Human Rights in the Age of Surveillance:

China's Expansion of Technological and Normative Power

By

Huimin Li

A thesis submitted in partial fulfillment

Of the requirements for the degree of

Master of Arts

Program in International Relations

New York University

May 2020

_____

Professor Anna Di Lellio

_____

Professor John Fousek

DEDICATION

I dedicate this thesis to my parents: for their unconditional love and support, and for giving me freedom to become the best version of myself.

ACKNOWLEDGEMENT

This thesis would not have been completed without help from my advisors Prof. Di Lellio and Prof. Fousek. They have provided invaluable guidance and feedbacks throughout the drafting process. I am also grateful to Prof. Helman: those informed and thoughtful conversations about national security and PhD programs changed my life.

Chenwei Xu is the best roommate I could ever ask for in times of pandemic. To all the food, tears, and laughters we shared, and many more to come. Janine Eduljee and Emma Nash, my best friends, thanks for always standing by my side.

A special thank you note to New York City, for its rainy days and sunshine; for everyday clap at 7pm; for all the medical and essential workers, especially their resilience and compassion; for all the restaurants, coffee shops, record store, theaters, and strangers walking on the street; for my neighbor's cats and those precious eye contacts we made while looking out the window.

ABSTRACT

In an interdependent world, it is crucial to analyze the diffusion of norms, the interactions among states and non-state actors, and the implications of state behaviors and narratives. By analyzing the mechanism and consequences of surveillance, this thesis sheds lights on the changing dynamics of state-citizen relations and the intricate balance between security and liberty. The interdisciplinary approach covers scholarship from both international relations and international law.

This thesis examines the role of China in shaping normative standards in surveillance and human rights protections. Its rising economic and military power enables China to develop a sophisticated surveillance system, exploit the security narrative, and reinterpret human rights norms. Two case studies look into the expansion of surveillance systems and state power, and how public security is achieved at the expense of individual rights. The COVID-19 outbreak analyzes China's domestic use of surveillance and justifications, as well as the unprecedented level of public-private collaboration. The Huawei "Safe City" project highlights China's global ambition in exporting surveillance technology and the security norms it represents. The unrestrained expansion of state power will likely lead to shrinking space for human rights in China, and possibly around the world.

TABLE OF CONTENT

Introduction

This thesis is concerned with the problem of state-citizen relations and the problem of norms. The augmentation of state capacity often affects the scope and conditions of human rights norms, while norms in turn provide justification for state's behaviors. As the state strives to expand its power, the legitimacy of its governance is contested in a variety of ways. In what circumstances may the public good outweigh personal interests? Where are the limits of state power, and how to assess intrusive intervention?

Realist theory emphasizes the central role of states. The anarchic nature of the international system determines that states seek power to project influence. Constructivist scholars complement the realist perspective by examining the relationship between norms and change. A contested and dynamic process, norm construction is shaped by the interactions among the states, yet also affects the patterns of behaviors in the international system.

From the Enlightenment discourse to the Universal Declaration of Human Rights, the essence of humanity calls for a liberal and equal world where individual rights are respected and fulfilled by states. The international human rights regime has provided an effective framework to balance between security and liberty and protect citizens from the excess of state power. Since World War II, human rights norms have reinvented and diffused through treaties, agreements, international bodies, regional courts, and governmental organizations. International law acknowledges the significance of sovereignty and community, as well as the fundamental freedoms of individuals. When a state of emergency is declared, legitimate restrictions of certain human rights are necessary for the sake of public goods.

The change of state-citizen relations and human rights norms are subjected to a range of factors, such as economic growth, political stability, and legal reforms. This research will analyze surveillance as a variable, especially how digital technology shapes power dynamics domestically and internationally. My main research questions are: Does China have intentions and capabilities to construct a new global norm of security through surveillance that might shape the scope and conditions of human rights norms? How can the international human rights framework respond to this emerging threat?

Surveillance studies analyze the social impacts of surveillance systems. Michel Foucault examined the mechanism of panopticon, arguing that the invisibility of surveillance systems has the power to correct and punish people's behaviors. Therefore, as a type of security apparatus, surveillance technology can significantly empower the state and discipline its citizens. Without judicial constraints and independent oversight, the abusive use of surveillance has chilling effects on privacy and freedoms.

While surveillance is not a modern phenomenon, the rise of electronic surveillance technology greatly increased its capacity. For decades, governments have used wiretapping and other message interception techniques for intelligence gathering and national security. Facial recognition, artificial intelligence, and cloud computing allow the actors to conduct mass surveillance by tracking, monitoring, and processing the details of people's private lives. Tech companies and their new forms of profit model also gradually changed the relations between capitalism and privacy. They also collaborate with public sectors to provide technical expertise. As the industry is mostly self-regulated, surveillance technology is likely to be abused by powerful actors without adequate oversight and human rights safeguard.

In countries like China, where public and private sectors maintain a close tie, they pose a different kind of challenge. Its distinct political and economic system determines a high level of cooperation and information sharing between political institutions and tech companies. Labelled as “Skynet,” the Chinese government utilizes CCTV cameras and facial recognition for law enforcement and security purposes. Based on the surveillance capitalism model, Chinese companies collect enormous data about people’s online activities, as to predict and shape consumer behaviors. The European Union has passed certain regulations to constrain the overpowering tech companies, as they appear intrusive to the right of privacy and freedom of expression. However, such limits of corporate power are unlikely in China. The government’s surveillance system for the purpose of public security, and the corporate’s surveillance system for the purpose of profits, are heading towards a unified, comprehensive surveillance system. The social credit system is likely to achieve an unprecedented surveillance system and cover every aspect of a citizen's private life. Yet, how the system monitors, classifies and disciplines the population as a whole is immensely ambiguous.

The trajectory of Chinese surveillance reflects the expansion of state power. Two major surveillance systems include Skynet, a police system based on video surveillance and big data analytics, and social credit system, a unified system aiming to incorporate both public and private databases. The Chinese government justifies the use of surveillance by emphasizing the significance of public security and collective interests. As the state’s security apparatus becomes increasingly sophisticated and professional, it is essential to assess its trade-offs of stability and security.

By addressing the dark side of surveillance, and its implications for human rights norms, this essay aims to shed light on an intangible form of control. I will first present a theoretical

framework for analyzing the role of states, the dynamics process of norms construction, the mechanism and social impact of surveillance, and the nuances of international human rights regime. Then I will provide relevant context to understand the trend and concerns of the global surveillance industry. This section also illustrates China's technological capabilities, regulatory environment, surveillance systems and ideology to analyze the factors that permit the proliferation of surveillance.

The first case study analyzes the unfolding COVID-19 outbreaks. In times of public health crisis, states are authorized with emergency powers to prioritize collective interests and impose restrictions on certain human rights, such as the right to privacy. The common public health strategies, such as contact tracing, quarantine and isolation require the use of surveillance techniques, which may interfere with the right to privacy and fundamental freedoms. This chapter examines the challenges of balancing human rights during the pandemic and compares surveillance and preventive measures in several countries. By evaluating China's emergency response, this thesis discusses the narratives of Chinese government, and how these justifications may influence the emergence of new norms.

I argue that the COVID-19 outbreak accelerates the transition from Skynet to the Social Credit system, as it provides an overarching justification for conducting surveillance at scale. The health code, for instance, provides a pretext to speed up the integration of public and private surveillance systems. The information collected for mitigating pandemic is likely to be used for other purposes. Some of China's public health strategies have challenged human rights norms during state of emergency, in particular the principle of proportionality. Consequently, the vaguely defined notion of security and collective interests may create a permissive environment for arbitrary surveillance and human rights abuses.

In addition to the domestic expansion of surveillance, China also contributes to the global proliferation of surveillance technology. The second case study, Huawei "Safe City," looks into how the goals of Chinese tech companies fit into the broader geopolitical interests of the Chinese government. From the will and capabilities of Huawei to China's Belt and Road Initiative, this chapter analyzes the role of tech companies, China's global ambition, and human rights implications in the international system. I argue that China seeks political alliances through the export of surveillance technology and becomes the norm entrepreneur of security narratives. The lack of international regulations and oversight on surveillance export can have far-reaching consequences. By reinforcing a security norm, China contributes to the growing fragmentation of cyberspace and increases the difficulty to reach any effective consensus on surveillance regulations.

In summary, surveillance technology has empowered China's security apparatus. As China expands the reach of surveillance, it also strives to find legitimacy for its intrusive governance model. As a result, the alternative security narrative becomes an effective tool to justify the use of surveillance systems and may exacerbate human rights violations. The blurred boundary between public and private spheres is likely to shape human rights norms, and potentially across the globe.

