenda. An example could be to aim at extending the membership of the Freedom Online Coalition or help legislation pertaining to the freedom of information to be passed by as many states as possible by 2030. Currently 119 countries have passed such laws, meaning that around 70 countries are still without such legislation.[21]

8.3. Further work on the future of surveillance, internet freedom, and technospheres

This thesis has studied norm promotion in the digital age, by looking at the diffusion of CCTV cameras, internet infrastructure surveillance gear, and journalist training in online media, amongst others. But the internet is transforming rapidly. The physical and digital layers are merging – so are online and offline freedoms. The study of internet freedom/sovereignty norm diffusion and the emerging technospheres needs to stay on pace with these transformations and current lacunae in research need to be filled.

[21] Freedom Info, "About Us," 2021, http://www.freedominfo.org/about-us/.

8.3.1. Technospheres, norms, and IR

IR scholars should study technospheres more profoundly. They could investigate how the relationship between the US hegemon with its technosphere is similar or different from the Chinese or Russian relationship with their technospheres, or whether an emerging Chinese technosphere translates into an increase in likelihood of great power conflict with the United States? Susanna Hast, for instance, claims that traditional spheres of influence have promoted stability since hegemons have recognised each other's spheres of influence and that there has been a tacit understanding of not interfering into each other's geographical area of influence.[22] In cyberspace, this question of stability is yet very much open, since no great power perceives another great power's technosphere as exclusive. Any hegemon can lead a cyber operation in any country. It may even occur that several great power cyber operations (e.g., US and Chinese) target and intrude into the same foreign system (e.g., Vietnam) at the same time.

When it comes to norm diffusion, norm scholars could adopt the norm framework proposed in this thesis. They could use the framework to define and study, for instance, regional norm-setters in the Arab-speaking world, i.e., the Saudi and Iranian cyber norms, which may have diffused to other Sunni and Shia countries, respectively. Academics could study whether the Saudi and Iranian norms – largely defined by their focus on establishing an internet in conformity with religious values – have diffused beyond the Sunni and Shia world, and why, or whether those norms have only an appeal to countries that share their religious worldview. Would neoclassical realist explanations provide a suitable explanation for Iranian and Saudi cyber norm diffusion, or would geographic proximity theory or constructivist theory provide a better insight into diffusion? What is the

[22] Hast, *Spheres of Influence in International Relations : History, Theory and Politics*.

relationship between regime survival and religion in Iran and Saudi Arabia and how does this relationship define the Iranian and Saudi cyber norms?

8.3.2. The changing nature of surveillance

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."[23]

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.[24] 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).

[23] Bruce Schneier, "Click Here to Kill Everyone," 2017, https://nymag.com/intelligencer/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html.
[24] Erika Kinetz, "In China, Your Car Could Be Talking to the Government," *AP NEWS*, November 29, 2018, https://apnews.com/c6e610eb8f4645b4806bc16479b64809.

8.3.3. Internet freedom – an evolving concept

Some experts have argued that internet freedom was defined too narrowly in the past and was initially largely focussed on exporting democracy, domestic US constitutional values, such as freedom of speech, as well as non-regulation of markets, as a principle, which allowed US companies to obtain a considerable global market share.[25] In a much-cited speech of 2010, Hillary Clinton evoked the American traditions such as the four freedoms (freedom of speech, freedom of worship, freedom from want, freedom from fear) and the First Amendment to the United States Constitution when contextualising internet freedom.[26] David Kaye, former UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, dubs this the "language of supply."[27] That focus disregarded other fundamental rights, e.g. right to privacy, which has been fundamental to the European conception of digital rights, as enshrined in the (GDPR) General Data Protection Regulation.[28] Instead Nani Jansen Reventlow, Director of the Digital Freedom Fund, suggests that internet freedom efforts ought to focus more on enforcing emerging human rights norms, e.g., as stipulated in the International Covenant on Civil and Political Rights. David Kaye, for his part, argues that internet freedom strengthening efforts should fundamentally build on the demand side of internet freedom.[29] In short, going beyond the rhetoric of "supply side internet freedom" means recognising that there is a global demand for digital rights. As shown in Chapter 5, which highlights the growing number of digital rights activists online, it is more than certain that such global demand exists.

---

[25] Goldsmith, "The Failure of Internet Freedom."
[26] Clinton, "Remarks on Internet Freedom."
[27] David Kaye, "The Limits of Supply-Side Internet Freedom," June 13, 2018, https://knightcolumbia.org/content/limits-supply-side-internet-freedom.
[28] Jansen Reventlow and McCully, "Internet Freedom Without Imperialism."
[29] Kaye, "The Limits of Supply-Side Internet Freedom"; Jansen Reventlow and McCully, "Internet Freedom Without Imperialism."

In addition to this, there is a need for a conversation about broadening the internet freedom definition, in order to account for the changing nature of the internet. The emergence and increasing pervasiveness of virtual/augmented reality may impact how we see internet freedom and therefore a discussion around the concept of virtual/augmented reality freedom needs to take place.

8.3.4. The future of technospheres

The character of internet freedom is changing with time, and so are technospheres. The following lines elaborate how especially the US, Chinese, and Russian technospheres are likely to evolve. Countries that are situated solidly within a technosphere are unlikely to switch from one technosphere to another. Amongst them, there is almost no resistance to the establishment of different zones of thinking about the governance of information — CIS countries will continue to follow the Russian model, BRI countries the Chinese, and countries of the Freedom Online Coalition + will continue to endorse internet freedom.

Countries which are at the periphery are more likely to exit a specific technosphere and enter another. However, it is likely that US-China-Russia competition will focus on countries that are already in their peripheral technospheres and try to draw them deeper into their respective technosphere. Hence, the pressure coming from a hegemon may make it more difficult for states that find themselves in a particular technosphere to switch to a different technospheres.

In summary, this thesis introduced a novel approach to studying cyber norm diffusion by looking at the diffusion indicators of technology transfer, imitation, and training. This approach can be used to examine the export/import of other cyber norms, such as the

Indian (marked by its emphasis on internet shutdowns) or the Iranian and Saudi Arabian ones (distinctive through their focus on content control based on religious grounds). In addition to this, the insights gained in this study of internet freedom/sovereignty could be used by IR scholars focussed on democracy promotion, authoritarian diffusion, and norm diffusion more broadly – all streams of literature which this thesis used to build its argument. The thesis also speaks to the countless IR scholars who study sovereignty. This thesis hopes to have added to the lively discussion surrounding this topic by showing that during internet freedom/sovereignty diffusion a change in the domestic and interdependence as well as Westphalian sovereignty of a country occurs. It studied this change in sovereignty on a global basis and provided a large dataset that can be used for future studies.

Bibliography

Access Now. “About Us.” *Access Now*, 2020. https://www.accessnow.org/about-us/.

———. “Funding.” *Access Now*, 2020. https://www.accessnow.org/financials/.

———. “History.” *RightsCon Summit Series*, 2020. https://www.rightscon.org/about-and-contact/.

———. “RightsCon Brussels - Outcomes Report,” 2017. https://www.rightscon.org/cms/assets/uploads/2017/06/Rightscon-2017-Brux-Outcome-Report.pdf.

———. “RightsCon Toronto - Outcomes Report,” 2018. https://www.rightscon.org/cms/assets/uploads/2018/07/RightCon2018-outcomes-report.pdf.

———. “RightsCon Tunis - Outcomes Report,” 2019. https://www.rightscon.org/cms/assets/uploads/2019/10/RC19-Tunis-outcomes-report.pdf.

Acharya, Amitav. “How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism.” *International Organization* 58, no. 2 (2004): 239–75.

———. “State Sovereignty After 9/11: Disorganised Hypocrisy.” *Political Studies* 55, no. 2 (2007): 274–96.

Action on Armed Violence. “UK Arms Exports to Bahrain,” November 29, 2018. https://aoav.org.uk/2018/uk-arms-exports-to-bahrain/.

Adam Quinn. “Kenneth Waltz, Adam Smith and the Limits of Science: Hard Choices for Neoclassical Realism.” *International Politics* 50, no. 2 (2013): 159–82.

“Afghanistan/Pakistan Workshop on Best Practices of Polio Reporting.” *USAGM*. Accessed December 30, 2020. https://www.usagm.gov/2018/07/12/afghanistanpakistan-workshop-best-practices-polio-reporting/.

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.

———. “Timeline: Egypt’s Revolution,” February 14, 2011. https://www.aljazeera.com/news/middleeast/2011/01/201112515334871490.html.

Alfa Bank. “Mikhail Fridman,” 2020. https://alfabank.com/members/mikhail-fridman/.

Allison, Lincoln. “Authoritarianism.” *Oxford Reference*, 2021. https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095435698.

Alshenqueeti, Hamza. “Interviewing as a Data Collection Method: A Critical Review.” *English Linguistics Research* 3, no. 1 (March 31, 2014): 39–45.

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

Ambrosio, Thomas. “Catching the ‘Shanghai Spirit’: How the Shanghai Cooperation Organization Promotes Authoritarian Norms in Central Asia.” *Europe-Asia Studies* 60, no. 8 (2008): 1321–44.

———. “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.
American Civil Liberties Union. “Checks, Balances, and the National Security Agency,” June 10, 2013. https://www.aclu.org/blog/national-security/secrecy/checks-balances-and-national-security-agency.
———. “Privacy & Technology.” *American Civil Liberties Union*, 2020. https://www.aclu.org/issues/privacy-technology.
Amnesty International. “Amnesty Tech,” 2020. https://www.amnesty.org/en/tech/.
———. “‘It’s Enough for People to Feel It Exists,’” 2016. https://www.amnesty.org/en/documents/eur49/4306/2016/en/.
———. “We Will Find You Anywhere,” 2017. https://www.amnesty.org/download/Documents/EUR6259742017ENGLISH.PDF.
Analysis, CAIDA: Center for Applied Internet Data. “About CAIDA.” *CAIDA*, 2020. https://www.caida.org/home/about/index.xml.
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.
Aron, Leon. “Everything You Think You Know About the Collapse of the Soviet Union Is Wrong.” *Foreign Policy*, June 20, 2011. https://foreignpolicy.com/2011/06/20/everything-you-think-you-know-about-the-collapse-of-the-soviet-union-is-wrong/.
Art, Robert J. *A Grand Strategy for America*. Cornell Studies in Security Affairs. Ithaca: Cornell University Press, 2003.
Article 19. “What We Do,” 2020. https://www.article19.org/what-we-do/.
Associated Press in Harare. “Thousands March in Harare in Rare Mass Protest Against Robert Mugabe.” *The Guardian*, April 14, 2016. http://www.theguardian.com/world/2016/apr/14/thousands-march-harare-rare-mass-protest-against-robert-mugabe.
Auerbach, Jonathan, 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.
Avast. “What Is TCP/IP? | How the Model & Protocols Work,” August 2, 2020. https://www.avast.com/c-what-is-tcp-ip.
Bagby, Laurie M. Johnson. “Thucydidean Realism: Between Athens and Melos.” *Security Studies* 5, no. 2 (1995): 169–93.
Balmer, Crispian. “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.
Bannister, Adam. “What Exactly Is a ‘Safe City’?” *IFSEC Global | Security and Fire News and Resources*, September 5, 2014. https://www.ifsecglobal.com/security/exactly-safe-cities-mean/.
Banzi, Asterius. “Tanzania: Govt Seeks Chinese Help in Social Media.” *The East African (Nairobi)*, August 1, 2017. https://allafrica.com/stories/201708020658.html.

Barlow, John Perry. “A Declaration of the Independence of Cyberspace.” *Electronic Frontier Foundation*, February 8, 1996. https://www.eff.org/de/cyberspace-independence.
Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R. B. J. Walker. “After Snowden: Rethinking the Impact of Surveillance.” *International Political Sociology* 8, no. 2 (2014): 121–44.
BBC. “Google Outrage at ‘NSA Hacking.’” *BBC News*, October 31, 2013, sec. US & Canada. https://www.bbc.com/news/world-us-canada-24751821.
———. “Russia Profile - Media,” April 25, 2017, sec. Europe. https://www.bbc.com/news/world-europe-17840134.
BBC News. “Arab Uprising: Country by Country - Bahrain,” December 16, 2013. //www.bbc.co.uk/news/world-12482295.
———. “Ex-Google Boss Defends Multiple Controversies,” May 13, 2019, sec. Technology. https://www.bbc.com/news/technology-48262148.
———. “Google’s Chinese Search Engine ‘Terminated,’” July 17, 2019, sec. Technology. https://www.bbc.com/news/technology-49015516.
———. “Google’s Project Dragonfly ‘Terminated’ in China,” July 17, 2019, sec. Technology. https://www.bbc.com/news/technology-49015516.
———. “Nicaragua Canal Protest: Thousands Oppose Atlantic-Pacific Plan,” June 14, 2015, sec. Latin America & Caribbean. https://www.bbc.com/news/world-latin-america-33125526.
———. “Nicaragua Unrest: Thousands Join Renewed Anti-Government Rallies,” May 27, 2018, sec. Latin America & Caribbean. https://www.bbc.com/news/world-latin-america-44269498.
———. “Nicaraguans Protest Against Canal Plans,” December 10, 2014, sec. Latin America & Caribbean. https://www.bbc.com/news/world-latin-america-30426100.
———. “Police Kill Tanzania Protesters,” January 6, 2011, sec. Africa. https://www.bbc.com/news/world-africa-12126861.
———. “Syrian President Bashar Al-Assad: Facing Down Rebellion,” August 31, 2020, sec. Middle East. https://www.bbc.com/news/10338256.
———. “‘Tanzanian Shot’ in Gas Crackdown,” May 24, 2013, sec. Africa. https://www.bbc.com/news/world-africa-22652809.
———. “Thai Military Seizes Power in Coup,” May 22, 2014, sec. Asia. https://www.bbc.com/news/world-asia-27517591.
———. “Thousands on Strike in Vietnam Over Insurance Law,” April 1, 2015, sec. Asia. https://www.bbc.com/news/world-asia-32142635.
———. “Transcript of Leaked US Ukraine Call,” February 7, 2014, sec. Europe. https://www.bbc.com/news/world-europe-26079957.
———. “Ukraine Crisis: Timeline,” November 13, 2014, sec. Europe. https://www.bbc.com/news/world-middle-east-26248275.
Bearak, Max. “‘Shut Down Zimbabwe’ Protests Are Met With Internet Blackouts and Arrests.” *Washington Post*, July 6, 2016. https://www.washingtonpost.com/news/worldviews/wp/2016/07/06/shut-down-zimbabwe-protests-are-met-with-internet-blackouts-and-arrests/.
Ben Gharbia, Sami. “The Internet Freedom Fallacy and the Arab Digital Activism.” *Nawaat*, September 17, 2010. https://nawaat.org/portail/2010/09/17/the-internet-freedom-fallacy-and-the-arab-digital-activism/.
Bender, Katja, Sonja Keller, and Holger Willing. “The Role of International Policy Transfer and Diffusion for Policy Change in Social Protection – A Review of