Regarding the scope limitation, this thesis mainly focuses on surveillance for security purposes, especially law enforcement and emergency response. Surveillance systems for espionage and foreign intelligence will be excluded in the analysis. The model of surveillance capitalism is briefly introduced as contextual background or examining the mechanism of surveillance system. However, this thesis will not dig into the relationship between commercial surveillance and human rights violations. The role of private companies is discussed in the

context of public-private collaboration, or in the case of surveillance export, the partnership between transnational corporations and foreign governments. Due to the social impacts of surveillance technology, relevant human rights include the right to privacy, freedom of opinion and expression, and the right to equality or free from discrimination. The types of materials used are academic books, peer-reviewed articles, news, press releases, news, corporate summary, and reports from think tanks and international organizations. Given the evolving nature of COVID-19 outbreaks, the sources gathered in the analysis section all date before May 1, 2020.

Chapter 1. Surveillance, Governmental Powers and Human Rights Norms

Norms refer to rules or standards of behavior, yet it is not a static concept. Information and communications technology create new possibilities, offers alternative ways of living, and redefines the boundary between public and private spheres. The interactions among political systems, private industry, and cultural traditions will have long-term impact on human rights norms and values.

As surveillance technologies emerge and develop, illiberal regimes are finding a new tool to reinterpret the ideals of freedom and equality. China, an authoritarian state, has developed a comprehensive surveillance system that is legitimized by a narrative of national and individual security. The expansion of state power is not only conspicuous in the domestic setting, but also exerts global influence through the export of surveillance technology. How does a state maintain legitimacy when intrusive policies may infringe on individual rights? What are the factors that affect the process of contestation and the exchange of ideas? How does norms interact with the behaviors of states? What is the relationship between security and liberty, and what could be the consequences if the balance between the two are not achieved?

A variety of disciplines and scholarship provides insights on the problem of state-citizen dynamics and the process of norm construction. By analyzing surveillance technology, the following chapter will focus on the security narratives and human rights implications, in particular the protection of citizens against the states. First, this chapter will provide a brief overview of surveillance industry, including its evolution, objectives and mechanisms. It is essential to study China in a broader context and how it fits into global trends. Second, I will look into how norms may emerge and diffuse, drawing theories from cybersecurity studies,

constructivism and international law. The third section will examine the use of surveillance technology in times of emergency, the expansion of state authority, and the balancing of human rights. The literature is drawn from surveillance studies and international human rights framework.

The Development of Surveillance as a Practice

Surveillance can relate to daily experience, a cultural phenomenon, a governance tool, and a condition of possibilities. In this thesis, it refers to a wide range of contexts within which "personal data is collected by employment, commercial, administrative agencies, as well as policing and security."[1] Surveillance has long been used as a governance tool and security apparatus. As the state authority increased, the motivation to track population and collect information became even stronger. The early requirements to register birth, marriage and deaths reflect similar governance logic as passport, social security card and health insurance.[2] Surveillance often represents citizen compliance with social order, and functions as a means of social control.[3] To improve efficiency and productivity, "surveillance society" has become a central and pervasive feature of modern society.[4]

As digital technology becomes more sophisticated, surveillance systems expand in its reach and frequency. For decades, it was common for governments to conduct wiretapping and message interception for intelligence and national security purposes.[5] Electronic technologies have greatly augmented surveillance capabilities, including video surveillance systems,

1 Lyon, ix.
2 David Lyon, *The electronic eye: The rise of surveillance society* (University of Minnesota Press, 1994): 4.
3 Lyon, 4.
4 Lyon, 24.
5 Ronald J. Deibert, "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace," *Millennium: Journal of International Studies* 32, no. 3 (2003): 514.

biometrics, facial recognition, big data analytics, and artificial intelligence software.[6] From targeted surveillance to mass surveillance, governments and corporations collect an increasing range of information on private lives, exploiting human experiences for control or profits.[7]

Surveillance has been on the rise globally since 9/11, which transformed the approaches of intelligence gathering and law enforcement. Surveillance tools are relatively low-cost, easy to obtain, and hard to detect. Many states around the world have adopted legislation to create a more permissive environment for surveillance, such as the United States Patriot Act and the United Kingdom Crime and Security Act.[8] According to a 2015 Freedom House report, 14 of 65 countries passed new laws to increase surveillance. France and Australia passed new measures authorizing wide-ranging surveillance, partly due to domestic terrorism concerns and the expansion of the Islamic State militant group.[9]

The public-private collaboration is common in digital surveillance. Governments have objectives and requirements, while private companies have "the incentives, the expertise and the resources to meet those needs."[10] As the major driver of technological advances, private companies develop surveillance software and provide technical support. Different forms of political systems determine the distinct relationships between public and private sectors. Yet in most countries, such collaboration operates with limited oversight, transparency, and data protection.[11] It is difficult to ensure state due diligence and end user-support, as private companies may be complicit in human rights abuses.

[6] Deibert, 515
[7] "Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression" (Human Rights Council, July 24, 2019).
[8] Deibert, 501–30.
[9] "Freedom on the Net 2015: Privatizing Censorship, Eroding Privacy," (Freedom House, October 2015)
[10] "Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression" (Human Rights Council, July 24, 2019).
[11] Human Rights Council, 2019.

Surveillance technology can be beneficial and used in legitimate ways. Governments around the world have been ambiguous to regulate tech industries, especially communications surveillance and sharing agreements. Yet without judicial authorization and independent oversight, unlawful and arbitrary surveillance can be highly intrusive and interfere with fundamental human rights.[12] The lack of regulation on the national and international level resulted in "ad hoc practices that are beyond the supervision of any independent authority."[13] A weak legal and regulatory environment contributes to the proliferation of surveillance technology, especially in countries with repressive policies. According to the NGO Reporters Without Borders, the Internet had become part of the "collateral damage" of the war on terror.[14]

Given the rate of technological change, legal measures tend to fall behind to a significant degree.[15] Existing legislation and practices are not updated or reviewed to incorporate new technology, and therefore inadequate to address emerging risks and challenges.[16] Human rights mechanisms have also been slow to assess the human rights implications of the Internet and new technology on communications surveillance and access to communications data.[17] It often takes years and even decades to reach international consensus on treaties and agreements.

Moreover, the risks posed by surveillance require a creative, forwarding-looking approach, yet existing human rights framework mostly responds to the past. From genocide, war crimes, to torture and discrimination, the international law community seeks accountability, retribution and reparation. However, the unrestricted spread of surveillance points to potential

[12] Human Rights Council, 2019
[13] Frank La Rue, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue" (United Nations General Assembly, Human Rights Council, April 17, 2013)
[14] "Enemies of the Internet Report 2012" (Reporters Without Borders, March 2012). https://issuu.com/rsf_webmaster/docs/rapport-internet2012_ang?backgroundColor=%2523222222
[15] Lyon, 13.
[16] Frank La Rue, 2013.
[17] Ibid.

harm in the future, including the possible data leaks, human rights implications, and invisible government interferences.

The Construction of New Norms

Although cyberspace is a new domain, the politics and dynamics of state power remain a continuity. The traditional International Relations (IR) theories, such as great power competition, national security, anarchy and sovereignty, are also applicable and relevant as surveillance technologies proliferate across the globe. As James Andrew Lewis points out, states are "the most dangerous actors" in cyberspace.[18] The external factors, such as the role of government, political trends, inter-state relations, and public opinions, determine the perceptions and strategies of cybersecurity.[19]

The rise of China's economic and technological strength will likely lead to conflicts of ideas, narratives, and ideologies in the international system. According to cybersecurity expert Adam Segal, cyberspace refers to "the global network of interconnected information technologies and the information on it."[20] He argues that one of the indicators of great cyber powers include an attractive narrative about cyberspace, in addition to the large or technologically advanced economy, public institutions that harness resources of the private sector, and strong military and intelligence agencies.[21]

Cyber norms are crucial to the activities of states and to the stability of the international system. James Lewis argues "norms are foundational for better governance," and developing

[18] James Andrew Lewis, *Rethinking Cybersecurity: Strategy, Mass Effect, and States* (Center for Strategic and International Studies, January 2018).
[19] Lewis, *Rethinking Cybersecurity*, 7.
[20] Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (United States: PublicAffairs, 2016): 38.
[21] Segal, *The Hacked World Order*, 39.

norms for responsible state behaviors is required to pursue a more safe and stable cyberspace.[22] The process of norm construction allows the states to maintain legitimacy and justify certain types of behavior.[23] As a result, various states are eager to push for alternative norms which better serve their strategic and geopolitical interests.

The ideals of the Internet were once considered to be open access of information and freedom of communication. An American invention, the Internet reflects free expression, individual liberty, and the aspiration to universal values. The U.S. government advocates "an open, interoperable, reliable, and secure Internet."[24] The promotion of this norm serves the ideological and economic interests of the United States and especially U.S. tech companies.[25]

Nonetheless, the Internet as a liberal, democratic and participatory platform is unlikely to sustain in a multipolar world. How cyberspace will be governed in the future is subjected to immense uncertainty, as cyber power may be particularly ephemeral.[26] The technological competition, the diverse forms of public-private relationships, and the conflicting views of Internet governance increases fragmentation in cyberspace.[27] One of the potential consequences is that it may be more difficult to reach consensus among states, undermining the prospect of a global and open Internet.

The Chinese government has both the cyber capabilities and intentions to redefine the norms of international behaviors. China perceives the Internet as threatening and imposing alien values, striving to reinstall the barriers of social control. Powers like Russia and China have been

[22] James Andrew Lewis, "Defining Rules of Behavior for Force and Coercion in Cyberspace," in "Confronting an "Axis of Cyber"? China, Iran, North Korea, Russia in Cyberspace" (Institute for International Political Studies, 2018): 162.
[23] Segal, *The Hacked World Order,* 116-117.
[24] "National Cyber Strategy of the United States of America" (The White House, September 2018).
[25] Segal, *The Hacked World Order*, 48.
[26] Segal, *The Hacked World Order,* 183.
[27] Ibid.

challenging international status quo and will continue to exploit the opportunities created by information technology.[28] Lewis calls this reassertion an "authoritarian alternative," an effort to "replace the U.S.-led international order and to rebalance the relationship between sovereignty and 'universal' values."[29] Chinese policy makers often justify their efforts as "de-Americanizing."[30] The pushback against liberal values will likely increase tension and undermine the U.S.-dominated narratives.

In an interdependent world, constructivist scholars also look into the centrality of norms and how these international norms evolve over time.[31] State behaviors and social interactions help shape the structure of world politics.[32] John Ruggie holds that normative factors, both domestic and international, influence the interests or behaviors of states.[33] The principles or beliefs affect the patterns of international outcome.[34] Through the diffusion of norms, the "collective intentionality" of state in turn creates new meanings, rights, and responsibilities in the international system.[35] Alexander Wendt also argues that shared knowledge and the practices of the actors involved are significant to understanding state behaviors.[36] Moreover, the multilateral process, such as the state's increased interactions in international institutions, can explain the changes in its military policy.[37]

[28] James Andrew Lewis, "Cognitive Effect and State Conflict in Cyberspace" (Center for Strategic & International Studies, September 2018).
[29] James Andrew Lewis, "China's Information Controls, Global Media Influence, and Cyber Warfare Strategy" (U.S. China Security and Economic Review Commission, May 4, 2017).
[30] Segal, *The Hacked World Order,* 183.
[31] Martha Finnemore, *The Purpose of Intervention: Changing Beliefs about the Use of Force* (Ithaca, NY: Cornell University Press, 2003).
[32] John Gerard Ruggie, "What Makes the World Hang Together? Neo-Utilitarianism and The Social Constructivist Challenge," *International Organization* 52, no. 4 (1998): 867.
[33] Ruggie, 864.
[34] Ruggie, 867.
[35] Ruggie, 870.
[36] Alexander Wendt, "Constructing International Politics," *International Security* 20, no. I (1995): 77-78.
[37] Alastair Iain Johnston, "Learning versus Adaptation: Explaining Change in Chinese Arms Control Policy in the 1980s and 1990s," *The China Journal* 35 (1996): 27-61.

Martha Finnemore and Duncan B. Hollis define cybersecurity norms as "social creatures," referring to content and products, as well as specific contexts, processes, and interactions.[38] They argue that the power of norms "lies in the processes by which they form and evolve."[39] The nature of norms is dynamic and ever-changing. Actors are capable of modifying and reinterpreting existing norms in different circumstances.[40] Finnemore and B. Hollis identify several factors in norm construction, such as entrepreneurship and changed habits, as well as incentives, persuasion, and socialization.[41] States or norm entrepreneurs pursue strategic choices and accept trade-offs in facilitating new cybernorms.[42] Their article applies the general characteristics of norm cultivation in cyberspace and explains "how norms evolve, spread, and affect behaviors."[43]

With regard to the content of norms, this essay will focus on human rights norms and international law framework. The dynamics of customary international law partly stem from a process of establishing norms. Article 38 of the International Court of Justice enlists one of the sources of international law, which refers to "international custom as evidence of a general practice is accepted as law." The general practices of states, if widely accepted, can impose constraints on other actors in the international system. *Opinio juris* is also a factor in customary international law, which denotes a subjective element or belief about a state's legal obligation.[44]

The international human rights framework not only refers to legally binding obligations, such as treaties and tribunals, but also soft laws, including declarations and quasi-legal

[38] Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *American Journal of International Law* 110, no. 3 (2016): 427.
[39] Ibid.
[40] Finnemore and Hollis, 428.
[41] Ibid.
[42] Finnemore and Hollis, 464.
[43] Ibid.
[44] Omri Sender and Michael Wood, "A Mystery No Longer? Opinio Juris and Other Theoretical Controversies Associated with Customary International Law," *Israel Law Review* 50, no. 3 (2017): 299-330.

instruments. While power politics plays an essential role in shaping patterns of behaviors, international law and institutions also exert pressure beyond the nation-states, shaping outcomes through norms, ideas and soft power. The Universal Declaration of Human Rights (UDHR) in 1948 was not legally binding yet formed the modern foundation of the human rights regime. The UDHR aspired to balance between individual rights and collective interests. It proclaimed that "all human beings are born free and equal in dignity and rights," and emphasized that "everyone has duties to the community in which alone the free and full development of his personality is possible."[45] International organizations, such as the United Nations, provide a political platform to discuss human rights issues, generate consensus, and create new norms.[46]

Discourse and dialogues are influential to bring about positive transformations. As Abbott and Snidal argue, soft law "facilitates compromise and thus mutually beneficial cooperation between actors with different interests and values, different time horizons and discount rates, and different degrees of power."[47] Nonetheless, state's socialization and engagement with international institutions may also exploit the existing mechanisms to serve their own interests. Over the past decade, China has been an active participant in the UN General Assembly and the Human Rights Council, shaping the scope of human rights norms such as the right to development.[48]

How to balance security and liberty and reconcile the conflicts of rights becomes a challenging task for states, civil societies, treaty bodies, and international institutions.

[45] Universal Declaration of Human Rights (Dec. 10, 1948). https://www.un.org/en/universal-declaration-human-rights/

[46] Philip Alston and Ryan Goodman, *International Human Rights: The Successor to International Human Rights in Context* (Oxford, United Kingdom: Oxford University Press, 2013).

[47] Kenneth W. Abbott, and Duncan Snidal, "Hard and Soft Law in International Governance," *International organization* 54, no. 3 (2000): 423.

[48] "The Right to Development: China's Philosophy, Practice and Contribution" (The State Council Information Office of the People's Republic of China, December 2016). http://www.scio.gov.cn/32618/Document/1534069/1534069.htm

International law provides the basis for assessing the scope and restrictions of human rights affected by surveillance technology. In the context of counterterrorism, Fionnuala Ní Aoláin, the Special Rapporteur for Counter Terrorism and Human Rights, argues that the balancing and trade-offs approach can "increase the lack of integration" between security and rights.[49] Instead, it is essential to view security and liberty as interdependent, and states should seek to protect human rights while countering terrorism.[50] As UDHR pronounced, "everyone has the right to life, liberty and security of person."[51] The suppression of human rights can trigger a wider security crisis. Take China as an example, the lack of free press was partly responsible for the slow response and testing of COVID-19 in the earlier stages.[52]

Surveillance, Emergency, and the Expanded Power of Government

Surveillance studies grapple with the concept of security, a changing approach in risk management, and the driving forces behind surveillance. This body of literature not only analyzes the logic and functions of a surveillance system, but also examines its broader implications on culture and society. The negative effects posed by surveillance technology include increasing inequality, human rights abuses, and encroachment on private space.