the State of the Art." *IZNE Social Protection Working Paper*, 2014. https://www.h-brs.de/files/izne/policy_diffusion_1.pdf.
Ben-Hassine, Wafa. "Egyptian Parliament Approves Cybercrime Law Legalizing Blocking of Websites and Full Surveillance of Egyptians." *Access Now*, June 20, 2018. https://www.accessnow.org/egyptian-parliament-approves-cybercrime-law-legalizing-blocking-of-websites-and-full-surveillance-of-egyptians/.
Benkler, Yochai, Robert Farris, and Rob Weiss. *Network Propaganda*. New York, U.S.: Oxford University Press, 2018.
Bennett, Andrew. "The Oxford Handbook of Political Methodology," 2008.
Bennett, Andrew, and Colin Elman. "Case Study Methods in the International Relations Subfield." *Comparative Political Studies* 40, no. 2 (February 1, 2007): 170–95.
Bennetts, Marc. "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.
Berkman Klein Center. "Funding & Support Policies," December 11, 2019. https://cyber.harvard.edu/about/support.
———. "Home," 2020. https://cyber.harvard.edu/.
Bernhard, Laurent. *Campaign Strategy in Direct Democracy*. Challenges to Democracy in the 21st Century. Basingstoke: Palgrave Macmillan, 2012.
Betts, Richard K. "Is Strategy an Illusion?" *International Security* 25, no. 02 (Fall 2000): 5–50.
Betz, David J., and Tim Stevens. "Chapter Two: Cyberspace and Sovereignty." In *Cyberspace and the State: Toward a Strategy for Cyber-Power*, 55–74. Adelphi Series. London, United Kingdom: International Institute of Strategic Studies, 2011.
Biden, Joe. "Remarks by President Biden at the 2021 Virtual Munich Security Conference." *The White House*, February 19, 2021. https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/02/19/remarks-by-president-biden-at-the-2021-virtual-munich-security-conference/.
Biersteker, Thomas J., and Cynthia Weber. *State Sovereignty as Social Construct*. Cambridge Studies in International Relations. Cambridge: Cambridge University Press, 1996.
Bisley, Nick. *The End of the Cold War and the Causes of Soviet Collapse*. Basingstoke: Palgrave Macmillan, 2004.
Björkdahl, Annika. "Norms in International Relations: Some Conceptual and Methodological Reflections." *Cambridge Review of International Affairs* 15, no. 1 (2002): 9–23.
Bondarchuk, Sergii. "This Should Be Zelenskyy's Next Big Push." *Atlantic Council*, October 29, 2019. https://www.atlanticcouncil.org/blogs/ukrainealert/this-should-be-zelenskyys-next-big-push/.
Borogan, Irina, 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-.
Borysov, Dmytro, and Adam Lelonek. "Analysis: Yandex and Mail.RU Group Blocking in Ukraine in the Context of Information Warfare." *Centrum Analiz Propagandy i Dezinformacji*. Accessed July 3, 2020.

https://capd.pl/en/analyses/188-analysis-yandex-and-mail-ru-group-blocking-in-ukraine-in-the-context-of-information-warfare.
Bourgelais, Peter. “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.
Brandom, Russell. “A New Trump Appointee Has Put Internet Freedom Projects in Crisis Mode.” *The Verge*, June 23, 2020. https://www.theverge.com/2020/6/23/21300424/open-technology-fund-usagm-circumvention-tools-china-censorship-michael-pack.
———. “After OTF Takeover, Trump Appointee Faces Pressure From Lawmakers and Courts.” *The Verge*, June 24, 2020. https://www.theverge.com/21301542/otf-usagm-michael-pack-lawsuit-congress-open-technology-fund.
Bronner, Ethan, and Michael Slackman. “Saudi Troops Enter Bahrain to Help Put Down Unrest.” *The New York Times*, March 14, 2011. https://www.nytimes.com/2011/03/15/world/middleeast/15bahrain.html.
Brooks, Stephen G., and William C. Wohlforth. “Power, Globalization, and the End of the Cold War: Reevaluating a Landmark Case for Ideas.” *International Security* 25, no. 3 (2001): 5–53.
Browne, Ryan. “Russia Follows China in VPN Clampdown, Raising Censorship Concerns.” *CNBC*, July 31, 2017. https://www.cnbc.com/2017/07/31/russia-follows-china-in-vpn-clampdown-raising-censorship-concerns.html.
Brzezinski, Zbigniew. *The Grand Chessboard: American Primacy and Its Geostrategic Imperatives*. BasicBooks, 1997.
Budd, Cristopher. “Angler: The Rise and Fall of an Exploit Kit.” *Trend Micro*, September 14, 2016. https://blog.trendmicro.com/angler-rise-fall-exploit-kit/.
Budnitsky, Stanislav, and Lianrui Jia. “Branding Internet Sovereignty: Digital Media and the Chinese–Russian Cyberalliance.” *European Journal of Cultural Studies* 21, no. 5 (January 31, 2018): 594–613.
Burgess, Matt. “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.
Burnham, James. *The Struggle for the World*. London: Jonathan Cape, 1947.
Busvine, Douglas. “Exclusive: China’s Huawei Opens up to German Scrutiny Ahead of 5G Auctions.” *Reuters*, October 23, 2018. https://www.reuters.com/article/us-germany-telecoms-huawei-exclusive-idUSKCN1MX1VB.
Cardenal, Juan Pablo. “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.
Carr, Madeline. *US Power and the Internet in International Relations - The Irony of the Information Age*. Basingstoke, Hampshire: Palgrave Macmillan, 2016. www.palgrave.com/gp/book/9781137550231.
Carrapico, Helena, and André Barrinha. “The EU as a Coherent (Cyber)Security Actor?” *Journal of Common Market Studies* 55, no. 6 (2017): 1254–72. doi:10.1111/jcms.12575.

Cavandoli, Sofia. “The Unresolved Dilemma of Self-Determination: Crimea, Donetsk and Luhansk.” *The International Journal of Human Rights* 20, no. 7 (2016): 875–92.
Cave, Danielle. “The African Union Headquarters Hack and Australia’s 5G Network.” *The Strategist*, July 12, 2018. https://www.aspistrategist.org.au/the-african-union-headquarters-hack-and-australias-5g-network/.
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/.
Center for International Media Assistance - National Endowment for Democracy. “Surveillance for Sale: How China and Russia Export Repression Technology,” September 17, 2019. https://www.cima.ned.org/event/surveillance-for-sale-how-china-and-russia-export-repression-technology/.
Central Intelligence Agency. “Middle East: Bahrain — The World Factbook,” 2020. https://www.cia.gov/library/publications/the-world-factbook/geos/ba.html.
Centre for International Governance Innovation. “Centre for International Governance Innovation,” 2020. https://www.cigionline.org/search?search_api_fulltext=censorship&sort_by=publishing_or_event_date.
Checkel, Jeffrey T. *Ideas and International Political Change : Soviet/Russian Behavior and the End of the Cold War*. New Haven: Yale University Press, 1997.
———. “Process Tracing.” In *Qualitative Methods in International Relations : A Pluralist Guide*, edited by Audie Klotz and Deepa Prakash. Research Methods Series. Basingstoke: Palgrave Macmillan, 2008.
Chin, Josh. “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.
China Public Diplomacy Association. “Executives,” July 24, 2018. https://web.archive.org/web/20180724123348/http://www.chinapda.org.cn/eng/xhgk/cwls/.
Chinaka, Cris. “Zimbabwe Tense Over Anti-Mugabe Protests Call.” *Reuters*, March 1, 2011. https://www.reuters.com/article/ozatp-zimbabwe-protests-20110301-idAFJOE7200B320110301.
Chowdhury, Hasan. “Russia’s Test-Run for Its Alternative Internet a Success, Says Kremlin.” *The Telegraph*, December 24, 2019. https://www.telegraph.co.uk/technology/2019/12/24/russia-successfully-tests-sovereign-internet/.
CIPESA. “Online Freedoms,” 2020. https://cipesa.org/thematic-areas/online-freedoms/.
Citizen Lab. “About the Citizen Lab.” *The Citizen Lab*, 2020. https://citizenlab.ca/about/.
“Citizen Lab Summer Institute on Monitoring Internet Openness and Rights.” *The Citizen Lab*, 2019. https://citizenlab.ca/summerinstitute-2019/.
Clark, Marilyn, and Anna Grech. “Journalists Under Pressure - Unwarranted Interference, Fear and Self-Censorship in Europe.” Council of Europe, 2017. https://rm.coe.int/168070ad5d.
Clinton, Hillary. “Remarks on Internet Freedom.” *U.S. Department of State*, January 21, 2010. //2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

———. “Secretary Clinton Remarks Internet Freedom.” *C-SPAN*, January 1, 2010. https://www.c-span.org/video/?291518-1/secretary-clinton-remarks-internet-freedom.
Clinton, William J., and Albert J. Gore. “The Framework for Global Electronic Commerce,” 1997. https://clintonwhitehouse4.archives.gov/WH/New/Commerce/index.html.
“Clinton’s Words on China: Trade Is the Smart Thing.” *The New York Times*, March 9, 2000, sec. World. https://www.nytimes.com/2000/03/09/world/clinton-s-words-on-china-trade-is-the-smart-thing.html.
Cloudflare. “What Is IPsec? | How IPsec VPNs Work,” 2021. https://www.cloudflare.com/learning/network-layer/what-is-ipsec/.
Coca, Nithin. “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/.
Cohen, Louis, Lawrence Manion, and Keith Morrison. *Research Methods in Education*. 6th ed. London: Routledge, 2007.
Cohen, Noam. “Egyptians Were Unplugged, and Uncowed,” February 20, 2011. https://www.nytimes.com/2011/02/21/business/media/21link.html.
Congressional Research Service. “U.S. Sanctions on Russia: An Overview,” March 23, 2020. https://fas.org/sgp/crs/row/IF10779.pdf.
Connolly, William E. *The Terms of Political Discourse*. 3rd ed. Princeton, N.J.: Princeton University Press, 1993.
Council on Foreign Relations. “Ukraine’s Post-Independence Struggles,” 2020. https://www.cfr.org/timeline/ukraines-post-independence-struggles.
Cox, Joseph, 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.
Cozzi, Alessandro. “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.
Creemers, Rogier, Paul Triolo, and Graham Webster. “Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017).” *New America*, June 29, 2018. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.
Crete-Nishihata, Masashi, Ronald J. Deibert, and Adam Senft. “Not by Technical Means Alone: The Multidisciplinary Challenge of Studying Information Controls.” *IEEE Internet Computing* 17, no. 3 (May 2013): 34–41.
Currier, Cora, and Morgan Marquis-Boire. “A Detailed Look at Hacking Team’s Emails About Its Repressive Clients.” *The Intercept*, July 7, 2015. https://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/.
Cyberspace Administration of China. “Internet Forum Community Service Management Regulations,” August 25, 2017. http://www.cac.gov.cn/2017-08/25/c_1121541921.htm.
Dabrowski, Marek, Marta Domínguez-Jiménez, and Georg Zachmann. “Six Years After Ukraine’s Euromaidan: Reforms and Challenges Ahead,” June 30, 2020. https://www.bruegel.org/2020/06/six-years-after-ukraines-euromaidan-reforms-and-challenges-ahead/.

DAC Beachcroft. “Kazakhstan - Localization of Personal Data,” January 12, 2016. https://www.lexology.com/library/detail.aspx?g=303621d9-e5b7-4115-9d8c-2a5d1d40ed2c.
Dahlberg, Lincoln. “Oxford Research Encyclopedia of Communication,” 2017.
Dahua Technology. “Dahua IP Megapixel Solution Secures Government Office in Tanzania,” April 3, 2015. https://www.dahuasecurity.com/newsEvents/successStories/51/30.
Dałek, Jakub. *Russian Blacklist*. Python, 2018. https://github.com/jakubd/russian-blacklist.
Dehghan, Saeed Kamali. “Iran Protests See Reinvigorated Activists Take to the Streets in Thousands.” *The Guardian*, February 14, 2011, sec. World news. https://www.theguardian.com/world/2011/feb/14/iran-protests-reinvigorated-activists.
Deibert, Ronald, ed. *Access Controlled : The Shaping of Power, Rights, and Rule in Cyberspace*. Information Revolution & Global Politics. Cambridge, Mass.: MIT Press, 2010.
Deibert, Ronald. *Black Code: Inside the Battle for Cyberspace*. Toronto: Signal, 2013.
Deibert, Ronald J., and Masashi Crete-Nishihata. “Global Governance and the Spread of Cyberspace Controls.” *Global Governance* 18 (2012): 339–61.
DeNardis, Laura. *The Internet in Everything: Freedom and Security in a World With No off Switch*. New Haven: Yale University Press, 2020.
Department Of State. The Office of Electronic Information. “Global Internet Freedom Task Force (GIFT) Strategy: A Blueprint for Action,” December 28, 2006. https://2001-2009.state.gov/g/drl/rls/78340.htm.
Detektor Media. “Указом Про Санкції Президент Незаконно Зобов’язав Провайдерів Блокувати 192 Нових Сайти – «Лабораторія Цифрової Безпеки».” *Detector.Media*, May 25, 2018. https://detector.media/infospace/article/137834/2018-05-25-ukazom-pro-sanktsii-prezident-nezakonno-zobovyazav-provaideriv-blokuvati-192-novikh-saiti-laboratoriya-tsifrovoi-bezpeki/.
Devereaux, Ryan. “Border Official Admits Targeting Journalists and Human Rights Advocates With Smuggling Investigations.” *The Intercept*, May 17, 2019. https://theintercept.com/2019/05/17/border-smuggling-journalists-activists/.
Deyermond, Ruth. “The Uses of Sovereignty in Twenty-First Century Russian Foreign Policy.” *Europe-Asia Studies* 68, no. 6 (2016): 957–84.
Dickinson, Steve. “China’s New Cybersecurity Program: NO Place to Hide.” *China Law Blog*, September 30, 2019. https://www.chinalawblog.com/2019/09/chinas-new-cybersecurity-program-no-place-to-hide.html.
Digital Asia Hub. “Home,” 2020. https://www.digitalasiahub.org/.
Digital Freedom Fund. “About,” 2020. https://digitalfreedomfund.org/about/.
Digital Security Lab Ukraine. “At Least 56 Ukrainian Websites Are Blocked in Luhansk, and Almost Nothing in Donetsk, Research Proves.” *Medium*, September 21, 2018. https://medium.com/@cyberlabukraine/at-least-56-ukrainian-websites-are-blocked-in-luhansk-and-almost-nothing-in-donetsk-a-research-c01577830b8e.
———. “Лабораторія цифрової безпеки – Захищаємо громадянське суспільство,” 2020. https://dslua.org/.
Digital Society of Africa. “About,” 2020. https://www.digitalsociety.africa/.

Dixon, Robyn. “After Rioting, Zambia’s Acting President Reinstates Official.” *Los Angeles Times*, November 4, 2014. https://www.latimes.com/world/africa/la-fg-riots-zambia-20141104-story.html.

Donnelly, Jack, ed. “Anarchy, Hierarchy, and Order.” In *Realism and International Relations*, 81–106. Themes in International Relations. Cambridge: Cambridge University Press, 2000.

———. “International Human Rights: A Regime Analysis.” *Int Org* 40, no. 3 (1986): 599–642.

Doroshevich, Mikhail, and Maria Sokolova. “Internet Development and Usage.” In *Belarusian Yearbook 2012*, edited by Anatoly Pankovsky and Valeria Kostyugova. Minsk: Belarusian Institute for Strategic Studies, 2013.

Douglas, Bruce. “Brazil Debates Internet Law in Wake of NSA Scandal.” *BBC News*, November 12, 2013, sec. Technology. https://www.bbc.com/news/technology-24899396.