The perception of risks and security determines the design of surveillance systems. Identifying 9/11 as a turning point, Louise Amoore argues that the "low probability, high consequence" events contribute to the politics of possibilities, aiming to make the uncertain

[49] Fionnuala Ni Aolain, "How Can States Counter Terrorism While Protecting Human Rights," *Ohio NUL Rev.* 45 (2019): 390.
[50] Ibid.
[51] Universal Declaration of Human Rights (Dec. 10, 1948).
[52] Gerry Shih, "In China's Coronavirus Crisis, a Fleeting Flicker of Freer Speech," *The Washington Post,* Feb. 6, 2020.

future calculable.[53] The focus has shifted from strict, deductive probability to anticipatory approaches, incorporating "suspicion, imagination and preemption."[54] The change of attitudes in managing uncertainty leads to the intersection of security and economy, redefining the relationship between individuals and states.[55] As a result, this risk management model "enables fractionation of ever-more finite categories of life,"[56] which also fits the underlying logic of surveillance systems. With regard to an unpredictable environment, Ayse Ceyhan suggests that biometrics and identification technologies have become markers of certainty. She argues that contemporary surveillance is a "security assemblage," functioning through a network of public, private and transnational databases.[57]

By employing surveillance technology, governments intend to achieve different political objectives, and sometimes repressive policies. An analysis of Rwanda's surveillance and politics, Andrea Purdeková's article discusses the network of "eyes and ears," which monitors both public and private interactions.[58] Purdeková argues that the penetrating state reach in Rwanda has enhanced its central power and increased its effectiveness of political control and mobilization.[59] During COVID-19 outbreaks, China has exhibited similar dynamics and decentralization through the "grid management" system, which ultimately led to the expansion of national power.

Jeremy Bentham created the panopticon model, which refers to the architectural apparatus composed of a central tower and the peripheric building divided into cells. Michel

[53] Louise Amoore, *The Politics of Possibility: Risk and Security beyond Probability* (Durham, NC: Duke University Press, 2013): 7.
[54] Amoore, 9.
[55] Amoore, 12.
[56] Ibid.
[57] Ayse Ceyhan, "Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics," *Surveillance & Society* 5, no. 2 (2008): 119.
[58] Andrea Purdeková, "'Even If I Am Not Here, There Are So Many Eyes': Surveillance and State Reach in Rwanda," *Journal of Modern African Studies* 49, no. 3 (2011): 487.
[59] Purdeková, 490-493.

Foucault used the mechanism of panopticon as a metaphor to illustrate the relationship between surveillance and power. The supervisor in the tower sees and monitors the individuals. People in the prison cells are seen but cannot see the supervisor, and this "invisibility is a guarantee of order." In prisons, hospitals, schools, and factories, this mechanism assures "dissymmetry, disequilibrium, and differences," and that surveillance is permanent in its effects. As a laboratory of disciplinary power, panopticon can be used to carry out behaviors and to "train or correct individuals." The power of norms comes into effect, as it speaks to measurement, homogeneity, and classification. The normalization becomes a coercive means to erase individual differences. [60]

While the government works with private sectors to monitor individuals, tech companies such as Google, Facebook and Amazon, rely on "surveillance capitalism" as their primary profit model.[61] Shoshana Zuboff asserts that corporations translate human experiences into data and sell predictions, leading to targeted modifications and control of individual behaviors.[62] Tim Wu also discusses the behavioral influence, which explains the link between technological surveillance and power. [63] Based on the information about someone's private life, a variety of techniques can be used to influence how individuals make choices. The surveillance model of capitalism encroaches on privacy and human autonomy, and the combination of state power and platform surveillance can have terrifying consequences.[64] The difficulty is that citizens with compromised human rights may not even be aware of the prediction and control.

[60] Michel Foucault, *Discipline and Punish: The Birth of the Prison* (Vintage Books, 1995).
[61] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019).
[62] Ibid.
[63] Tim Wu, "Bigger Brother," *The New York Review of Books*, April 9, 2020.
[64] Ibid.

While the surveillance studies analyze the motivations, objectives, and mechanism of surveillance systems, scholarship on international law examines the legal implications of surveillance, especially the increased ambiguity of security narrative. Although surveillance has always been utilized by the government in its daily functions, it is often the major crisis and disasters that trigger the expansion of surveillance technology. Various forms of government tend to respond to threats by increasing the reach of state control over its citizens. For instance, after 9/11, the National Security Agency initiated the domestic-wiretapping program to collect metadata and obtained an increased level of surveillance power.[65] The world witnessed the increased push from governments to pass surveillance laws and policies.[66] London is also heavily surveilled, with the most cameras of any non-Chinese city. [67]

The security and liberty dilemma can be particularly challenging during emergencies, which permit the increase of state capacity under unusual circumstances. International legal regime provides some basic principles on how to maintain the balance between the public goods and individual interests, as well as the criteria to evaluate the legitimacy of emergency strategies and policies.

The states are not only discouraged from unjustified restrictions, but also have positive obligations to "respect, protect and fulfill" human rights, especially in times of crisis.[68] To strike a balance between national security and human rights, the international law framework recognizes certain restrictions posed by the state. Fundamental freedoms, such as the freedom of

[65] Babu-Kurra, "How 9/11 Completely Changed Surveillance in U.S," *Wired,* September 11, 2011.
[66] "Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy" (Freedom House, November 2017).
[67] Matthew Keegan, "Big Brother is Watching: Chinese City with 2.6m Cameras is World's Most Heavily Surveilled," *The Guardian,* December 2, 2019.
[68] Gabor Rona and Lauren Aarons, "State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace," *Journal of National Security Law & Policy* 8, no. 3 (2016): 503–30.

thought, expression, association and assembly are not absolute,[69] but subjected to limitations and derogations. A balanced approach is suggested to consider the right of others and public interests, namely, "public order, health, morality, or national security."[70] Article 4 of the International Covenant on Civil and Political Rights gives the state the right of derogation "in times of public emergency which threatens the life of the nation."[71]

Legal scholars contribute to the "security vs. liberty" debate by analyzing implications of unspecified security narratives and safeguards against abuses of power. When collective interests or public security are in conflicts with individual rights, international law provides a framework for balancing the conflicts of diverse human rights. Several principles are proposed to define the circumstances of government restrictions, such as the rule of law, legitimate aim, proportionality, and presumption of freedom.[72] The government bears the burden to prove the validity of the restriction.[73] A state of emergency also asks for careful justification, that specific measures should be necessary and legitimate, and "strictly required by the exigencies of the situation."[74]

Excessively prioritizing national security can have a chilling effect on fundamental freedoms and human rights protection. The justification of national security is often "misapplied or abused to the detriment of freedom of expression."[75] States often exploit the "vague and unspecified notions of national security" to justify the targeting of vulnerable groups, such as journalists and activists.[76] According to a UN report on targeted surveillance, limited restraints

[69] Kevin Boyle and Sangeeta Shah, *Thought, Expression, Association, and Assembly*, in "International Human Rights Law," ed. Daniel Moeckli et al. (Oxford: Oxford University Press, 2010), 257–79.
[70] Boyle and Shah, 217-218.
[71] International Covenant on Civil and Political Rights (December 16, 1966). https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx
[72] Boyle and Shah, 219.
[73] "The Johannesburg Principles on National Security, Freedom of Expression and Access to Information" (ARTICLE 19, November 1996).
[74] "General Comment No.29, States of Emergency (Article 4)" (Human Rights Committee, July 24, 2001).
[75] Boyle and Shah, 228.
[76] Frank La Rue, 2013.

on the sale and transfer of surveillance technology has exacerbated human rights violations, such as arbitrary detention and torture.[77] A lack of national standards to regulate private surveillance industry is likely to undermine transparency and accountability, threatening the right to privacy and fundamental freedom.[78] Joel Bergenfalk also suggests that a lack of feasible policies and guidelines makes it challenging to tackle future human rights concerns.[79] Two major factors concerning AI, namely efficiency and human imperfection, will further raise concerns for the relevance of human rights doctrines and policies.[80]

In summary, theories of international relations will explain the process of norm construction, what factors contribute to the changes, and interactions among states and other non-state actors. International law provides a legal framework to analyze the lawfulness and legitimacy of state behaviors. Two case studies focus on export regulations and state of emergency, and their influence on human rights norms and practices. This thesis will analyze China's role in developing an alternative security norm which is likely to interfere with liberal values and behaviors of other states. Through the proliferation of surveillance technology, Chinese government and tech companies represent a different vision for public security, governance and stability.

[77] Human Rights Council, "Surveillance and Human Rights," July 24, 2019.
[78] Ibid.
[79] Joel Bergenfalk, "AI and Human Rights — An Explorative Analysis of Upcoming Challenges," *Human Rights Studies,* (2019): 4.
[80] Bergenfalk, 35-37.