Dzirutwe, MacDonald. “No ‘Arab Spring’ in Zimbabwe, Mugabe Warns Protesters.” *Reuters*, August 26, 2016. https://www.reuters.com/article/us-zimbabwe-protest-idUSKCN1110Q6.

Eades, Mark C. “China’s Newest Export: Internet Censorship.” *US News & World Report*, January 30, 2014. https://www.usnews.com/opinion/blogs/world-report/2014/01/30/china-is-exporting-internet-censorship-to-iran.

Economy, Elizabeth C. “The Great Firewall of China: Xi Jinping’s Internet Shutdown.” *The Guardian*, June 29, 2018, sec. News. https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown.

ECPAT International. “REGIONAL OVERVIEW on Child Sexual Abuse Images through the Use of Information and Communication Technologies in Belarus, Moldova, Russia and Ukraine,” September 2008. https://www.ecpat.org/wp-content/uploads/2016/04/regional_overview.pdf.

EDRi. “About,” 2020. https://edri.org/about/.

Ekman, Alice, Sinikukka Saari, and Stanislav Secrieru. “STAND BY ME!: The Sino-Russian Normative Partnership in Action,” August 2020. https://www.iss.europa.eu/content/stand-me-sino-russian-normative-partnership-action.

El País. “Nicaragua’s Daniel Ortega Shows His True Colors,” August 8, 2016. https://english.elpais.com/elpais/2016/08/08/inenglish/1470656537_002840.html.

Elder, Miriam. “Clashes in Belarus After Thousands Turn out in Protest at Alleged Vote-Rigging.” *The Guardian*, December 20, 2010, sec. World news. https://www.theguardian.com/world/2010/dec/20/belarus-protest-alleged-vote-rigging.

———. “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.

Electronic Frontier Foundation. “A Not Terribly Brief History of the Electronic Frontier Foundation.” *Electronic Frontier Foundation*, July 15, 2014. https://www.eff.org/pages/not-terribly-brief-history-electronic-frontier-foundation.

———. “Home.” *Electronic Frontier Foundation*, 2020. https://www.eff.org/.

———. “Secretary of State Hillary Rodham Clinton Remarks on Internet Freedom,” February 15, 2011. https://www.eff.org/files/filenode/clinton_internet_rights_wrongs_20110215.pdf .
Ellick, Adam B., 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.
Elman, Colin. “Horses for Courses: Why Not Neorealist Theories of Foreign Policy?” *Security Studies* 6, no. 1 (1996): 7–53.
English, Robert. *Russia and the Idea of the West : Gorbachev, Intellectuals, and the End of the Cold War*. New York: Columbia University Press, 2000.
Equalit.ie. “Deflect Labs Report #6: Phishing and Web Attacks Targeting,” May 9, 2019. https://equalit.ie/deflect-labs-report-6/.
eQualitie. “Home,” 2020. https://equalit.ie/portfolio/censorship-no/.
Erdbrink, Thomas, and Rick Gladstone. “Clashes and Protest Over Iran Currency Plunge Hit Tehran - The New York Times,” October 3, 2012. https://www.nytimes.com/2012/10/04/world/middleeast/clashes-reported-in-tehran-as-riot-police-target-money-changers.html.
Erskine, Toni, and Madeline Carr. “Beyond ‘Quasi-Norms’: The Challenges and Potential of Engaging with Norms in Cyberspace.” In *International Cyber Norms: Legal, Policy & Industry Perspectives*, 87–109. Tallinn: NATO CCD COE, 2016. https://ccdcoe.org/multimedia/international-cyber-norms-legal-policy-industry-perspectives.html.
Etzioni, Amitai. “Spheres of Influence: A Reconceptualization.” *The Fletcher Forum of World Affairs* 39, no. 2 (Summer 2015): 117–32.
Eurasianet. “Kyrgyzstan: Bishkek Snoops Relying on Russian Spyware,” November 7, 2012. https://eurasianet.org/kyrgyzstan-bishkek-snoops-relying-on-russian-spyware.
European Parliament. “JOINT MOTION FOR A RESOLUTION on Kyrgyzstan, Homosexual Propaganda Bill,” January 14, 2015. https://www.europarl.europa.eu/doceo/document/RC-8-2015-0054_EN.html.
Evans, Jon. “‘The Dream Of Internet Freedom Is Dying.’” *TechCrunch*, August 5, 2015. https://social.techcrunch.com/2015/08/05/the-dream-of-internet-freedom-is-dying/.
Farley, Robert. “America Ruled the World in the 1990s - But It Doesn’t Anymore.” Text. *The National Interest*. The Center for the National Interest, December 20, 2020. https://nationalinterest.org/blog/reboot/america-ruled-world-1990s-it-doesnt-anymore-174709.
Fassbender, Bardo, Knut Traisbach, Douglas A. Johnson, and Kathryn Sikkink, eds. “Strategizing for Human Rights: From Ideals to Practice.” In *The Limits of Human Rights*. Oxford: Oxford University Press, 2019.
Federal Antimonopoly Service of the Russian Federation. “Yandex vs. Google,” June 27, 2016. http://en.fas.gov.ru/documents/documentdetails.html?id=14677.
Fellner, Sebastian. “Kabinett Bierlein Angelobt, Van Der Bellen Bittet Bevölkerung um Vertrauen.” 3 June 2019. *DER STANDARD*. Accessed April 16, 2021. https://www.derstandard.at/story/2000104268475/kabinett-bierlein-angelobt-van-der-bellen-bittet-bevoelkerung-um-vertrauen.

Feng, Emily. “Chinese Tech Groups Display Closer Ties with Communist Party.” *Financial Times*, October 10, 2017. https://www.ft.com/content/6bc839c0-ace6-11e7-aab9-abaa44b1e130.
Figliola, Patricia Moloney. “Promoting Global Internet Freedom: Policy and Technology,” October 22, 2013, 17.
Finnemore, Martha, and Duncan B. Hollis. “Constructing Norms for Global Cybersecurity.” *American Journal of International Law* 110, no. 3 (2016): 425–79.
Finnemore, Martha, and Kathryn Sikkink. “International Norm Dynamics and Political Change.” *International Organization* 52, no. 4 (1998): 887–917.
Flintoff, Corey. “Are ‘Color Revolutions’ A New Front In U.S.-Russia Tensions?” Accessed July 3, 2020. https://text.npr.org/s.php?sId=321392873.
Fontaine, Richard, and Kara Frederick. “The Autocrat’s New Tool Kit.” *Wall Street Journal*, March 15, 2019. https://www.wsj.com/articles/the-autocrats-new-tool-kit-11552662637.
Fontaine, Richard, and Will Rogers. “Internet Freedom: A Foreign Policy Imperative in the Digital Age.” Center for New American Security, June 2011. https://www.cnas.org/publications/reports/internet-freedom-a-foreign-policy-imperative-in-the-digital-age.
France 24. “Riots Erupt Amid Claims of Vote-Rigging,” September 22, 2011. https://www.france24.com/en/20110922-zambia-presidential-election-rupiah-banda-michael-sata-riots-erupt-rumours-vote-rigging.
Freedom House. “Countries and Territories.” *Freedom House*, 2020. https://freedomhouse.org/countries/freedom-world/scores.
———. “Egypt,” January 13, 2012. https://freedomhouse.org/report/freedom-net/2009/egypt.
———. “Freedom in the World 2018,” January 13, 2018. https://freedomhouse.org/report/freedom-world/freedom-world-2018.
———. “Freedom on the Net.” *Freedom House*, 2020. https://freedomhouse.org/report/freedom-net.
———. “Freedom on the Net 2018: The Rise of Digital Authoritarianism,” October 30, 2018. https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism.
———. “Kyrgyzstan,” 2019. https://freedomhouse.org/country/kyrgyzstan/freedom-net/2019.
———. “The Crisis of Social Media.” *Freedom House*, 2020. https://freedomhouse.org/report/freedom-net/2019/crisis-social-media.
———. “The Pandemic’s Digital Shadow.” *Freedom House*, 2020. https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow.
Freedom Info. “About Us,” 2021. http://www.freedominfo.org/about-us/.
Freedom Online Coalition. “FOC Issues Joint Statement on Freedom of Expression Online at the 47th Session of the United Nations Human Rights Council.” *Freedom Online Coalition*, July 4, 2021. https://freedomonlinecoalition.com/foc-issues-joint-statement-on-freedom-of-expression-online-at-the-47th-session-of-the-united-nations-human-rights-council/.
———. “History.” *Freedom Online Coalition*, 2020. https://freedomonlinecoalition.com/about-us/history/.
Freitas, Nathan. “The Great Firewall Inverts.” *Berkman Klein Center*, January 13, 2014. https://cyber.harvard.edu/events/luncheon/2015/01/freitas.

Gagliardone, Iginio. *China, Africa, and the Future of the Internet*. Zed Books, 2019.
Galeotti, Mark. "'RepressIntern': Russian Security Cooperation with Fellow Authoritarians." In *No Shelter: The Harassment of Activists Abroad by Intelligence Services from the Former Soviet Union*, edited by Adam Hug. London: The Foreign Policy Centre (FPC), 2016. https://fpc.org.uk/wp-content/uploads/2016/11/1786.pdf.
Gallacher, John D., 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.
Gallagher, Ryan. "Google's Censored Search Would Help China 'Be More Open,' Said Ex-CEO Eric Schmidt." *The Intercept*, May 14, 2019. https://theintercept.com/2019/05/14/google-search-china-eric-schmidt-comments/.
Gallagher, Sean. "For Decades, US and Germany Owned Swiss Crypto Company Used by 120 Countries." *Ars Technica*, November 2, 2020. https://arstechnica.com/tech-policy/2020/02/us-german-intel-owned-swiss-crypto-used-by-dozens-of-countries/.
———. "Photos of an NSA 'Upgrade' Factory Show Cisco Router Getting Implant." *Ars Technica*, May 14, 2014. https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/.
Ganguly, Sunayana. "A Constructivist Analysis Linking Norm Diffusion to Policy." Berlin, 2010. https://refubium.fu-berlin.de/bitstream/handle/fub188/18589/Ganguly-A_constructivist_analysis_linking_norm_diffusion-269.pdf?sequence=1&isAllowed=y.
Gaye, Frederick P. W. "China's $60M Ministerial Complex Project in Liberia Finally Begins." *People's Daily*, September 16, 2016. http://en.people.cn/n3/2016/0916/c90000-9115672.html.
———. "Chinese Medical Team Expands Services in Liberia." *People's Daily Online*, August 22, 2016. http://en.people.cn/n3/2016/0822/c90000-9103618.html.
Gaye, Fredrick. "China Completes Hand Pumps Project In Many Liberian Schools." Inprofiledaily, December 4, 2018. http://inprofiledaily.com/index.php/2018/12/04/china-completes-hand-pumps-project-in-many-liberian-schools/.
Gaye, Fredrick P. W. "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.
Geier, Ben. "What Did We Learn From the Dotcom Stock Bubble of 2000?" *Time*, March 12, 2015. https://time.com/3741681/2000-dotcom-stock-bust/.
Gerring, John. "What Is a Case Study and What Is It Good For?" *The American Political Science Review* 98, no. 2 (2004): 341–54.
Gerrits, André. "Normative Power in a Changing World: A Discussion." Clingendael, December 2009. https://www.clingendael.org/sites/default/files/pdfs/20091200_cesp_paper_gerrits.pdf.
Gessen, Masha. "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.
Giles, Keir. *Moscow Rules: What Drives Russia to Confront the West*. What Drives Russia to Confront the West. Washington, D.C. : London: Brookings Institution Press, 2019.
Gilpin, Robert. *U.S. Power and the Multinational Corporation : The Political Economy of Foreign Direct Investment*. Political Economy of International Relations Series. New York: Basic Books, 1975.
Gladstone, Nikki. "Thank You for a Historic RightsCon Online." *RightsCon Summit Series*, July 31, 2020. https://www.rightscon.org/thank-you-for-a-historic-rightscon-online/.
Global Network Initiative. "GNI Home." *Global Network Initiative*. Accessed October 16, 2019. https://globalnetworkinitiative.org/.
———. "The GNI Principles." *Global Network Initiative*, 2020. https://globalnetworkinitiative.org/gni-principles/.
Global Voices. "Self-Proclaimed 'Donetsk People's Republic' Now Has an Internet Blacklist," June 17, 2015. https://globalvoices.org/2015/06/17/self-proclaimed-donetsk-peoples-republic-now-has-an-internet-blacklist/.
Gold, Hadas. "UK Bans Huawei From Its 5G Network." *CNN*, July 14, 2020. https://edition.cnn.com/2020/07/14/tech/huawei-uk-ban/index.html.
Goldsmith, Jack. "The Failure of Internet Freedom." *Knight First Amendment Institute at Columbia University*, June 2018. https://knightcolumbia.org/content/failure-internet-freedom.
Goldsmith, Jack L, and Tim Wu. *Who Controls the Internet?: Illusions of a Borderless World*. New York: Oxford University Press, 2006.
Golubev, Vladimir. "Fighting Cybercrime in CIS: Strategy and Tactics." *Computer Crime Research Center*, June 29, 2005. http://www.crime-research.org/articles/golubev_Jul/.
Google. "Enabling Trade in the Era of Information Technologies: Breaking Down Barriers to the Free Flow of Information," November 15, 2010. https://static.googleusercontent.com/media/www.google.com/de//googleblogs/pdfs/trade_free_flow_of_information.pdf.
Google Maps. "Kerch Strait." *Google Maps*, June 13, 2020. https://goo.gl/maps/Qc553yB7DfFXRp116.
Gorenburg, Dmitry. "External Support for Central Asian Military and Security Forces." SIPRI, January 2014. https://www.sipri.org/sites/default/files/SIPRI-OSFno1WP.pdf.
Gould, Joe. "US Senate Upholds Arms Sales to Bahrain, Qatar." *Defense News*, June 13, 2019. https://www.defensenews.com/congress/2019/06/13/us-senate-upholds-arms-sales-to-bahrain-qatar/.
Government and the People's Council of the DPR. "The Next Meeting of the People's Council of the DPR," May 30, 2015. https://web.archive.org/web/20150530084135/http://dnr-online.ru/news/sostoyalos-ocherednoe-zasedanie-narodnogo-soveta-dnr-2/.
Government of Egypt. "2018 Cybercrime Law," May 1, 2018. https://www.youm7.com/story/2018/5/1/تعرف-على-كيفية-التصالح-فى-الجرائم-الإلكترونية-وفقا-للقانون-الجديد/3773230.
Government of India - Press Information Bureau. "Government Bans 59 Mobile Apps Which Are Prejudicial to Sovereignty and Integrity of India, Defence of India,