Chapter 2. Surveillance in China

This section will look into China's comprehensive surveillance systems, the role of the government and tech companies, as well as its security narratives for the expansion of surveillance. With regard to Internet governance, the Chinese government has developed a comprehensive regulatory framework for cybersecurity, critical infrastructure, Internet content, and information and telecommunications technology.[81] China was able to clear restraints on expanding digital surveillance, Internet filtering and facial recognition.

Over the past decade, China has passed numerous laws with increasingly expansive interpretation of national security. The National People's Congress authorized a new national security law in 2015, increasing government control over cyberspace.[82] The texts read that China would make key internet and information systems to be "secure and controllable."[83] In 2017, detailed implementing regulations to the Counter Espionage Law (2014) said that "fabricating or distorting facts, publishing or disseminating words or information that endanger state security" are considered as an espionage-related offence.[84] The Cybersecurity law was approved in 2016. Aimed to erase the anonymity of online activities, the law required the Internet users to register their real names.[85] The Chinese government perceives threats in a preemptive way, and adopts a vague, expansive notion of security.

[81] Samm Sacks, "China's Emerging Cyber Governance System" (Center for Strategic & International Studies). https://www.csis.org/chinas-emerging-cyber-governance-system
[82] "China Passes New National Security Law Extending Control over Internet," *The Guardian*, July 1, 2015.
[83] "Xinhua Insight: China Adopts New Law on National Security," *Xinhua*, July 1, 2015.
[84] "China's Intelligence Law and the Country's Future Intelligence Competitions," Government of Canada. https://www.canada.ca/en/security-intelligence-service/corporate/publications/china-and-the-age-of-strategic-rivalry/chinas-intelligence-law-and-the-countrys-future-intelligence-competitions.html
[85] Paul Mozur, "China's Internet Controls Will Get Stricter, to Dismay of Foreign Business," *The New York Times*, November 7, 2016.

To counter globalism and the spread of Western culture, China has sought to promote its nationalist sentiment and socialism with Chinese characteristics.[86] President Xi emphasized the necessity to cherish traditional cultural roots and bolster global influence of Chinese culture.[87] Values like loyalty, honesty and impartiality are encouraged, in contrast to "self-centered behavior, decentralism," and disregard of the rules.[88] The Internet is viewed as the external interference.[89] While facing the complexity and vulnerability of domestic issues, the Chinese government has put an end to the liberalizing potential of the Internet.[90] Rather than individualism and freedom, China's cyberspace governance values security, stability and order.

To promote the "dissemination of core socialist values," China has established a cyber monitoring, early warning, and information communication system.[91] Tightly controlled information, the Great Firewall, censorship on social media, video surveillance and facial recognition allow the government to provide its own narratives and silence the dissidents.[92] In Xinjiang, where surveillance is ubiquitous, Chinese officials have claimed to prioritize social security, justifying the use of surveillance tools as preventing deadly terrorist attacks and other crimes.[93]

In addition to the regulatory environment, China also has strong technological capabilities to achieve its goals. China's rise in economic and military power is accompanied by

[86] "Backgrounder: Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era," *Xinhua*, March 17, 2018.
[87] Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era," Delivered at the 19th National Congress of the Communist Party of China, October 18, 2017.
[88] Xi Jinping, October 18, 2017.
[89] James Lewis, "Cognitive Effect and State Conflict in Cyberspace," 2018.
[90] Adam Segal, "When China Rules the Web," Foreign Affairs, September/October 2018.
[91] "Overview of China's Cybersecurity Law" (KPMG China, February 2017). https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf
[92] Isobel Cockerell, "Inside China's Massive Surveillance Operation," *The Wired*, May 9, 2019.
[93] Josh Chin, "Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life," *The Wall Street Journal*, December 19, 2017

a growing dominance in the high-tech industry. State capitalism and government intervention indicate that China can direct its resources to priority industries.[94] State-owned firms and certain sectors receive subsidies, protected markets, and favorable loans.[95] In recent years, China has established many government-backed funds worth billions of dollars that target the advanced manufacturing and technology sectors, including a 40 billion yuan fund for high-tech industries, and a 147.2 billion yuan fund for new materials, information technology, and electrical equipment.[96] Decades of economic growth allows China to increase its research and development (R&D) spending, which has grown by an average of 20% a year since 1999.[97] The R&D investment reached $410 billion in 2016, more than that of Japan, Germany, and South Korea combined.[98] The Chinese government wants to reduce its dependence on foreign suppliers of digital and communications equipment, leading the world in advanced technologies such as artificial intelligence, quantum computing, and 5G networks.[99]

As the next generation of wireless networks, 5G is expected to be up to 100 times faster than 4G networks,[100] and promises to "revolutionize the entire global economy."[101] Faster connection speeds will enable the Internet of Things and precise surveillance systems. [102] In 2018, Huawei spent approximately $16 billion on R&D, roughly 15% of annual sales.[103] It is

[94] Steven Rattner, "Is China's Version of Capitalism Winning," *The New York Times,* March 27, 2018.
[95] Robert J. Samuelson, "Why China Clings to State Capitalism." *The Washington Post,* January 9, 2019.
[96] Yoko Kubota, "China's New $21 Billion High-Tech Manufacturing Fund Likely to Rankle U.S.," *The Wall Street Journal,* November 20, 2019.
[97] Ibid.
[98] Ezekiel Emanuel, Amy Gadsden and Scott Moore, "How the U.S. Surrendered to China on Scientific Research," *The Wall Street Journal,* April 19, 2019.
[99] Segal, "When China Rules the Web," 2018.
[100] Elliot Bentley and Sarah Krouse, "How Fast 5G Mobile Internet Feels," *The Wall Street Journal*, February 22, 2019.
[101] Keith Johnson, Elias Groll, "The Improbable Rise of Huawei," *Foreign Policy,* April 3, 2019
[102] James Rundle and Angus Loten, "The Power of Combining 5G and AI," The Wall Street Journal, November 8, 2019.
[103] Louise Lucas, and James Kynge, "Huawei Continues Global Push Despite Setbacks in West," *Financial Times,* December 16, 2018.

now the top company of 5G patents internationally, such as data transmission and network security.[104]

China's centralized approach is also favorable to develop artificial intelligence. As Yuval Noah Harari argues, democracy and dictatorship represent two different data-processing systems. While dictatorship concentrates information and power in one place, democracy distributes them among many people and institutions.[105] As a result, the centralized tendencies of artificial intelligence can be a decisive advantage for China,[106] as it has huge data sets, strong government support, and an environment with little concern for privacy.[107] The combination of 5G networks and artificial intelligence is able to greatly empower surveillance capability.[108]

Due to increasingly sophisticated technology, the Chinese government is able to push for comprehensive surveillance systems. Skynet, a literal translation of its Chinese name "Tianwang," is a big-data police system composed of video surveillance, facial recognition, and artificial intelligence.[109] To catch criminals, CCTV cameras are ubiquitous in airports, train stations, and streets. According to South China Morning Post, Skynet had 170 million cameras in 2017 and the government plans to add another 400 million units nationwide by 2020.[110] Although officials say that the objective of Skynet is to capture more fugitive suspects and

[104] Johnson and Groll, "The Improbable Rise of Huawei," *Foreign Policy*, April 3, 2019.
[105] Yuval Noah Harari, "Why Technology Favors Tyranny," *The Atlantic,* October 2018.
[106] Ibid.
[107] Adam Segal, "Chinese Technology Development and Acquisition Strategy and the U.S. Response," Council on Foreign Relations, December 12, 2017.
[108] James Rundle and Angus Loten, "The Power of Combining 5G and AI," *The Wall Street Journal,* November 8, 2019.
[109] Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," *The New York Times,* July 8, 2018.
[110] Stephen Chen, "How tensions with the West are putting the future of China's Skynet mass surveillance system at stake," *South China Morning Post,* September 23, 2018.

corrupt officials,[111] the system also puts political dissidents, rights activists, and journalists at greater risk. A permissive regulatory environment raises concerns over human rights protections.