Security of State and Public Order," June 29, 2020. pib.gov.in/Pressreleaseshare.aspx?PRID=1635206.
Government of the Republic of Kazakhstan. "Утвержден План Мероприятий По Реализации Концепции Кибербезопасности («Киберщит Казахстана») До 2022 Год (Аннотация к Документу От 28.10.2017)." *Zakon.Kz*, November 1, 2017. https://www.zakon.kz/4886464-utverzhden-plan-meropriyatiy-po.html.
Government of Vietnam. "Cybersecurity Law," June 12, 2018. http://tulieuvankien.dangcongsan.vn/he-thong-van-ban/van-ban-quy-pham-phap-luat/luat-an-ninh-mang-so-242018qh14-ngay-1262018-hieu-luc-thi-hanh-tu-ngay-01012019-4474.
Government of Zimbabwe. "Interception of Communications Act [Chapter 11:20]." *Veritaszim*, 2007. http://www.veritaszim.net/node/252.
Grace, Ryan. "Shatter the Web: Internet Fragmentation in Iran." *Middle East Institute*, December 14, 2020. https://www.mei.edu/publications/shatter-web-internet-fragmentation-iran.
Gray, Colin S. *The Future of Strategy*. Cambridge: Polity, 2015.
GreatFire.org. "Home," 2020. https://en.greatfire.org/.
Greenberg, Andy. "It's Been 20 Years Since John Perry Barlow Declared Cyberspace Independence." *Wired*, February 8, 2016. https://www.wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence/.
Greenstein, Fred I. "The Impact of Personality on the End of the Cold War: A Counterfactual Analysis." *Political Psychology* 19, no. 1 (1998): 1–16.
Greenwald, Glenn. "Glenn Greenwald: How the NSA Tampers With US-Made Internet Routers." *The Guardian*, May 12, 2014, sec. US news. https://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden.
Grieco, J. M. "Understanding the Problem of International Cooperation: The Limits of Neoliberal Institutionalism and the Future of Realist Theory." In *Neo- Realism and Neoliberalism: The Contemporary Debate*, edited by D. A. Baldwin. New York, N.Y.: Columbia University Press, 1993.
Grieco, Joseph M. "Anarchy and the Limits of Cooperation: A Realist Critique of the Newest Liberal Institutionalism." *International Organization* 42, no. 3 (1988): 485–507.
Griffiths, James. *The Great Firewall of China : How to Build and Control an Alternative Version of the Internet*. London: Zed Books, 2019.
Grunow, Florian, and Niklaus Schiess. "Lecture: Lifting the Fog on Red Star OS." *Chaos Computer Club*, December 27, 2015. https://fahrplan.events.ccc.de/congress/2015/Fahrplan/events/7174.html.
Guardian Project. "About." *Guardian Project*, 2020. https://guardianproject.info/.
Gvalia, Giorgi, Bidzina Lebanidze, and David S. Siroky. "Neoclassical Realism and Small States: Systemic Constraints and Domestic Filters in Georgia's Foreign Policy." *East European Politics* 35, no. 1 (January 2, 2019): 21–51. doi:10.1080/21599165.2019.1581066.
Haas, Benjamin. "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.
Hackel, Joyce. "When the Internet Goes Down in North Korea, There Aren't Many to Notice." *The World from PRX*, December 23, 2014.

https://www.pri.org/stories/2014-12-23/when-internet-goes-down-north-korea-theres-not-many-notice.
Hakim, Danny. “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.
Han, Rongbin. “Manufacturing Consent in Cyberspace: China’s ‘Fifty-Cent Army.’” *Journal of Current Chinese Affairs* 2 (2015): 105–34.
Hansen, Robert. “North Korea’s Naenara Web Browser: It’s Weirder Than We Thought | WhiteHat Security Blog,” January 8, 2015. https://web.archive.org/web/20150108223420/https://blog.whitehatsec.com/north-koreas-naenara-web-browser-its-weirder-than-we-thought/.
Hansler, Jennifer, and Brian Stelter. “‘Wednesday Night Massacre’ as Trump Appointee Takes Over at Global Media Agency.” *CNN*, June 18, 2020. https://www.cnn.com/2020/06/17/media/us-agency-for-global-media-michael-pack/index.html.
Hao, Karen. “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/.
Harmon, Elliot. “Once Again, DMCA Abused to Target Political Ads.” *Electronic Frontier Foundation*, November 17, 2015. https://www.eff.org/deeplinks/2015/11/once-again-dmca-abused-target-political-ads.
Hasenclever, Andreas, Peter Mayer, and Volker Rittberger. *Theories of International Regimes*. Cambridge Studies in International Relations. Cambridge: Cambridge University Press, 1997.
Hast, Susanna. *Spheres of Influence in International Relations : History, Theory and Politics*. Burlington, VT: Ashgate Pub. Company, 2014.
Hawkins, Amy. “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/.
Hayes, Andrew F., 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.
He, Huifeng. “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.
Hechter, Michael, and Satoshi Kanazawa. “Sociological Rational Choice Theory.” *Annual Review of Sociology* 23 (1997): 191.
Helmus, Todd C., Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman. “Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe.” Product Page. RAND Corporation, 2018. https://www.rand.org/pubs/research_reports/RR2237.html.
Henry, Ryan, Stacie L. Pettyjohn, and Erin York. “Portfolio Assessment of the Department of State Internet Freedom Program.” RAND Corporation, 2014. https://www.rand.org/content/dam/rand/pubs/research_reports/RR700/RR794/RAND_RR794.pdf.

Hersher, Rebecca. “North Korea Accidentally Reveals It Only Has 28 Websites.” *NPR.Org*. Accessed December 28, 2020. https://www.npr.org/sections/thetwo-way/2016/09/21/494902997/north-korea-accidentally-reveals-it-only-has-28-websites.

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.

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

———. “Hikvision Helping Bangkok’s Police Force Stay Ahead of the Curve-Hikvision,” July 11, 2012. https://webcache.googleusercontent.com/search?q=cache:05fh0kJfhrIJ:https://www.hikvision.com/uk/Press/Success-Stories/Government/305528970582113+&cd=1&hl=en&ct=clnk&gl=uk.

———. “Hikvision Protects Ministry of Commerce (MOC) Thailand,” June 24, 2010. https://webcache.googleusercontent.com/search?q=cache:QlraCG2ayrkJ:https://www.hikvision.com/europe/News--Events/Success-Stories/Government/305528969213861+&cd=1&hl=en&ct=clnk&gl=uk.

Hill, Wiliam H. “Unrecognized Actors from Unrecognized States: Moscow’s Puppets or Inevitable Interlocutors.” European Leadership Network, November 2017. https://www.europeanleadershipnetwork.org/wp-content/uploads/2017/11/171117-William-H.-Hill-Unrecognized-Actors-from-Unrecognized-States.pdf.

Hogg, Chris. “China Restores Xinjiang Internet,” May 14, 2010. http://news.bbc.co.uk/1/hi/world/asia-pacific/8682145.stm.

Holsti, Olavi Rudolf. “Theories of Crisis Decision-Making.” In *Diplomacy: New Approaches in History, Theory, and Policy*, 99–136. New York: Free Press, n.d.

Hopkins, Nick, and Jake Morris. “UK Firm’s Surveillance Kit ‘Used to Crush Uganda Opposition.’” *BBC News*, October 15, 2015, sec. UK. https://www.bbc.com/news/uk-34529237.

Huawei. “Huawei Smart City Overview Presentation.” *Huawei Enterprise*, 2018. https://e.huawei.com/en/material/onLineView?MaterialID=02ad4d5ab608492ea24659ec667f04bd.

Hughes, William J. “H.R.3889 - 100th Congress (1987-1988): Child Protection and Obscenity Enforcement Act of 1988.” Webpage, November 18, 1988. 1987/1988. https://www.congress.gov/bill/100th-congress/house-bill/3889.

Human Rights Watch. “China: How Mass Surveillance Works in Xinjiang,” May 1, 2019. https://www.hrw.org/news/2019/05/01/china-how-mass-surveillance-works-xinjiang.

———. “Descent into Chaos | Thailand’s 2010 Red Shirt Protests and the Government Crackdown.” *Human Rights Watch*, May 3, 2011. https://www.hrw.org/report/2011/05/03/descent-chaos/thailands-2010-red-shirt-protests-and-government-crackdown.

———. “Freedom of Expression and the Internet in China.” Washington, D.C., 2001. https://www.hrw.org/legacy/backgrounder/asia/china-bck-0701.pdf.

———. “Iran: Violent Crackdown on Protesters Widens.” *Human Rights Watch*, June 23, 2009. https://www.hrw.org/news/2009/06/23/iran-violent-crackdown-protesters-widens.

———. “The Right to Privacy in Uzbekistan,” June 2015. https://privacyinternational.org/sites/default/files/2017-12/PI%20submission%20Uzbekistan.pdf.
———. “Ukraine,” 2003. https://www.hrw.org/reports/2003/ukraine0303/Ukraine0303.pdf.
———. “Vietnam: Crackdown on Peaceful Environmental Protesters,” May 18, 2016. https://www.hrw.org/news/2016/05/19/vietnam-crackdown-peaceful-environmental-protesters.
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.
Ikeda, Scott. “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/.
Imbrie, Andrew, Ryan Fedasiuk, Catherine Aiken, Tarun Chhabra, and Husanjot Chahal. “Agile Alliances,” February 2020. https://cset.georgetown.edu/research/agile-alliances/.
Interfax - Ukraine. “Боевики ОРДЛО Вводят Внешнее Управление На Предприятиях Под Украинской Юрисдикцией На Временно Оккупированных Территориях - Источник.” *Интерфакс-Украина*, March 1, 2017. https://interfax.com.ua/news/general/406251.html.
International Religious Freedom Roundtable. “Template Multi-Faith Letter.” *21Wilberforce*, 2020. https://wilberforce.salsalabs.org/internetfreedom/index.html.
Internet Assigned Numbers Authority. “Patrik Fallström,” July 28, 2014. https://www.ianacg.org/icg-files/bios/bio-falstrom-28jul14-en.pdf.
Internet Freedom Festival. “Partners and Supporters.” *Internet Freedom Festival*, 202AD. https://internetfreedomfestival.org/partners-supporters/.
Internet Svoboda. “Напередодні Українських Виборів СБУ Пропонує Заблокувати Нові 100 Інтернет-Сайтів,” February 12, 2019. https://netfreedom.org.ua/article/naperedodni-ukrayinskih-viboriv-sbu-proponuye-zablokuvati-novi-100-internet-sajtiv.
IPVM. “First US State, Vermont, Bans Dahua and Hikvision,” 01:31 500. https://ipvm.com/reports/vermont-hikua.
IREX. “Internet Freedom Festival,” 2020. http://www.irex.org/project/internet-freedom-festival.
Ishay, Micheline. “Historical Strategies for Human Rights.” In *The Limits of Human Rights*, edited by Bardo Fassbender and Knut Traisbach. Oxford: Oxford University Press, 2019.
ISMS. “Backdoor (Computing).” *ISMS.Online*, December 14, 2020. https://www.isms.online/glossary/backdoor-computing/.
Jackson, Van. “Understanding Spheres of Influence in International Politics.” *European Journal of International Security*, n.d., 1–19.
Janeliūnas, Tomas. “‘Sovereign Democracy’ - Yet Another Attempt to Define Russia’s Regime.” *Lithuanian Foreign Policy Review*, no. 18 (2006): 117–32.
Jansen Reventlow, Nani, and Jonathan McCully. “Internet Freedom Without Imperialism.” *Knight First Amendment Institute*, June 13, 2018. https://knightcolumbia.org/content/internet-freedom-without-imperialism.
Jervis, Robert. “Security Regimes.” *Int Org* 36, no. 2 (1982): 357–78.
Jigsaw. “Issues,” 2020. https://jigsaw.google.com/issues/.

Jones, Howard. “Mistaken Prelude to Vietnam: The Truman Doctrine and ‘A New Kind of War’ in Greece.” *Journal of Modern Greek Studies* 10, no. 1 (1992): 121.
Judah, Tim. *In Wartime: Stories from Ukraine*. Great Britain: Penguin Random House UK, 2015.
Kadercan, Burak. “Making Sense of Survival: Refining the Treatment of State Preferences in Neorealist Theory.” *Review of International Studies* 39, no. 4 (2013): 1015–37.
Kafeero, Stephen. “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/.
Katzenstein, Peter J. *The Culture of National Security : Norms and Identity in World Politics*. New Directions in World Politics. New York: Columbia University Press, 1996.
Kaufman, Edy. *The Superpowers and Their Spheres of Influence : The United States and the Soviet Union in Eastern Europe and Latin America*. London: Croom Helm, 1976.
Kavalski, Emilian. “Normative Power Beyond the Eurocentric Frame.” Oxford Bibliographies, August 28, 2018. https://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0239.xml.
Kaye, David. “The Limits of Supply-Side Internet Freedom,” June 13, 2018. https://knightcolumbia.org/content/limits-supply-side-internet-freedom.
Keal, Paul. “Contemporary Understanding About Spheres of Influence.” *Rev. Int. Stud.* 9, no. 3 (1983): 155–72.
Keck, Margaret E., and Kathryn Sikkink. *Activists beyond Borders*. Cornell University Press, 1998.
Kello, Lucas. *The Virtual Weapon and International Order*. New Haven, CT: Yale University Press, 2017.
Keohane, Robert O. “The Demand for International Regimes.” *International Organization* 36, no. 2 (1982): 325–55.
Keohane, Robert O, and Joseph S Nye. *Power and Interdependence*. 2nd ed. New York: Longman, 1989.
Kerr, Jaclyn. “The Russian Model of Internet Control and Its Significance.” LLNL-TR-764577. Lawrence Livermore National Laboratory, December 21, 2018.
Khalil, Lydia. “Digital Authoritarianism, China and COVID.” *Lowy Institute*, November 2, 2020. https://www.lowyinstitute.org/publications/digital-authoritarianism-china-and-covid.
KICTAnet. “About KICTANET | KICTANet Think Tank.” Accessed July 31, 2020. https://www.kictanet.or.ke/about-kictanet/.
Kinetz, Erika. “In China, Your Car Could Be Talking to the Government.” *AP NEWS*, November 29, 2018. https://apnews.com/c6e610eb8f4645b4806bc16479b64809.
King, Gary, Robert O Keohane, and Sidney Verba. *Designing Social Inquiry : Scientific Inference in Qualitative Research*. Scientific Inference in Qualitative Research. Princeton, New Jersey: Princeton University Press, 1994.
King, Gary, 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.

Kingsbury, Benedict. “Krasner, Stephen D. ‘Sovereignty: Organized Hypocrisy’ (Book Review).” Edited by Richard Bilder. *American Journal of International Law* 94, no. 3 (2000): 591.

Klotz, Audie, and Cecelia Lynch. *Strategies for Research in Constructivist International Relations*. International Relations in a Constructed World. Armonk, N.Y.: M.E. Sharpe, 2007.

KM.RU. “Rostelecom Launches Cable Laid to Crimea,” October 28, 2018. https://web.archive.org/web/20181028002313/http://www.km.ru/economics/2014/04/28/ministerstvo-svyazi-i-massovykh-kommunikatsii-rf/738619-rostelekom-zapustil-v-e.

Knorr Mackensie. “Why Did Russia Let the Republics Go? Revisiting the Fall of the USSR | Wilson Center,” 2017. https://www.wilsoncenter.org/publication/why-did-russia-let-the-republics-go-revisiting-the-fall-the-ussr.

Kogan Rami. “Bedep Trojan Malware Spread by the Angler Exploit Kit Gets Political.” *Trustwave*, April 29, 2015. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/bedep-trojan-malware-spread-by-the-angler-exploit-kit-gets-political/.

Kontorovich, Vladimir. “The Economic Fallacy.” *The National Interest*, no. 31 (1993): 35–45.