In addition, China's surveillance system is not limited to the public security domain. The social credit system aims to monitor and control people's daily routines and activities. The system rates the "trustworthiness" of citizens by combining data on their online and offline behaviors. Millions of citizens have been prohibited from buying flights or train tickets if they are put on the blacklists for social credit offences.[112] The violations may range from spreading false information and taking drugs to smoking on a train and not paying taxes.[113] Local activists also reported that their freedom of movement is restricted for criticizing government policies.[114] Domestic companies are implementing the measures to incorporate state-run systems, amplifying the effects of state's blacklists.[115] To establish a unified social credit system, the Chinese government also plans to combine private-run systems such as the Sesame Credit, a financial credit score.[116] Legal scholarship argues that the Chinese government is trying to replace "rule of law" with "rule of trust," which relies on wide-ranging, arbitrary and disproportionate punishments."[117]

The following two chapters are case studies about COVID-19 outbreaks and Huawei's "safe city" project, looking at the expansion of surveillance in distinct circumstances. Under the public health crisis, declaring a state of emergency permits certain restrictions for human rights, such as the right to privacy. The strategies for mitigating infectious disease pushes for public and

[111] "China Launches "Sky Net 2019" to Capture Fugitive Officials," *Xinhua*, January 28, 2019.
[112] Lily Kuo, "China Bans 23m from Buying Travel Tickets as Part of 'Social Credit' System," *The Guardian*, March 1, 2019.
[113] Ibid.
[114] "Freedom on the Net 2018: The Rise of Digital Authoritarianism" (Freedom House, October 2018).
[115] Ibid.
[116] Freedom on the Net 2018.
[117] Yu-Jie Chen, Ching-Fu Lin, and Han-Wei Liu, "Rule of Trust: The Power and Perils of China's Social Credit Megaproject," *Columbia Journal of Asian Law* 32, no. 1 (2018): 1–36.

private collaboration in surveillance. From domestic to international, China also contributes to the global proliferation of surveillance technology. Through a process of sale and export, surveillance also represents a narrative of stability and public security, which sometimes is in tension with human rights norms.

Chapter 3: COVID-19: Emergency Power and Expansion of Surveillance

While the export of surveillance technology is gradual and intangible, altering the international system in the long run, the COVID-19 outbreak is likely to transform societies in a sudden yet fundamental way. Within three months, a coronavirus outbreak in Wuhan, China has developed into a pandemic with over 2.5 million cases worldwide.[118] Globalization drives increasing specialization of labor and efficiency, yet an infectious disease has revealed the fragility of such interdependence.[119] A global health crisis has the potential to overwhelm healthcare systems and threaten economic growth and stability.

Public health emergencies grant the state legitimate power and authority to impose restrictive policies. As governments around the world have been struggling to mitigate the situation, it is extremely challenging to balance between public health and economy, security and liberty, or collective interests and individual rights. One of the public health strategies is to trace and monitor contacts of infected people, which encourages the expansion of surveillance systems. Without judicial or independent oversight, the future of a surveillance society may look like the panopticon, where every citizen is watched by an invisible central power. This chapter will focus on the use of surveillance, China's narratives during COVID-19 outbreaks, and the human rights implications.

[118] "Global coronavirus cases pass 2.5 million as U.S. tally surpasses 800,000," *Reuters*, April 21, 2020.
[119] Henry Farrell and Abraham Newman, "Will the Coronavirus End Globalization as We Know It?" *Foreign Affairs*, March 16, 2020.

Balancing Human Rights During the Pandemic

COVID-19 is the infectious disease caused by a recently discovered coronavirus. Around 80% people recover from the disease without special treatment, yet around 1 out of every six people who gets COVID-19 becomes seriously ill and develops difficulty breathing.[120] Older adults and people of any age who have serious underlying medical conditions might be at higher risk for severe illness from COVID-19, such as lung disease, heart problems, diabetes, and cancer.[121]

The virus that causes COVID-19 is thought to spread very easily and sustainably between people, including close contact and respiratory droplets from infected people.[122] Some studies have suggested that COVID-19 may be spread by people who are not showing symptoms.[123] The transmission dynamics of the coronavirus determines that a comprehensive set of government interventions is required to protect public health.[124] For most governments, the goal is to slow the spread of the virus or "flatten the curve."[125] Given the capacity of the healthcare system, the explosive rise of cases may overwhelm hospitals and possibly lead to higher fatality rates. Reducing the number of confirmed coronavirus cases will assure a relatively stable rate of hospitalization, and provide more time for doctors, nurses, scientists, and government officials to respond and prepare.[126]

[120] "Q&A on Coronaviruses (COVID-19)," World Health Organization. https://www.who.int/news-room/q-a-detail/q-a-coronaviruses
[121] "Groups at Higher Risk for Severe Illness," Center for Disease Control and Prevention. https://www.cdc.gov/coronavirus/2019-ncov/need-extra-precautions/groups-at-higher-risk.html
[122] "How COVID-19 Spreads," Center for Disease Control and Prevention. https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/how-covid-spreads.html
[123] Ibid.
[124] "Report of the WHO-China Joint Mission on Coronavirus Disease 2019 (COVID-19)" (World Health Organization, February 16-24, 2020).
[125] Siobhan Roberts, "Flattening the Coronavirus Curve," *The New York Times*, March 27, 2020.
[126] "How COVID-19 Spreads."

The right to health is a well-established human right in international law. The constitution of the World Health Organization proclaims that "the enjoyment of the highest attainable standard of health is one of the fundamental rights of every human being without distinction of race, religion, political belief, economic or social condition."[127] Realizing the right to health is a legal obligation enshrined in the International Covenant on Economic, Social and Cultural Rights and other international treaties.[128] States bear the primary responsibility for realizing the right to health for the population as a whole, balancing health with other policy and social goals.[129] In times of pandemic, governments have an obligation to prevent, treat and control infectious disease, and introduce measures like screening, contact tracing, isolation and quarantine.[130]

States can declare public health emergencies to trigger a range of additional powers, justifying certain restrictions and derogations of other rights. In times of coronavirus outbreak, governments have significantly increased their surveillance capacity to track, monitor, and control individuals. Yet the role of state involves an intricate balance between security and liberty. The control of infectious disease may interfere with freedom of movement, the right to property, and the right to control one's health and body.[131] The closure of schools may interrupt the right to education, especially the poor and homeless households. The shutdown of non-essential business can lead to a high rate of unemployment and undermine economic and social rights.

Moreover, states have due diligence to respect, protect and fulfill human rights. COVID-19 not only disproportionately affects people over 65 and those with a compromised immune

[127] Constitution, World Health Organization. https://www.who.int/about/who-we-are/constitution
[128] "Advancing the Right to Health: The Vital Role of Law" (World Health Organization, 2017).
[129] "Advancing the Right to Health," 2017
[130] Ibid.
[131] "Advancing the Right to Health," 153.

system, but also communities with low socioeconomic status.[132] According to a WHO report, the great health burdens mostly "fall on the most vulnerable, marginalized and impoverished individuals," and the goal of law is to protect them from discrimination and provide access to essential services.[133] Non-state actors are also likely to exacerbate human rights violations. Mass quarantine, isolation and travel restrictions may lead to discrimination against patients and people from the outbreak zone. When human rights are ignored or disregarded during emergencies, significant sections of the population are under the risks of being marginalized.[134]

Therefore, emergency power should not be exercised in an arbitrary and discriminatory way.[135] The government should strive to pursue a refined public health strategy and minimize the tension between public goods and personal rights. The WHO identifies a set of ethical principles, including public health necessity, reasonable and effective means, proportionality, distributive justice, trust and transparency.[136] In particular, the principle of proportionality requires that the government must strive to ensure that there is "a reasonable fit between the coercive measures imposed on individuals and the public health benefit that they seek to achieve."[137] The measures adopted should be the least burdensome, available and reasonably appropriate to mitigate the risks in question.

To slow the transmission of infectious disease, the public health strategies range from lockdowns, school closures to travel restrictions and bans on mass gatherings.[138] Governments and private companies have been utilizing surveillance technology for contact tracing, which

[132] Max Fisher and Emma Bubola, "As Coronavirus Deepens Inequality, Inequality Worsens Its Spread," *The New York Times*, March 15, 2020.
[133] "Advancing the Right to Health," xvi.
[134] "Advancing the Right to Health," 12.
[135] "Advancing the Right to Health," 166.
[136] "Advancing the Right to Health," 153-154.
[137] Ibid.
[138] "Coronavirus: Countries Enforce Mass Closures to Stem Spread," *BBC*, March 13, 2020.

allows the transition to normal life while containing the spread of pandemic.[139] Surveillance can also help public health officials to track the effectiveness of executive orders and monitor potential violations. The restrictions of human rights are considered to be legitimate and necessary trade-offs during emergencies, yet the scale of social control varies depending on the local context. In both democratic and authoritarian countries, the use of surveillance systems can be widespread and intrusive.