Korolev, Igor. “ДНР и ЛНР Полностью Переключили Магистральный Трафик На Россию.” *CNews.Ru*, January 9, 2019. https://www.cnews.ru/news/top/2019-01-08_dnr_i_lnr_polnostyu_pereklyuchili_magistralnyj.

Koslowski, Rey, and Friedrich V Kratochwil. “Understanding Change in International Politics: The Soviet Empire’s Demise and the International System.” *International Organization* 48, no. 2 (1994): 215–47.

Krasner, Stephen. “Transforming International Regimes: What the Third World Wants and Why.” *International Studies Quarterly* 25, no. 1 (1981): 119.

Krasner, Stephen D. *Sovereignty: Organized Hypocrisy*. Princeton, N.J.: Princeton University Press, 1999.

———. “Structural Causes and Regime Consequences: Regimes as Intervening Variables.” *International Organization* 36, no. 2 (1982): 185–205.

Krastev, Ivan. “‘Sovereign Democracy’, Russian-Style.” *Insight Turkey* 8, no. 4 (December 2006): 113–17.

Kratochwil, Friedrich. “The Embarrassment of Changes: Neo-Realism as the Science of Realpolitik Without Politics.” *Review of International Studies* 19, no. 1 (1993): 63–80.

Kucera, Joshua. “With Eye To Arab Spring, CSTO Strengthens Cyber, Military Powers.” *Eurasianet*, August 15, 2011. https://eurasianet.org/with-eye-to-arab-spring-csto-strengthens-cyber-military-powers.

Kuo, Lily. “China Bans 23m From Buying Travel Tickets as Part of ‘Social Credit’ System.” *The Guardian*, March 1, 2019, sec. World news. https://www.theguardian.com/world/2019/mar/01/china-bans-23m-discredited-citizens-from-buying-travel-tickets-social-credit-system.

Kyrgyz Ministry of Justice. “Инструкция о Порядке Взаимодействия Операторов Электросвязи и Операторов Мобильной Сотовой Связи с Государственными Органами Кыргызской Республики, Осуществляющими Оперативно-Розыскную Деятельность,” June 30, 2014. https://web.archive.org/web/20191026180458/http://cdb.minjust.gov.kg:80/act/view/ru-ru/96622.

Kyrgyz Republic's State Committee for National Security. "Об Утверждении Правил Внутреннего Распорядка Изоляторов Временного Содержания Органов Национальной Безопасности Кыргызской Республики," August 17, 2012. https://web.archive.org/web/20130902225513/http://www.gknb.kg/index.php?option=com_content&view=category&layout=blog&id=29&Itemid=57.

Lake, David A. "The New Sovereignty in International Relations." *International Studies Review* 5, no. 3 (2003): 303–23.

Landler, Mark, and Brian Stelter. "Washington Taps Into a Potent New Force in Diplomacy." *The New York Times*, June 16, 2009, sec. Middle East. https://www.nytimes.com/2009/06/17/world/middleeast/17media.html.

Lantis, Jeffrey S. "Theories of International Norm Contestation: Structure and Outcomes." Oxford Research Encyclopedia of Politics. http://politics.oxfordre.com/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-590, June 2017.

Lantis, Jeffrey S, and Daniel J Bloomberg. "Changing the Code? Norm Contestation and US Antipreneurism in Cyberspace." *International Relations* 32, no. 2 (March 13, 2018): 149–72. doi:10.1177/0047117818763006.

Lazitski, Olga. "Media Endarkenment: A Comparative Analysis of 2012 Election Coverage in the United States and Russia." Edited by J. Gregory Payne. *American Behavioral Scientist* 58, no. 7 (2014): 898–927.

Lee, Catherine H. "To Thine Own Self Be True: IMF Conditionality and Erosion of Economic Sovereignty in the Asian Financial Crisis.(International Monetary Fund)." *University of Pennsylvania Journal of International Economic Law* 24, no. 4 (2003): 875–904.

Lee, Kai-Fu. "The Real Threat of Artificial Intelligence." *The New York Times*, June 24, 2017. https://www.nytimes.com/2017/06/24/opinion/sunday/artificial-intelligence-economic-inequality.html.

Leetaru, Kalev. "The Death Of Internet Freedom: Mourning The Demise Of A 20-Year-Old Dream." *Forbes*, February 17, 2016. https://www.forbes.com/sites/kalevleetaru/2016/02/17/the-death-of-internet-freedom-mourning-the-demise-of-a-20-year-old-dream/.

Lefebvre, Stéphane, and Roger N Mcdermott. "Russia and the Intelligence Services of Central Asia." *International Journal of Intelligence and CounterIntelligence* 21, no. 2 (2008): 251–301.

Letain, Margot. "The 'Denim Revolution': A Glass Half Full." *OpenDemocracy*, April 10, 2006. https://www.opendemocracy.net/en/denim_3441jsp/.

Levitsky, Steven, and Lucan Way. *Competitive Authoritarianism : Hybrid Regimes After the Cold War*. Problems of International Politics. New York: Cambridge University Press, 2010.

———. "Linkage Versus Leverage: Rethinking the International Dimension of Regime Change." *Comparative Politics* 38, no. 4 (2006): 379–400. doi:10.2307/20434008.

Li, Jeffrey (Chien-Fei). "Internet Control or Internet Censorship? Comparing the Control Models of China, Singapore, and the United States to Guide Taiwan's Choice." *Pittsburgh Journal of Technology Law and Policy* 14, no. 1 (2014): 1–43.

Lianyungang Forum. "Focusing on 'Made in China' Weapons and Strong Police Prestige." Accessed March 14, 2020. http://www.lygforum.gov.cn/index.php?m=news&a=details&content_id=306.

———. “Participating Countries and Organizations.” Accessed March 14, 2020. http://www.lygforum.gov.cn/index.php?m=countries&a=index&classify_id=209.
———. “The 4th Lianyungang Forum Was Successfully Held,” 2018. http://www.lygforum.gov.cn/index.php?m=news&a=details&content_id=294.
———. “The First Training Seminar on Law Enforcement Cooperation of the New Asia-Europe Continental Bridge Security Corridor,” 2017. http://www.lygforum.gov.cn/index.php?m=news&a=details&content_id=318.
———. “即使不露脸，照样知道你是谁,” November 23, 2018. http://www.lygforum.gov.cn/english.php?m=news&a=details&content_id=535.
Liga.net. “Smart City - Города с Разумом.” Accessed May 1, 2019. http://www.liga.net/projects/smart_city/.
Lim, Gabrielle. “Disinformation Annotated Bibliography.” Citizen Lab, May 2019. https://citizenlab.ca/wp-content/uploads/2019/05/Disinformation-Bibliography.pdf.
Lim, Louisa, 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.
Litera, Bohuslav. “The Kozyrev Doctrine - a Russian Variation on the Monroe Doctrine.” *Perspectives*, no. 4 (1994): 45–52.
Lobell, Steven E, Jeffrey W Taliaferro, and Norrin M Ripsman. “A Methodology of Neoclassical Realism.” In *Neoclassical Realist Theory of International Politics*, Vol. Oxford University Press. New York: New York: Oxford University Press, 2016.
Lokot, Tetyana. “Ukrainian MP Pushes for Carbon Copy Of Russian Blogger Law, Meets Resistance.” *Global Voices*, February 16, 2015. https://globalvoices.org/2015/02/16/ukraine-russia-blogger-law/.
———. “Ukrainian Separatists Block 100+ News Websites in ‘Lugansk People’s Republic’ · Global Voices.” *Global Voices*, January 14, 2016. https://globalvoices.org/2016/01/14/ukrainian-separatists-block-100-news-websites-in-lugansk-peoples-republic/.
Long, Tom, and Francisco Urdinez. “Status at the Margins: Why Paraguay Recognizes Taiwan and Shuns China.” *Foreign Policy Analysis*, 2020. https://academic.oup.com/fpa/advance-article-abstract/doi/10.1093/fpa/oraa002/5825378?redirectedFrom=fulltext.
Long, Trinh Huu. “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/.
Longanecker, Mindy K. “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.
Loudon Virginia. “Business & Industry Stats.” *Loudon County Economic Development, VA*, n.d. https://biz.loudoun.gov/information-center/business-industry-stats/.
Luhansk People’s Republic. “Luhan People’s Republic of Law About the Media,” November 7, 2014. https://nslnr.su/zakonodatelstvo/normativno-pravovaya-baza/906/.
———. “Госкомнадзор Минкомсвязи ЛНР.” *Министерство Связи и Массовых Коммуникаций Луганской Народной Республики*, 2020. https://mslnr.su/goskomnadzor.html.

Lyngaas, Sean. “How Uzbekistan’s Security Service (Allegedly) Began Developing Its Own Malware.” *CyberScoop*, October 3, 2019. https://www.cyberscoop.com/uzbekistan-sandcat-kaspersky/.
Lyon, David. “Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique.” *Big Data & Society* 1, no. 2 (2014).
Maass, Dave, and Cindy Cohn. “A Warning to Know Your Customer: Computerlinks Fined for Dealing Blue Coat Surveillance Technology to Syria.” *Electronic Frontier Foundation*, May 28, 2013. https://www.eff.org/deeplinks/2013/05/blue-coat-syria-scandal-next-shoe-drops-computerlinks-fzco.
MacAskill, Ewen, Gabriel Dance, Feilding Cage, Greg Chen, and Nadja Popovich. “NSA Files Decoded: Edward Snowden’s Surveillance Revelations Explained.” *The Guardian*, November 1, 2013. http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded.
MacFarquhar, Neil. “Vladimir Putin, in First Remarks on Russian Protests, Warns of Potential Chaos.” *The New York Times*, March 30, 2017, sec. World. https://www.nytimes.com/2017/03/30/world/europe/putin-russia-protests.html.
Mackinder, Halford John. *Democratic Ideals and Reality : A Study in the Politics of Reconstruction*. London: Constable, 1919.
MacKinnon, Rebecca. “It’s Not Too Late to Save the Internet.” *Slate Magazine*, August 19, 2020. https://slate.com/technology/2020/08/save-the-internet.html.
———. “The U.S. Just Undercut Its Mission to Support Internet Freedom Worldwide.” *Slate Magazine*, June 26, 2020. https://slate.com/technology/2020/06/us-open-technology-fund-hong-kong-protest.html.
———. “Yahoo! Abomination. (YHOO).” *RConversation*, March 29, 2006. https://rconversation.blogs.com/rconversation/2006/03/yahoo_abominati.html.
Madory, Doug. “No Turning Back: Russia Activates Crimean Cable,” July 31, 2014. https://dyn.com/blog/no-turning-back-russia-crimea/.
Mahoney, James. “Process Tracing and Historical Explanation.” *Security Studies* 24, no. 2 (2015): 200–218.
Mallett-Outtrim, Ryan. “30,000 More Security Cameras and 17,000 Less Guns on Venezuelan Streets.” *Venezuelanalysis.Com*, November 27, 2013. https://venezuelanalysis.com/news/10198.
Manancourt, Vincent. “The Demise of Privacy Shield May Be the End of US-Europe Data Transfers.” *POLITICO*, August 3, 2020. https://www.politico.eu/article/privacy-shield-is-dead-long-live-data-localization/.
Manson, Katrina. “US Boosts Funding of Tech Companies to Help Anti-Tehran Protests.” *Financial Times*, January 19, 2020. https://www.ft.com/content/740a385a-3924-11ea-a6d3-9a26f8c3cba4.
Manyika, James, and Charles Roxburgh. “The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity.” *McKinsey*, October 1, 2011. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-great-transformer.
March, James G., and Johan P. Olsen. “The Institutional Dynamics of International Political Orders.” *International Organization* 52, no. 4 (1998): 943.
Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. “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/.
Mardell, Jacob. “The ‘Community of Common Destiny’ in Xi Jinping’s New Era.” Accessed March 16, 2020. https://thediplomat.com/2017/10/the-community-of-common-destiny-in-xi-jinpings-new-era/.
Marima, Tendai. “Violence Erupts Days Ahead of Uganda Elections,” February 16, 2016. https://www.aljazeera.com/news/2016/02/uganda-opposition-leader-arrested-days-elections-160215132155444.html.
Mason, Jennifer. *Qualitative Researching*. 2nd ed. Sage Publications, 2002.
Maurer, Tim. “Cyber Norm Emergence at the United Nations – An Analysis of the UN‘s Activities Regarding Cyber-Security.” Explorations in Cyber International Relations Discussion Paper Series. Belfer Center for Science and International Affairs, September 2011. https://www.belfercenter.org/sites/default/files/legacy/files/maurer-cyber-norm-dp-2011-11-final.pdf.
McCaul, Michael T. “Text - H.R.6621 - 116th Congress (2019-2020): Open Technology Fund Authorization Act.” Webpage, April 24, 2020. 2019/2020. https://www.congress.gov/bill/116th-congress/house-bill/6621/text.
McDermott, Roger. “Central Asian Security Post - 2014.” Danish Institute for International Studies, 2013. https://www.diis.dk/files/media/publications/import/extra/rp2013-12-mcdermott-kazakhstan_web.jpg_1.pdf.
———. “CSTO Moves Into The Information Age.” *RadioFreeEurope/RadioLiberty*, September 4, 2011. https://www.rferl.org/a/commentary_csto_moves_into_information_age/24317363.html.
McDonell, Stephen. “WeChat and the Surveillance State.” *BBC News*, June 7, 2019, sec. China blog. https://www.bbc.com/news/blogs-china-blog-48552907.
McGonigle, Brendan. “Yandex Catches Google on Android in Russia.” *Russian Search Marketing*, August 28, 2018. https://russiansearchmarketing.com/yandex-catches-google-on-android-in-russia/.
McLaughlin, Jenna, and Zach Dorfman. “‘Shattered’: Inside the Secret Battle to Save America’s Undercover Spies in the Digital Age,” December 30, 2019. https://news.yahoo.com/shattered-inside-the-secret-battle-to-save-americas-undercover-spies-in-the-digital-age-100029026.html.
McVeigh, Karen. “Over 100,000 Have Fled Nicaragua Since Brutal 2018 Crackdown, Says UN.” *The Guardian*, March 11, 2020, sec. Global development. https://www.theguardian.com/global-development/2020/mar/11/over-100000-have-fled-nicaragua-since-brutal-2018-crackdown-says-un.
Mearsheimer, John J. *The Tragedy of Great Power Politics*. New York, N.Y.: W. W. Norton & Company, 2001.
Medvedev, Dmitry. “Дмитрий Медведев on Twitter.” *Twitter*, March 24, 2014. https://twitter.com/MedvedevRussia/status/448048962474225664.
Megaloudi, Fragkiska. “Transforming the World’s Most Isolated Nation.” *Al Jazeera*, December 18, 2014. https://www.aljazeera.com/features/2014/12/18/transforming-the-worlds-most-isolated-nation.
Meiches, Benjamin, and Raymond Hopkins. “Regime Theory.” *Oxford Research Encyclopedia of International Studies*, 2018.
Meiya Pico. “Training,” 2019. https://meiyapico.com/training/index.html.

"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.

Melvin, Neil, and Tolkun Umaraliev. "New Social Media and Conflict in Kyrgyzstan." SIPRI Insights on Peace and Security. Stockholm: SIPRI, August 2011. https://www.sipri.org/sites/default/files/files/insight/SIPRIInsight1101.pdf.

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.

Merkel-Hess, Kate, and Jeffrey N. Wasserstorm. "Will the Real Chinese Internet Please Stand Up?" *Dissent Magazine*, February 11, 2010. https://www.dissentmagazine.org/online_articles/will-the-real-chinese-internet-please-stand-up.

Miller, Christopher. "Ukraine's Top Intelligence Agency Deeply Infiltrated by Russian Spies." *Mashable*. Accessed June 2, 2020. https://mashable.com/2014/12/30/russian-vs-ukrainian-spies/.

Ministry of Communications and Information Technology of Iran. "مهندس جهانگرد در خبرداد: تبادل China-Iran ICT Cooperation2014," دیدار با مقام های 'شورای اطلاعات 'چین. https://www.ict.gov.ir/fa/news/10162/مهندس-جهانگرد-در-دیدار-با-مقام-های-شورای-اطلاعات-چین-خبرداد-تبادل-تجربیات-با-کشور-چین-در-حوزه-توسعه-ICT.

Ministry of Foreign Affairs of the Republic of Belarus. "Commonwealth of Independent States," 2019. http://mfa.gov.by/en/organizations/membership/list/c2bd4cebdf6bd9f9.html.

Ministry of Foreign Affairs, Republic of China. "Diplomatic Allies." *(Taiwan) 中華民國外交部 - 全球資訊網英文網*. Accessed March 13, 2020. https%3a%2f%2fwww.mofa.gov.tw%2fen%2fAlliesIndex.aspx%3fn%3dDF6F8F246049F8D6%26sms%3dA76B7230ADF29736.

Ministry of Interior of the Kyrgyz Republic. "Safe City." Accessed May 18, 2020. http://www.guobdd.kg/safecity.

Ministry of Justice of the Republic of Kazakhstan. "Law on Communications," July 5, 2004. http://adilet.zan.kz/eng/docs/Z040000567_.

Moldabekov, Daniyar. "Евразийский Киберсоюз - Аналитический Интернет-Журнал Vласть." *VLAST*, December 19, 2019. https://vlast.kz/obsshestvo/31791-evrazijskij-kibersouz.html.

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

Moyer, Jonathan D., Tim Sweijs, Mathew J. Burrows, and Hugo Van Manen. "Power and Influence in a Globalized World." Atlantic Council, University of Denver, The Hague Centre for Strategic Studies, January 2018. https://www.atlanticcouncil.org/in-depth-research-reports/report/power-and-influence-in-a-globalized-world/.

Mozur, Paul, 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.

Mueller, John. "The Impact of Ideas on Grand Strategy." In *Domestic Bases of Grand Strategy*, edited by Richard Rosecrance and Arthur A. Stein. Ithaca: Cornell University Press, 1993.

Mueller, Milton L. “Against Sovereignty in Cyberspace.” *International Studies Review* 22, no. 4 (November 26, 2020): 779–801.
Mueller, Milton, John Mathiason, and Hans Klein. “The Internet and Global Governance: Principles and Norms for a New Regime.” *Global Governance: A Review of Multilateralism and International Organizations* 13, no. 2 (2007): 237–54.
Mugerwa, Yasiin. “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.
Murgia, Madhumita, and Anna Gross. “Inside China’s Controversial Mission to Reinvent the Internet,” March 27, 2020. https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f.
Nakato, Sachio. “North Korea’s Second Nuclear Test: Neoclassical Realism Perspectives: North Korea’s Second Nuclear Test.” *Pacific Focus* 27, no. 1 (2012): 10–35. doi:10.1111/j.1976-5118.2012.01074.x.
NASA. “Earthrise,” February 23, 2015. http://www.nasa.gov/multimedia/imagegallery/image_feature_1249.html.
National Security Agency. “Project Bullrun,” 2010. https://search.proquest.com/docview/1679098764/abstract/7B14BB5285C84FFBPQ/1.
Nations, United. “Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression (Articles 39-51).” *United Nations*. United Nations. Accessed April 5, 2021. https://www.un.org/en/about-us/un-charter/chapter-7.
NATO StratCom Centre of Excellence. “Analysis of Russia’s Information Campaign Against Ukraine.” Riga, 2015.
Naughton, John. “The Evolution of the Internet: From Military Experiment to General Purpose Technology.” *Journal of Cyber Policy* 1, no. 1 (2016): 5–28.
Negroponte, Diana Villiers. “Would the Soviet Union Have Collapsed Without Mikhail Gorbachev?” *Brookings Institution*, October 17, 2019. https://www.brookings.edu/blog/order-from-chaos/2019/10/17/would-the-soviet-union-have-collapsed-without-mikhail-gorbachev/.
New America. “Open Technology Institute,” 2020. https://www.newamerica.org/oti/.
Nguyen, Mai. “Exclusive: Vietnam Cyber Law Set for Tough Enforcement Despite Google, Facebook Pleas.” *Reuters*, October 10, 2018. https://www.reuters.com/article/us-vietnam-socialmedia-exclusive/exclusive-vietnam-cyber-law-set-for-tough-enforcement-despite-google-facebook-pleas-idUSKCN1MK1HL.
Ng’wanakilala, Fumbuka. “Zanzibar Islamists Burn Churches, Riot - Police.” *Reuters*, May 27, 2012. https://www.reuters.com/article/zanzibar-protest-idUSL5E8GR1HB20120527.
Nisbet, Erik C., 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.
Obama, Barack. “International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World,” 2011. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

OECD. “Bridging the Digital Divide,” n.d. https://www.oecd.org/site/schoolingfortomorrowknowledgebase/themes/ict/bridgingthedigitaldivide.htm.
OONI. “OONI - Open Observatory of Network Interference,” n.d. https://ooni.torproject.org/.
Open Technology Fund. “A New, Independent OTF.” *Open Technology Fund*, November 25, 2019. https://www.opentech.fund/news/new-independent-otf/.
———. “Projects We Support.” *Open Technology Fund*, 2020. https://www.opentech.fund/results/supported-projects/.
Ordónez, Sandra, and Dan McDevitt. “Open Technology Fund Summit 2017: Community Snapshot.” *Open Technology Fund*, August 31, 2018. https://www.opentech.fund/news/open-technology-fund-summit-2017-community-snapshot/.
Orphanides, K. G. “Why Everyone Should Be Using Signal Instead of WhatsApp.” *Wired UK*, April 16, 2020. https://www.wired.co.uk/article/signal-vs-whatsapp.
“Oxford English Dictionary.” In *OED Online*. Oxford University Press. Accessed March 11, 2021. https://www.oed.com/view/Entry/122086.
Oxford Internet Institute. “Mahsa Alimardani,” 2020. https://www.oii.ox.ac.uk/people/mahsa-alimadeni/.
———. “People - Joss Wright,” 2020. https://www.oii.ox.ac.uk/people/joss-wright/.
Oxford Reference. “Autocracy,” 2021. https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095435876.
Pannier, Bruce. “Russia’s Star On Rise Again In Kyrgyzstan.” *RadioFreeEurope/RadioLiberty*, April 8, 2011. https://www.rferl.org/a/kyrgyzstan_back_in_russian_embrace/3551508.html.
Park, Susan. “Norm Diffusion Within International Organizations: A Case Study of the World Bank.” *Journal of International Relations and Development Volume*, 2005, 111–41.
Parkinson, Joe, 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.
Patman, Robert G. “Reagan, Gorbachev and the Emergence of New Political Thinking.” *Review of International Studies* 25, no. 4 (1999): 577–601.
Pegg, David. “Bahraini Arab Spring Dissidents Sue UK Spyware Maker.” *The Guardian*, October 11, 2018, sec. World news. https://www.theguardian.com/world/2018/oct/11/bahraini-arab-spring-dissidents-sue-uk-spyware-maker.
Penney, Jonathon W. “Chilling Effects: Online Surveillance and Wikipedia Use.” *Berkeley Technology Law Journal* 31, no. 1 (2016): 118–82.
Perez, Sarah. “Facebook Blocked in Vietnam Over the Weekend Due to Citizen Protests.” *TechCrunch*, May 17, 2016. https://social.techcrunch.com/2016/05/17/facebook-blocked-in-vietnam-over-the-weekend-due-to-citizen-protests/.
Peterson, Dahlia. “Designing Alternatives to China’s Repressive Surveillance State.” Center for Security and Emerging Technologyy, October 2020. https://cset.georgetown.edu/publication/designing-alternatives-to-chinas-repressive-surveillance-state/.

———. “Foreign Technology and the Surveillance State.” In *China’s Quest for Foreign Technology: Beyond Espionage*, edited by William C. Hannas and Didi Kirsten Tatlow. London and New York: Routledge, 2021.
Petrova, Margarita H. “The End of the Cold War: A Battle or Bridging Ground Between Rationalist and Ideational Approaches in International Relations?” *European Journal of International Relations* 9, no. 1 (2003): 115–63.
Philpott, Daniel. “Sovereignty.” In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Summer 2016. Metaphysics Research Lab, Stanford University, 2016. https://plato.stanford.edu/archives/sum2016/entries/sovereignty/.
Pielemeier, Jason. “Reports of the Death of Internet Freedom Are Greatly Exaggerated.” *Council on Foreign Relations*, July 9, 2018. https://www.cfr.org/blog/reports-death-internet-freedom-are-greatly-exaggerated.
Polityuk, Pavel, and Finkle Jim. “Ukraine Says Communications Hit, MPs Phones Blocked.” *Reuters*, March 4, 2014. https://www.reuters.com/article/us-ukraine-crisis-cybersecurity-idUSBREA231R220140304.
Polyakova, Alina. “Russian Foreign Policy.” *Council on Foreign Relations*, April 13, 2017. https://www.cfr.org/event/russian-foreign-policy.
Polyakova, Alina, and Chris Meserole. “Exporting Digital Authoritarianism.” *Brookings Institution*, August 26, 2019. https://www.brookings.edu/research/exporting-digital-authoritarianism/.
Ponciano, Jonathan. “The Largest Technology Companies In 2019: Apple Reigns As Smartphones Slip And Cloud Services Thrive.” *Forbes*, May 15, 2019. https://www.forbes.com/sites/jonathanponciano/2019/05/15/worlds-largest-tech-companies-2019/.
Poroshenko, Petro. “Post on VKontakte.” *VKontakte*, May 16, 2017. https://vk.com/poroshenko.petro?w=wall-69234729_7815.
Porter, Jon. “Whatsapp Now Has 2 Billion Users.” *The Verge*, February 12, 2020. https://www.theverge.com/2020/2/12/21134652/whatsapp-2-billion-monthly-active-users-encryption-facebook.
Powers, Shawn M, and Michael Jablonski. *The Real Cyber War: The Political Economy of Internet Freedom*. Urbana, Chicago, and Springfield: University of Illinois Press, 2015.
Prasso, Sheridan. “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.
President of Russia. “Address by President of the Russian Federation.” *President of Russia*, March 18, 2014. http://en.kremlin.ru/events/president/news/20603.
———. “Заседание Совета Безопасности.” *Президент России*, July 22, 2014. http://kremlin.ru/events/president/news/46305.
President of the Republic of Belarus. “On Approval of the Regulation on the Procedure for the Interaction of Telecommunication Operators With Agencies Engaged in Operational-Search Activities,” March 3, 2010. https://web.archive.org/web/20190104143950/http://oac.gov.by:80/files/files/pravo/ukazi/Ukaz_129.htm.
President of Ukraine. “Про Доктрину інформаційної безпеки України.” *Законодавство України*, July 8, 2009. https://zakon.rada.gov.ua/go/514/2009.

———. “УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №126/2018.” *Офіційне інтернет-представництво Президента України*, 2018. https://www.president.gov.ua/documents/1262018-24150.
———. “УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №133/2017.” *Офіційне інтернет-представництво Президента України*, May 15, 2017. https://www.president.gov.ua/documents/1332017-21850.
Privacy International. “Bahraini Government, With Help From FinFisher, Tracks Activists Living In The United Kingdom.” Accessed December 15, 2020. http://privacyinternational.org/blog/1231/bahraini-government-help-finfisher-tracks-activists-living-united-kingdom.
———. “Lawful Interception: The Russian Approach,” March 4, 2013. https://privacyinternational.org/blog/1296/lawful-interception-russian-approach.
———. “Open Season: Building Syria’s Surveillance State,” December 12, 2016. http://privacyinternational.org/report/1016/open-season-building-syrias-surveillance-state.
———. “Private Interests: Monitoring Central Asia,” November 2014. https://privacyinternational.org/report/837/private-interests-monitoring-central-asia.
Proceedings on Privacy Enhancing Technologies Symposium. “PoPETs/PETS,” 2020. https://petsymposium.org/.
Psiphon. “Home,” 2020. https://psiphon.ca/.
Putin, Vladimir. “Russia and the Changing World.” *Moskovskie Novosti*, March 28, 2020. http://web.archive.org/web/20200328133258/https://www.mn.ru/politics/78738.
Qiu, Qing. “India’s Internet Shutdown Shows Normal Practice for Sovereign Countries,” December 17, 2019. http://en.people.cn/n3/2019/1217/c90000-9641267.html.
Radio Free Asia. “Vietnamese Authorities Crack Down on Rare Protests Targeting Xi Visit.” Accessed January 6, 2021. https://www.rfa.org/english/news/vietnam/protests-11052015153610.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.
———. “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.
Radio Free Europe/Radio Liberty. “Ukraine Arrests Ex-Chief of Counterintelligence,” November 10, 2014. https://www.rferl.org/a/treason-ukraine-bik-arrest-counterintelligence/26683395.html.
Rahimi, Babak. “Censorship and the Islamic Republic: Two Modes of Regulatory Measures for Media in Iran.” *The Middle East Journal* 69, no. 3 (2015): 358–78.
Ranking Digital Rights. “2019 Ranking Digital Rights Corporate Accountability Index.” *Ranking Digital Rights*, 2020. https://rankingdigitalrights.org/index2019/.
Recorded Future. “How North Korea Revolutionized the Internet as a Tool for Rogue Regimes,” February 10, 2020. https://www.recordedfuture.com/north-korea-internet-tool/.
———. “North Korea Is Not Crazy,” June 15, 2017. https://www.recordedfuture.com/north-korea-cyber-activity/.