In South Korea, epidemiological investigations and contact tracing become the alternatives to slow the transmission rather than a total lockdown. After the MERS outbreak, South Korea revised the law to prioritize social security over individual privacy at times of infectious disease outbreak.[140] When someone tests positive, health workers would retrace the patient's recent movement using interviews, security camera footage, credit card record, and GPS data from their cars and cellphones. Emergency alerts will be sent out when new cases are discovered in the district, in order to test and isolate more people who might have been exposed to the virus. South Korean officials can enforce self-quarantine through a location-tracking smartphone app. By identifying and treating infections early and segregating mild cases to special centers, South Korea can save the hospital resources to treat seriously ill patients and manage to keep its fatality rate among the lowest in the world.[141] The names on the travel logs are kept confidential, yet the identity of the patient might be revealed through the details of personal lives.[142]

[139] Tony Romm, Drew Harwell, Elizabeth Dwoskin and Craig Timberg, "Apple, Google Debut Major Effort to Help People Track if They've Come in Contact with Coronavirus," *The Washington Post,* April 10, 2020.
[140] Max Fisher and Choe Sang-Hun, "How South Korea Flattened the Curve," *The New York Times,* March 23, 2020.
[141] Ibid.
[142] Min Too Kim and Simon Denyer, "A 'Travel Log' of the Times in South Korea: Mapping the Movements of Coronavirus Carriers," *The Washington Post,* March 13 ,2020.

Singapore initiated a similar contact tracing program. The Infectious Disease Act gives the country "wide latitude in prioritizing the common good over privacy concerns."[143] The details of the patient's movement and activities are released online, and close contacts of patients are put into mandatory quarantine to limit the spread.[144] Taiwan also took early and aggressive response to COVID-19. The government integrated its national health insurance database with the immigration and customs database for big data analytics.[145] Through QR code scanning and health declaration form, health officials were able to classify the risks of travelers based on their travel history in the past 14 days. Those with higher risks were quarantined at home and monitored through mobile phone to ensure compliance. On February 18, the government announced that all hospitals, clinics and pharmacies in Taiwan would have access to patients' travel histories.[146]

Despite the initial reluctance, Western liberal countries are considering more aggressive public health strategies that may infringe on individual liberty. Government officials across the U.S. are using cellphone location data to analyze the presence and movement of people in certain areas.[147] Google and Apple also announced that they will partner on Bluetooth-based contact tracing, hoping to "harness the power of technology" to help slow the spread of the disease and accelerate the return of everyday life.[148] If a person has been tested positive, they can voluntarily

[143] Hannah Beech, "Tracking the Coronavirus: How Crowded Asian Cities Tackled an Epidemic," *The New York Times*, March 17, 2020.
[144] Ibid.
[145] Jason Wang, C., Chun Y. Ng, and Robert H. Brook. "Response to COVID-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing." *JAMA* (2020).
[146] Ibid.
[147] Byron Tau, "Government Tracking How People Move Around in Coronavirus Pandemic," *The Wall Street Journal*, March 28, 2020.
[148] "Apple and Google Partner on COVID-19 Contact Tracing Technology," April 10, 2020. https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

report that to the app, and people in the vicinity with either Apple or Google software will be notified.[149]

Emergency Response and Surveillance in China

The magnitude of the perceived threats determines how draconian public health strategies can be.[150] Infectious disease is often regarded as security threats, with the potential to destabilize the state and diminish its power.[151] Severe outbreaks can have destructive effects on the legitimacy of governance and social cohesion. Driven by fear and uncertainty of the novel virus, it is difficult for governments to assess the level of the threat accurately.[152] In China, the intrusive and ineffective use of surveillance has revealed the dysfunction of governance structures.

During the early stages, China's automatic mechanism of communications surveillance became one of the biggest impediments to solve a public health crisis. Through monitoring and control of Chinese social media, the government is able to silence political dissidents, activists, and censor any sensitive topics online. Li Wenliang, an ophthalmologist in Wuhan, sent a message to fellow doctors on December 30. He warned in a WeChat group that the virus was similar to SARS, which led to the 2003 coronavirus outbreak.[153] Four days later he was summoned to the Public Security Bureau, and signed a statement denouncing his warning as "an

[149] Tony Romm, Drew Harwell, Elizabeth Dwoskin and Craig Timberg, "Apple, Google Debut Major Effort to Help People Track If They've Come in Contact with Coronavirus," *The Washington Post,* April 10, 2020.
[150] Frank M. Snowden, *Epidemics and Society: From the Black Death to the Present.* (Yale University Press, 2019): 8.
[151] Andrew Price-Smith, *Contagion and Chaos: Disease, Ecology, and National Security in the Era of Globalization* (Cambridge, MA: MIT Press, 2009): 194.
[152] Ibid.
[153] "Li Wenliang: Coronavirus Death of Wuhan Doctor Sparks Anger," *BBC*, February 2020.

unfounded and illegal rumor."[154] Dr. Li was among the eight doctors who were reprimanded by officials, as they "severely disturbed the social order."[155] Instead of confronting the outbreak, the officials played down the risks and were reluctant to act.

Since the outbreak occurred, Chinese scientists quickly identified the virus and shared the genome sequences with the World Health Organization on Jan.12.[156] Nonetheless, the "incongruity between 21st-century science and 19th-century politics" led to the initial missteps of government response.[157] Only until January 20, Dr. Zhong announced in a state television that there was no doubt that the coronavirus spread with human contact, which Wuhan's health commission previously denied. [158]

The death of Li Wenliang triggered widespread criticism of China's communist rule. The inadequate response and lack of transparency generated anger, frustration, and despair among Chinese citizens. The legitimacy of China's surveillance system is undermined, as it prioritizes social stability yet fails to protect human security. Under the perception of illegitimate governance, states often take severe or even draconian measures to restore order and authority.[159] In China, the harsh criticism about restricting freedom of expression was countered by heightened surveillance and control.

Beijing blamed local authorities for the crisis, replacing senior officials in Hubei and launched investigations regarding alleged negligence.[160] Surveillance on social media was

[154] Chris Buckley, "Chinese Doctor, Silenced After Warning of Outbreak, Dies from Coronavirus," *The New York Times*, February 6, 2020.
[155] "Li Wenliang," *BBC*.
[156] "China publishes timeline on COVID-19 information sharing, int'l cooperation," *Xinhua*, April 6, 2020.
[157] Nicholas Kristof, "I Cannot Remain Silent," *The New York Times*, February 15, 2020.
[158] Chris Buckley and Steven Lee Myers, "As New Coronavirus Spread, China's Old Habits Delayed Fight," *The New York Times*, February 1, 2020.
[159] Price-Smith, *Contagion and Chaos*, 210.
[160] Chun Han Wong, "Beijing Portrays President Xi Jinping as Hero of Coronavirus Fight," *The Wall Street Journal*, March 8, 2020.

augmented, especially targeting antiparty rhetoric and demands for free speech.[161] Local officials have continued to crack down on "online rumors" about the virus, which was lauded by China's public security ministry.[162] Chinese media outlets were to report on positive stories about the coronavirus outbreak. Internet platforms, especially social media, deleted a range of articles that criticized Chinese government's response. Chinese journalists have gone missing and critics were detained.[163] According to Xinhua, a state-run press agency, the media should focus on "conveying the stirring achievements from the front lines of epidemic prevention" and "showing the Chinese people's unity and spirit of pulling together in difficult times."[164]

Regarding China's public health strategies, the scale of the shutdown and restrictions is unprecedented. On Jan.23, China issued a lockdown on Wuhan, the epicenter of the outbreak, including the suspension of the city's public transport and all outbound flights and trains.[165] Chinese officials justified the necessity of its measures to "effectively cut off the transmission of the virus", and "ensure the safety and health of the people."[166] The order was announced just hours before it was to take effect, without detailed contingency plans and human rights safeguard. The ban on buses, subways and ferries within the city was later extended to private cars,[167] limiting freedom of movement to its most strict forms.

The health code, or QR code, is a major surveillance tool adopted by Chinese officials.

[161] Ibid.
[162] Raymond Zhong, "China Clamps Down on Coronavirus Coverage as Cases Surge," *The New York Times,* February 5, 2020.
[163] Lily Kuo, "'They're chasing me': the journalist who wouldn't stay quiet on Covid-19," *The Guardian*, March 1, 2020.
[164] Zhong, "China Clamps Down on Coronavirus Coverage as Cases Surge."
[165] Amy Qin and Vivian Wang, "Wuhan, Center of Coronavirus Outbreak, Is Being Cut Off by Chinese Authorities*," The New York Times,* January 22, 2020.
[166] Ibid.
[167] "Coronavirus: China Enacts Tighter Restrictions in Hubei," *BBC*, February 16, 2020.