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.
Republic of Uzbekistan. “Об Оперативно-Розыскной Деятельности,” December 2012. https://lex.uz/docs/2106527.
Reuters. “Thailand Scraps Unpopular Internet ‘Great Firewall’ Plan.” *Reuters*, October 15, 2015. https://www.reuters.com/article/us-thailand-internet-idUSKCN0S916I20151015.
Roberts, Margaret E. *Censored: Distraction and Diversion Inside China’s Great Firewall*. Princeton N.J.: Princeton University Press, 2018.
Rollet, Charles. “China Enforces Barriers Against Foreign AI and VSaaS Providers.” *IPVM*, 02:06 400AD. https://ipvm.com/reports/vats.
Rose, Gideon. “Neoclassical Realism and Theories of Foreign Policy.” *World Politics* 51, no. 1 (1998): 144–72.
Rosert, Elvira. “Norm Emergence as Agenda Diffusion: Failure and Success in the Regulation of Cluster Munitions.” *European Journal of International Relations* 25, no. 4 (2019): 1103–31. doi:10.1177/1354066119842644.
Roudik, Peter. “ECHR, Russian Federation: Breaches of Human Rights in Surveillance Legislation |.” *Global Legal Monitor*, March 2, 2016. //www.loc.gov/law/foreign-news/article/echr-russian-federation-breaches-of-human-rights-in-surveillance-legislation/.
Russian Federation. “Federal Law of July 28, 2012 N 139-ФЗ (as Amended on October 14, 2014),” 2012. http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=169766&fld=134&dst=1000000001,0&rnd=0.6093347731359393#07964751504707204.
———. Information Security Doctrine of the Russian Federation (2000). https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf.
———. “On Amendments to the Federal Law ‘on Communications’ and the Federal Law ‘on Information, Information Technologies and the Protection of Information,’” May 1, 2019. https://sozd.duma.gov.ru/bill/608767-7.
———. “The Law of the Russian Federation of 12.27.1991 N 2124-1 (as Amended on 01.03.2020) ‘On the Mass Media,’” March 1, 2020. https://www.consultant.ru/document/cons_doc_LAW_1511/285787630b41d4963964c4c89fada1196a65cf3e/.
———. “В Законодательство Внесены Изменения, Устанавливающие Ответственность За Размещение Информации в Интернете.” *Президент России*, May 5, 2014. http://kremlin.ru/acts/news/20929.
———. “Об Информации, Информационных Технологиях и о Защите Информации,” July 14, 2006. http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102108264.
———. “Федеральный закон о защите детей от пропаганды гомосексуализма.” *Российская газета*, June 29, 2013. https://rg.ru/2013/06/30/deti-site-dok.html.
———. “Федеральный Закон От 5 Мая 2014 г. N 97-ФЗ.” *Российская Газета*, 2014. https://rg.ru/2014/05/07/informtech-dok.html.
———. “Федеральный Закон От 05.05.2014 г. № 97-ФЗ,” August 1, 2014. http://kremlin.ru/acts/bank/38409.

Russian Ministry of Communications and Mass Media. “Alexey Volin: ‘Internet Security and Reliability Issues Are Now Key.’” *Министерство Цифрового Развития, Связи и Массовых Коммуникаций Российской Федерации*, April 7, 2014. https://digital.gov.ru/ru/events/30084/.

———. “Nikolai Nikiforov: ‘FOCL Through the Kerch Strait Will Cover the Current Needs of Crimea in Communication Services.’” *Министерство Цифрового Развития, Связи и Массовых Коммуникаций Российской Федерации*, April 25, 2014. /ru/events/30028/.

———. “The Ministry of Communications of Russia Has Created the Territorial Administration of Roskomnadzor in Crimea.” *Министерство Цифрового Развития, Связи и Массовых Коммуникаций Российской Федерации*, April 2, 2014. /ru/events/30092/.

———. “Обработка и хранение персональных данных в РФ. Изменения с 1 сентября 2015 года :” *Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации*, September 2015. https://digital.gov.ru/ru/personaldata/.

Rydzak, Jan. “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.

Sacks, Samm. “Beijing Wants to Rewrite the Rules of the Internet.” *The Atlantic*, June 18, 2018. https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/.

Safire, William. “ON LANGUAGE; The Near Abroad.” *The New York Times*, May 22, 1994. https://www.nytimes.com/1994/05/22/magazine/on-language-the-near-abroad.html.

Sandholtz, Wayne. “Dynamics of International Norm Change: Rules against Wartime Plunder.” *European Journal of International Relations* 14, no. 1 (2008): 101–31.

Sanger, David E. “North Korea’s Internet Use Surges, Thwarting Sanctions and Fueling Theft.” *The New York Times*, February 10, 2020, sec. U.S. https://www.nytimes.com/2020/02/09/us/politics/north-korea-internet-sanctions.html.

Satter, Raphael. “Exclusive-Suspected Chinese Hackers Stole Camera Footage From African Union - Memo.” *Reuters*, December 16, 2020. https://www.reuters.com/article/us-ethiopia-african-union-cyber-exclusiv-idUSKBN28Q1DB.

Save Internet Freedom. “All Signatories,” July 29, 2020. https://saveinternetfreedom.tech.

SBU. “СБУ Провела Обшуки в Офісах Дочірньої Структури Російської Компанії «Яндекс» (Оновлено Відео) :: Служба Безпеки України,” May 29, 2017. https://web.archive.org/web/20200608164106/https://ssu.gov.ua/ua/news/1/category/21/view/3431.

Schauer, Frederick. “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.

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

Schneier, Bruce. “Click Here to Kill Everyone,” 2017. https://nymag.com/intelligencer/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html.
———. “Every Part of the Supply Chain Can Be Attacked.” *The New York Times*, September 25, 2019, sec. Opinion. https://www.nytimes.com/2019/09/25/opinion/huawei-internet-security.html.
Schwartz, Christopher, and Rebekah Overdorf. “Disinformation from the Inside: Combining Machine Learning and Journalism to Investigate Sockpuppet Campaigns.” *Companion Proceedings of the Web Conference 2020*, Taipei, Taiwan. doi:https://doi.org/10.1145/3366424.3385777.
Schweller, Randall L. *Deadly Imbalances : Tripolarity and Hitler’s Strategy of World Conquest*. New York: Columbia University Press, 1998.
Schweller, Randall L, and William C Wohlforth. “Power Test: Evaluating Realism in Response to the End of the Cold War.” *Security Studies* 9, no. 3 (2000): 60–107.
Security Service of Ukraine. “SBU Presents Draft Version of New Law ‘on the Security Service of Ukraine’ to the President,” October 15, 2019. https://ssu.gov.ua/en/news/25/category/21/view/6613#.PdJ0jWrs.dpbs.
Seddon, Max. “MTS Sells Ukrainian Unit as It Focuses on Russia,” November 25, 2019. https://www.ft.com/content/4a5a21ee-0f9b-11ea-a7e6-62bf4f9e548a.
Seddon, Max, 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.
Sending, Ole Jacob. “Constitution, Choice and Change: Problems with the `Logic of Appropriateness’ and Its Use in Constructivist Theory.” *European Journal of International Relations* 8, no. 4 (2002): 443–70.
Shah, Saeed. “CIA Organised Fake Vaccination Drive to Get Osama Bin Laden’s Family DNA.” *The Guardian*, July 11, 2011, sec. World news. https://www.theguardian.com/world/2011/jul/11/cia-fake-vaccinations-osama-bin-ladens-dna.
———. “CIA’s Fake Vaccination Programme Criticised by Médecins Sans Frontières.” *The Guardian*, July 14, 2011, sec. Society. https://www.theguardian.com/world/2011/jul/14/cia-fake-vaccination-medecins-frontieres.
Shaw, Tony, and Denise Youngblood. “Cold War Sport, Film, and Propaganda: A Comparative Analysis of the Superpowers.” *Journal of Cold War Studies* 19, no. 1 (2017): 160–92.
Sheehan, Matt. “How Google Took on China—and Lost.” *MIT Technology Review*, December 19, 2018. https://www.technologyreview.com/2018/12/19/138307/how-google-took-on-china-and-lost/.
Signal Messenger. “Home.” *Signal Messenger*, 2020. https://signal.org/.
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.
Smith, Noah. “Google’s Prototype Chinese Search Engine Links Searches to Phone Numbers.” *The Guardian*, September 19, 2018, sec. Technology. https://www.theguardian.com/technology/2018/sep/18/google-china-dragonfly-search-engine.

Soldatov, Andrei, and Irina Borogan. “In Ex-Soviet States, Russian Spy Tech Still Watches You.” *WIRED*, December 21, 2012. https://www.wired.com/2012/12/russias-hand/.

Soldatov, Andreĭ, and Irina Borogan. *The Red Web: The Struggle between Russia’s Digital Dictators and the New Online Revolutionaries*. First. New York: PublicAffairs, 2015.

Solove, Daniel J. “A Taxonomy of Privacy.” *University of Pennsylvania Law Review* 154, no. 3 (January 1, 2006): 477.

Soshnikov, Andrei. “Inside a Pro-Russia Propaganda Machine in Ukraine.” *BBC News*, November 13, 2017, sec. BBC Trending. https://www.bbc.com/news/blogs-trending-41915295.

Sottek, T. C. “Everything You Need to Know About PRISM.” *The Verge*, July 17, 2013. https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet.

Sozialdemokratischen Partei Deutschlands (SPD), BÜNDNIS 90 / DIE GRÜNEN, and Freien Demokraten (FDP). “Koalitionsvertrag 2021 – 2025 Zwischen Der Sozialdemokratischen Partei Deutschlands (SPD), BÜNDNIS 90 / DIE GRÜNEN Und Den Freien Demokraten (FDP),” 2021.

Spykman, Nicholas John. *America’s Strategy in World Politics : The United States and the Balance of Power*. Hamden, Conn: Archon Books, 1970.

Staff, Reuters. “China Tells U.N. Rights Chief to Respect Its Sovereignty After Xinjiang Comments.” *Reuters*, September 11, 2018. https://in.reuters.com/article/un-rights-china-idINKCN1LR0KB.

———. “State Department OKs Nearly $6 Billion in Weapons Sales to Gulf Allies.” *Reuters*, May 3, 2019. https://www.reuters.com/article/us-usa-defense-arms-idUSKCN1S924P.

Statcounter. “Social Media Stats Russian Federation.” *StatCounter Global Stats*. Accessed April 30, 2019. http://gs.statcounter.com/social-media-stats/all/russian-federation.

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.

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.

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

Stecklow, Steve, 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.

Stein, Janice Gross. “Political Learning by Doing: Gorbachev as Uncommitted Thinker and Motivated Learner.” *Int Org* 48, no. 2 (1994): 155–83.

Stewart, Patrick M., and Ashley Feng. “Belt and Router: China Aims for Tighter Internet Controls with Digital Silk Road.” *Net Politics - Council on Foreign Relations*, July 2, 2018. https://www.cfr.org/blog/belt-and-router-china-aims-tighter-internet-controls-digital-silk-road.

Stone, Biz. “The Tweets Must Flow,” January 28, 2011. https://blog.twitter.com/official/en_us/a/2011/the-tweets-must-flow.html.

Strange, Susan. “Cave! Hic Dragones : A Critique of Regime Analysis.” *Int Org* 36, no. 2 (1982): 479–96.
Stubbs, Jack. “Uzbek Spies Attacked Dissidents With Off-The-Shelf Hacking Tools.” *Reuters*, October 3, 2019. https://www.reuters.com/article/us-uzbekistan-cyber-idUSKBN1WI0YL.
Suhauna, Hussain. “‘Please Disregard, Vote for Bernie’: Inside Bloomberg’s Paid Social Media Army.” *Los Angeles Times*, February 23, 2020. https://www.latimes.com/business/technology/story/2020-02-23/mike-bloomberg-paid-twitter-social-media.
Sunstein, Cass. “Social Norms and Social Roles.” *Columbia Law Rev.* 96, no. 4 (1996): 903–68.
Surkov, Vladislav. “Nationalization of the Future.” *Expert Online 2.0*, November 20, 2006. https://web.archive.org/web/20101110050502/http://expert.ru:80/printissues/expert/2006/43/nacionalizaciya_buduschego/.
Tahir, Muhammad. “Governments Move To Thwart ‘Arab Spring’ In Central Asia.” *Radio Free Europe / Radio Liberty*, April 28, 2011. https://www.rferl.org/a/governments_move_to_thwart_arab_spring_in_central_asia/16796618.html.
Taiwan Association for Human Rights. “Home.” *台灣人權促進會 | Taiwan Association for Human Rights Since Dec.10 1984*, 2020. https://www.tahr.org.tw/.
Tao, Li. “Japan Latest Country to Exclude Huawei, Zte From 5G Roll-Out.” *South China Morning Post*, December 10, 2018. https://www.scmp.com/tech/tech-leaders-and-founders/article/2177194/japan-decides-exclude-huawei-zte-government.
Telecommunications Industry Dialogue. “Provision of Real-Time Lawful Interception Assistance,” June 2015. https://www.telecomindustrydialogue.org/resources/kazakhstan/.
telecompaper. “Rostelecom Launches Fibre Link to Crimea,” April 25, 2014. https://www.telecompaper.com/news/rostelecom-launches-fibre-link-to-crimea--1010208.
Telia. “Respecting Freedom of Expression - Telia Company’s View on New Surveillance Regulation (‘Direct Access’) in Kazakhstan,” May 10, 2017. https://www.teliacompany.com/en/news/news-articles/2017/freedom-of-expression-kazakhstan/.
Thai Government Public Relations Department. “Prime Minister’s Orders,” September 4, 2015. https://pr.prd.go.th/chaiyaphum/ewt_news.php?nid=9060.
Thai Ministry of Digital Economy and Society. “Cybersecurity Act,” 2019. https://www.mdes.go.th/law/detail/1904-Cybersecurity-Act--B-E--2562--2019-.
The Boston Consulting Group. “The Internet Economy in the G-20,” March 2012. https://image-src.bcg.com/Images/The_Internet_Economy_G-20_tcm9-106842.pdf.
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?from=mdr.
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.

The General Prosecutor's Office of the Republic of Kazakhstan. "The Strategy «Kazakhstan 2030»," April 9, 2012. http://prokuror.gov.kz/eng/state/acts-president/strategy-kazakhstan-2030.
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.
The ISC Project. "Home," 2020. https://www.iscproject.org.
The New York Times. "Yahoo Chief Apologizes to Chinese Dissidents' Relatives," November 7, 2007, sec. Business. https://www.nytimes.com/2007/11/07/business/worldbusiness/07iht-yahoo.1.8226586.html.
The President of Russia. "Телефонный Разговор с Президентом США Бараком Обамой," March 2, 2014. http://kremlin.ru/events/president/news/20355.
The Russian Federation (State Duma). "Федеральный Закон 'Об Оперативно-Розыскной Деятельности' От 12.08.1995 N 144-ФЗ (Последняя Редакция)," August 12, 1995. https://www.consultant.ru/document/cons_doc_LAW_7519/.
The White House. "Monaco Letter on Vaccine Workers," May 16, 2014. https://www.documentcloud.org/documents/1164764-monaco-letter-on-vaccine-workers.html.
The World Bank. "Population, Total," 2019. https://data.worldbank.org/indicator/SP.POP.TOTL?locations=AG.
Thornberry, Mac. "Text - H.R.2810 - 115th Congress (2017-2018): National Defense Authorization Act for Fiscal Year 2018." Webpage, December 12, 2017. doi:/bill/115th-congress/house-bill/2810/text.
Tilouine, Joan, 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.
Toor, Amar. "Cutting the Cord: Brazil's Bold Plan to Combat the NSA." *The Verge*, September 25, 2013. https://www.theverge.com/2013/9/25/4769534/brazil-to-build-internet-cable-to-avoid-us-nsa-spying.
Towindo, Lincoln. "Government to Regulate Social Media," April 10, 2016. http://www.sundaymail.co.zw/social-media-regulation-is-nigh/.
Tracy, Brian. *Business Strategy*. Brian Tracy Success Library. New York, New York: American Management Association, 2015.
Turkson, Nshira. "A Social-Media Shutdown in Uganda's Presidential Election." *The Atlantic*, February 18, 2016. https://www.theatlantic.com/international/archive/2016/02/uganda-election-social-media-shutdown/463407/.
Twitter. "Greg Walton (@meta_lab) / Twitter." *Twitter*, 2020. https://twitter.com/meta_lab.
UK Parliament. "Suppliers, Network Operators and Academics Questioned on UK Telecommunications Infrastructure - News from Parliament." *UK Parliament*. Accessed October 8, 2019. https://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/news-parliament-2017/uk-telecommunications-infrastructure-evidence-17-19/.
Ukraine, Digital Security Lab. "Crimea Has a Website Ban List Additional to Russia-Wide List, a Research Proves." *Medium*, September 20, 2018.

https://medium.com/@cyberlabukraine/crimea-has-a-website-ban-list-additional-to-russia-wide-list-a-research-proves-4f20fa6fc762.
Ungerleider, Neal. “Iran Cracking Down Online With ‘Halal Internet.’” *Fast Company*, April 18, 2011. https://www.fastcompany.com/1748123/iran-cracking-down-online-halal-internet.
United Nations Economic Commission for Africa. “CoM2019 Ends With African Governments Being Urged to Embrace Digital Transformation,” March 26, 2019. https://www.uneca.org/stories/com2019-ends-african-governments-being-urged-embrace-digital-transformation.
United Nations General Assembly. “Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General.” New York, January 13, 2015. https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.
United States Air Force. “Three Levels of War.” *Air and Space Power Mentoring Guide* 1 (1997).
University of Hong Kong. “WeChatSCOPE | an Insight to Censorship in China,” 2020. https://wechatscope.jmsc.hku.hk/.
University of Maryland. “Geneva: Evolving Censorship Evasion.” *Censorship.Ai*, 2020. https://geneva.cs.umd.edu/.
University of Michigan. “Censored Planet.” *Censored Planet*, 2020. https://censoredplanet.org/.
US Agency for Global Media. “BBG Provides Bird Flu Reporting Workshops,” April 9, 2013. https://www.usagm.gov/2013/04/09/bbg-provides-bird-flu-reporting-workshops/.
———. “News Coverage: Delivering News to Television,” August 16, 2019. https://www.usagm.gov/2019/08/16/news-coverage-delivering-news-to-television/.
U.S. Congress. “17 U.S. Code § 107 - Limitations on Exclusive Rights: Fair Use.” *LII / Legal Information Institute*. Accessed July 7, 2020. https://www.law.cornell.edu/uscode/text/17/107.
———. “International Broadcasting Act.” *USAGM*, 1994. https://www.usagm.gov/who-we-are/oversight/legislation/international-broadcasting-act/.
———. “Text - H.R.2048 - 114th Congress (2015-2016): USA FREEDOM Act of 2015.” Legislation, February 6, 2015. 2015/2016. https://www.congress.gov/bill/114th-congress/house-bill/2048/text.
———. “Text - S.2943 - 114th Congress (2015-2016): National Defense Authorization Act for Fiscal Year 2017,” May 18, 2016. https://www.congress.gov/bill/114th-congress/senate-bill/2943/text.
U.S. Customs and Border Protection. “CBP Response to DHS Coalition Letter,” November 11, 2019. https://web.archive.org/web/20191111201841/https://www.documentcloud.org/documents/6009352-CBP-Response-to-DHS-Coalition-Letter.html.
U.S. Deparment of State. “Internet Freedom.” Accessed November 2, 2018. https://www.state.gov/j/drl/internetfreedom/.
US Department of Defense. “Summary - Department of Defense Cyber Strategy,” 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

US Department of State. “Department of State International Cyberspace Policy Strategy.” Department of State, March 2016. https://www.state.gov/documents/organization/255732.pdf.
U.S. Geological Survey. “U.S. Geological Survey, Mineral Commodity Summaries - Rare Earths,” February 2019. https://prd-wret.s3-us-west-2.amazonaws.com/assets/palladium/production/atoms/files/mcs-2019-raree.pdf.
USAID. “Greater Internet Freedom,” 2020. https://www.grants.gov/web/grants/view-opportunity.html?oppId=323976.
USENIX. “FOCI ’20,” December 17, 2019. https://www.usenix.org/conference/foci20.
VAS Experts. “About Us.” *VAS Experts*, 2019. https://vasexpertsdpi.com/about-us/.
Vega. “The System of Photo-Video Recording of Traffic Violations ‘Prism.’” Accessed May 18, 2020. http://vega.su/production/detail.php?ID=2301.
Verkhovna Rada of Ukraine. “Draft Law on Amendments to the Law of Ukraine ‘on Information’ (Concerning the Dissemination of Mass Information on the Internet),” February 12, 2015. http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=54006.
———. “Про Рішення Ради Національної Безпеки і Оборони України Від 2 Травня 2018 Року ‘Про Застосування Та Скасування Персональних Спеціальних Економічних Та Інших Обмежувальних Заходів (Санкцій).’” *Офіційний Вебпортал Парламенту України*, May 14, 2018. https://zakon.rada.gov.ua/go/126/2018.
Vernon, Raymond. “Sovereignty at Bay Ten Years After.” *International Organization* 35, no. 3 (1981): 517–29.
———. *Sovereignty at Bay: The Multinational Spread Of U.S. Enterprises*. London: Longman, 1971.
Ververis, Vasilis, Marios Isaakidis, Valentin Weber, and Benjamin Fabian. “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.
Volz, Dustin. “NSA Improperly Collected U.S. Phone Records a Second Time.” *Wall Street Journal*, June 26, 2019. https://www.wsj.com/articles/nsa-improperly-collected-u-s-phone-records-a-second-time-11561541520.
Wajid Khan, Abdul. “Anti-CPEC Propaganda and Reality.” *China Daily*, October 30, 2018. http://www.chinadaily.com.cn/a/201810/30/WS5bd7fda5a310eff3032857a2.html.
Walker, Shaun. “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.
Walt, Stephen M. *Revolution and War*. Ithaca and London: Cornell University Press, 1997.
Waltz, Kenneth, N. *Theory of International Politics*. Reading, MA: Addison-Wesley, 1979.
“Wayback Machine.” Accessed April 15, 2021. https://web.archive.org/.
Weber, Valentin. “How China’s Control of Information Is a Cyber Weakness.” *The Lawfare Institute*, November 12, 2020. https://www.lawfareblog.com/how-chinas-control-information-cyber-weakness.

———. “Linking Cyber Strategy with Grand Strategy: The Case of the United States.” *Journal of Cyber Policy*, August 17, 2018.
———. “Making Sense of Technological Spheres of Influence.” Strategic Update. LSE IDEAS, April 2020. http://www.lse.ac.uk/ideas/publications/updates/technological-spheres-of-influence.
———. “States and Their Proxies in Cyber Operations.” *Lawfare*, May 15, 2018. https://www.lawfareblog.com/states-proxies-cyber-operations.
———. “The Worldwide Web of Chinese and Russian Information Controls.” *Centre for Technology and Global Affairs, University of Oxford*, September 2019. https://ctga.web.ox.ac.uk/files/theworldwidewebofchineseandrussianinformationcontrolspdf.
———. “Why China’s Internet Censorship Model Will Prevail over Russia’s,” December 12, 2017. https://www.cfr.org/blog/why-chinas-internet-censorship-model-will-prevail-over-russias.
Weber, Valentin, and Vasilis Ververis. “Measuring Censorship on Mobile App Stores.” *OxPol*, May 3, 2019. https://blog.politics.ox.ac.uk/measuring-censorship-on-mobile-app-stores/.
Wei, Lu, ContributorDirector, State Internet Information Office; Cyberspace Administration of China, and Beijing. “Cyber Sovereignty Must Rule Global Internet.” *HuffPost*, December 15, 2014. https://www.huffpost.com/entry/china-cyber-sovereignty_b_6324060.
Wendt, Alexander. “Anarchy Is What States Make of It: The Social Construction of Power Politics.” *International Organization* 46, no. 2 (1992): 391–425.
———. *Social Theory of International Politics*. Cambridge Studies in International Relations. Cambridge, U.K.: Cambridge University Press, 1999.
Wendt, Alexander, and Daniel Friedheim. “Hierarchy Under Anarchy: Informal Empire and the East German State.” *International Organization* 49, no. 4 (1995): 689–721.
West, Darrell M. “Internet Shutdowns Cost Countries $2.4 Billion Last Year.” Brookings Institution, October 6, 2016. https://www.brookings.edu/research/internet-shutdowns-cost-countries-2-4-billion-last-year/.
———. “Internet Shutdowns Cost Countries $2.4 Billion Last Year.” *Brookings Institution*, October 6, 2016. https://www.brookings.edu/research/internet-shutdowns-cost-countries-2-4-billion-last-year/.
Weyland, Kurt. “Crafting Counterrevolution: How Reactionaries Learned to Combat Change in 1848” 110, no. 2 (2016): 215–31.
Whittaker, Zack. “Documents Reveal How Russia Taps Phone Companies for Surveillance.” *TechCrunch*. Accessed July 31, 2020. https://social.techcrunch.com/2019/09/18/russia-sorm-nokia-surveillance/.
Wiener, Antje. *The Invisible Constitution of Politics: Contested Norms and International Encounters*. Cambridge: Cambridge University Press, 2008.
Williams, Martyn. “How the Internet Works (‘Works’) in North Korea.” *Slate Magazine*, November 28, 2016. https://slate.com/technology/2016/11/how-the-internet-works-in-north-korea.html.
Wilson, Tom, and Madhumita Murgia. “Uganda Confirms Use of Huawei Facial Recognition Cameras,” August 20, 2019. https://www.ft.com/content/e20580de-c35f-11e9-a8e9-296ca66511c9.

Wines, Michael. “As Inflation Soars, Zimbabwe Economy Plunges.” *The New York Times*, February 7, 2007. https://www.nytimes.com/2007/02/07/world/africa/07zimbabwe.html.
Winston, Carla. “Norm Structure, Diffusion, and Evolution: A Conceptual Approach.” *European Journal of International Relations* 24, no. 3 (2018): 638–61.
Wittmeyer, Alicia P. Q. “Why Is Google’s Eric Schmidt Heading to North Korea?,” January 2, 2013. https://foreignpolicy.com/2013/01/02/why-is-googles-eric-schmidt-heading-to-north-korea/.
Wohlforth, William. “Realism and the End of the Cold War.” *International Security* 19, no. 3 (1994): 91–129.
World Bank. “African Leaders Committed to Building a Digital Economy,” May 30, 2018. https://blogs.worldbank.org/voices/african-leaders-committed-to-building-digital-economy.
———. “Individuals Using the Internet (% of Population) | Data,” 2020. https://data.worldbank.org/indicator/IT.NET.USER.ZS.
Wrong, Dennis H. *Power: Its Forms, Bases, and Uses*. Key Concepts in the Social Sciences. Oxford: Blackwell, 1979.
Wu, Ben Blanchard, J. R. “With Gambia Move, China Ends Diplomatic Truce With Taiwan.” *Reuters*, March 17, 2016. https://www.reuters.com/article/us-china-gambia-idUSKCN0WJ1DT.
Wu, Tim. “Is the First Amendment Obsolete?” Knight First Amendment Institute at Columbia University, September 1, 2017. https://knightcolumbia.org/content/tim-wu-first-amendment-obsolete.
Wu, Timothy S. “Cyberspace Sovereignty? The Internet and the International System.” *Harvard Journal of Law & Technology* 10, no. 3 (1997): 647–66.
Xue, Yujie. “Camera Above the Classroom.” *Sixth Tone*, March 26, 2019. https://www.sixthtone.com/news/1003759/camera-above-the-classroom.
Xynou 2020-07-22, Maria. “Support the OTF: Support a Free and Open Internet,” July 22, 2020. https://ooni.org/post/2020-support-otf/.
Yacoubian, Mona. “Syria Timeline: Since the Uprising Against Assad.” United States Institute of Peace. Accessed December 14, 2020. https://www.usip.org/syria-timeline-uprising-against-assad.
Yeo, Sophie. “How the Largest Environmental Movement in History Was Born,” April 22, 2020. https://www.bbc.com/future/article/20200420-earth-day-2020-how-an-environmental-movement-was-born.
Yin, Robert K. *Case Study Research: Design and Methods*. Sage Publications, 1984.
York, Jillian C. “Internet Freedom Initiative Mere Lip Service?,” November 3, 2011. https://www.aljazeera.com/indepth/opinion/2011/10/201110301020514111 30.html.
———. “The Trump Administration Is Attacking Critical Internet Privacy Tools,” July 10, 2020. https://www.vice.com/en_us/article/v7gz4d/the-trump-administration-is-attacking-critical-internet-privacy-tools.
Yuan, Zhou, 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.
Zakaria, Fareed. *From Wealth to Power : The Unusual Origins of America’s World Role*. Princeton Studies in International History and Politics. Princeton, N.J.: Princeton University Press, 1998.
Zhang, Hongpei. “Chinese Facial ID Tech to Land in Africa.” *Global Times*, May 17, 2018. http://www.globaltimes.cn/content/1102797.shtml.

Zhang, Lei. “Invisible Footprints of Online Commentators.” *Global Times*, February 5, 2010. http://www.globaltimes.cn/special/2010-02/503820.html.

Zhang, Xiaoling, 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.

Zhu, Tao, David Phipps, Adam Pridgen, Jedidah R. Crandall, and Dan S. Wallach. “The Velocity of Censorship: High-Fidelity Detection of Microblog Post Deletions.” Washington, D.C., 2013. https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/zhu.

ZN.ua. “В Донбассе Заблокированы Сайты Ряда Проукраинских СМИ.” *ZN.Ua*, September 30, 2014. https://zn.ua/TECHNOLOGIES/v-donbasse-zablokirovany-sayty-ryada-proukrainskih-smi-154664_.html.

КОСТЕНКО, Юлия. “«Безопасный Город». Где Установлены Видеокамеры Для Фиксации Нарушений.” *24.Kg*, May 14, 2019. https://24.kg/obschestvo/114794_bezopasnyiy_gorod_gde_ustanovlenyi_videokameryi_dlya_fiksatsii_narusheniy/.

Муканов, Бауржан. “Центр Мониторинга и Реагирования На Кибератаки Создадут Казахстан и Россия,” April 27, 2017. https://informburo.kz/novosti/centr-monitoringa-i-reagirovaniya-na-kiberataki-sozdadut-kazahstan-i-rossiya.html.

Навальный, Алексей. “Алексей Навальный.” *YouTube*. Accessed March 19, 2019. https://www.youtube.com/channel/UCsAw3WynQJMm7tMy093y37A.

Однако. “Лавров, Шойгу и Генштаб: О «цветных Революциях», Украине, Сирии и Роли России,” May 23, 2014. http://www.odnako.org/blogs/konferenciya-po-mezhdunarodnoy-bezopasnosti-o-cvetnih-revolyuciyah-ukraine-sirii-i-roli-rossii/.

РИА Новости. “В Кремле Заявили, Что Национализацию Заводов в ДНР и ЛНР Можно Понять,” March 3, 2017. https://ria.ru/20170301/1489002715.html.

СКМ. “ПАТ «Укртелеком» Повідомляє Про Неможливість Надання Абонентам Послуг Зв’язку На Непідконтрольній Частині Донецької Області Через Протиправні Дії Щодо Його Об’єктів На Цій Території,” March 1, 2017. https://web.archive.org/web/20170309052617/https://www.scm.com.ua/uk/media-centre/news/view/2589/.

Сошников, Андрей, and Андрей Захаров. “‘Стоп-слово’ - Навальный. Хакеры разоблачили ‘проект ФСБ’ в соцсетях.” *BBC News Русская служба*, December 20, 2018, sec. Подробности. https://www.bbc.com/russian/features-46621322.