First introduced in Hangzhou and later rolled out nationwide, the code was produced by the mobile app Alipay, which is connected with users' national ID, electronic healthcare, social security cards, and financial credits.[168] People are assigned a color code that indicates their health status. A green code entails unrestricted movement in public spaces, a yellow code may be asked to self-isolate for seven days, and a red code means a two-week quarantine.[169] Yunnan Province wants people to have their QR code scanned whenever they enter or exit public places. Nanjing requires anybody who takes a cab to show ID and leave contact information.[170]

The scale of collaboration and information sharing between public and private sectors is striking. The tech companies draw on information about coronavirus cases and government-held data, and the system may send alarms whether the users have come in close contact with people tested positive on plane, train or bus.[171] The system also appears to share information with the police and track people's movement overtime.[172] Instead of filling in health report forms, state media asserted that the use of health codes facilitates registration and checkpoints, so that "no-contact checks can be carried out to reduce virus transmission risks."[173] However, it is unclear how the system works and classifies people as a contagion risk.[174] It is likely that the health code may set "a template for new forms of automated social control" which outlast its original purpose.[175] In times of pandemic, the state is authorized to expand its power for public goods. However, when there is no constraint, draconian measures are likely to blur the boundary

168 "Xinhua Headlines: Seven Things China Has Done Right to Battle Coronavirus," *Xinhua,* March 13, 2020.
169 Paul Mozur, Raymond Zhong and Aaron Krolik, "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags," *The New York Times,* March 1, 2020.
170 Raymond Zhong and Paul Mozur, "To Tame Coronavirus, Mao-Style Social Control Blankets China," *The New York Times,* February 15, 2020.
171 Ibid.
172 Mozur, Zhong and Krolik, "In Coronavirus Fight, China Gives Citizens a Color Code."
173 "Xinhua Headlines: Seven Things China Has Done Right to Battle Coronavirus," *Xinhua,* March 13, 2020.
174 Mozur, Zhong and Krolik, "In Coronavirus Fight, China Gives Citizens a Color Code."
175 Ibid.

between public and private space. As the scale of surveillance systems is escalating, a unified system is likely to change people's behaviors in a gradual and intangible way and create new security norms.

In addition to the high-tech tools, most surveillance tactics have been implemented at the neighborhood level via mass mobilization. The local bodies were assigned more powers in crisis, as community workers monitor residents for COVID-19 symptoms, screening, quarantine, and guard the checkpoints against outsiders.[176] The public health crisis has reinforced the "grid management' system, which divides the country into tiny sections for monitor and control. Myriad neighborhood committees serve as an intermediary for residents and the local authorities, as the frontline epidemic prevention becomes "a supercharged version of a neighborhood watch."[177]

The central government has put enormous pressure on local officials, which may explain why mitigation policies have shifted from over-conservative to radical.[178] In order to keep the number of infected people down, sometimes the local governments have taken enforcement at the extreme level. In times of emergency, the decentralization has led to more arbitrary policies to achieve the ultimate goal. Some tenants were unable to return to their apartment buildings if they travelled out of town. Train stations blocked people from entering cities if they didn't have residence proof. According to a New York Times analysis, residential lockdowns of varying strictness may cover at least 760 million people in China, with checkpoints at building entrances

[176] Amy Qin and Sui-Lee Wee, "In China's War on the Coronavirus, a Community Is Besieged," *The New York Times*, February 28, 2020.
[177] Zhong and Mozur, "Mao-Style Social Control Blankets China."
[178] Ibid.

and limits on going outdoors.[179] The arbitrary and inflexible measures are likely to exacerbate collateral damage and human rights abuses.

China's Narratives: Rebrand the Legitimacy

Most Western countries have adopted the "flatten the curve" strategy, which aims to reach the same infected number within longer periods of time. Yet the objective of Chinese government is to completely halt the spread and eliminate all new cases. Based on this estimate, virus is the enemy, state of emergency is equivalent to war, and numbers of confirmed cases becomes the only measurement for success. However, military strategies and concepts in public health emergencies can be dangerous and have far-reaching consequences. It stresses the necessity of expanding state power yet downplay the limits of power and human rights safeguard. To regain legitimacy, the Chinese government has emphasized victory and progress to justify its initial missteps, draconian measures and unnecessary sacrifices.

State media in China often use military slogans to emphasize the severity of the situation and maintain legitimacy for its emergency power. On January 26, Xinhua wrote that China has "fortified a nationwide defense," prioritized "putting people's lives first," and will "win antivirus battle at all cost."[180] President Xi Jinping stressed that people of Hubei and Wuhan are "heroic people who have never been crushed by any difficulty and danger in history." [181] During his inspection in Wuhan, President Xi "vowed to fight for a victory in the war" against the COVID-19, and take epidemic prevention and control as "a task of paramount importance."[182] When

[179] Ibid.
[180] "Commentary: China Firm to Win Anti-virus Battle at All Cost," *Xinhua*, January 26, 2020.
[181] "Xi Focus: Xi Vows to Win People's War Against Novel Coronavirus," *Xinhua*, February 11, 2020.
[182] "Update: Xi in Wuhan Vows Victory over Coronavirus, "*Xinhua*, March 10, 2020.

ordinary citizens are rebranded as heroes, they are expected to take on more duties in times of crisis, and willing to accept the excessive restrictions of their fundamental rights and freedom.

As the rate of infection was slowing down, the Chinese government announced on March 10 that China had succeeded in stabilizing the situation and "turning the tide."[183] The strict measures were instrumental in halting the spread of COVID-19 in China. The number of infected cases becomes the primary standard to measure success. By emphasizing the progress, China strived to rewrite the narratives.

China highlighted the effectiveness of its prevention and mitigation measures. Xinhua listed seven things that China has done right to battle the virus, such as full response, Wuhan lockdown, and "selfless sacrifice" of Chinese people to maintain stability and public health.[184] In particular, science and technology are the "most powerful weapon" in the battle against diseases, "making life easier and safer."[185] When Wuhan reported zero increase in both confirmed and suspected cases, it was due to the "strict measures, mass mobilization and dedication of millions of Wuhan residents."[186]

Through its emergency response, China has strived to demonstrate the superiority of Chinese model.[187] Xi announced plans to publish a book in six languages that reports on the emergency mobilization, the progress of the epidemic prevention, and the significant strength of socialist system with Chinese characteristics.[188] China's UN Envoy Zhang Jun described

[183] "Xinhua Headlines-Xi Focus: "Turning the tide" - Xi leads anti-virus war toward victory," *Xinhua*, March 10, 2020.
[184] "Xinhua Headlines: Seven things China has done right to battle coronavirus," *Xinhua*, March 13, 2020.
[185] Ibid.
[186] Yao Yuan and Cheng Lu, "Xinhua Headlines: No New Coronavirus Cases in Wuhan Sends Encouragement to World," *Xinhua*, March 19, 2020.
[187] Javier C. Hernández, "China Spins Coronavirus Crisis, Hailing Itself as a Global Leader," *The New York Times, February 28, 2020.*
[188] http://www.xinhuanet.com/politics/2020-02/26/c_1125627516.htm

prevention and control measures in China as the "most comprehensive, strict, and thorough," and that demonstrates the "power of a united Chinese nation and the strength of China's system."[189]

Security narratives were used to defend unnecessary sacrifice and painful costs. In a city where thousands of lives are lost, and millions of people are struggling in a strict shutdown, it is hardly a victory. Yet in times of "war," extreme measures are allowed, collateral damage is unavoidable, and individual sacrifices are taken for granted. Security and order are justified to outweigh individual interests and freedom.

As the coronavirus outbreak turned out to be of international concern, China has taken advantage of the alarming levels of its spread and severity, as well as slow response of governments around the world. The development of the pandemic helped China claim that they are not the cause of the problem.[190] The state-owned media Global Times said that the prevention and control measures in many countries are insufficient, as they underestimate how contagious this virus can be.[191] The United States has been slow in responding to the outbreak, and that the public health crisis reflects the flaws in the U.S. governance system.[192]

While the COVID-19 began to spread across the globe, China began to present itself as a global leader in pandemic response. International experts said that Chinese government's "strict, top-down response" has stopped the outbreak more successfully compared to many other countries.[193] Xinhua tweeted a poll, asking which part of China's fight against the epidemic was most impressive. The choices included "spirit of self-sacrifice," "solidarity among Chinese," and

[189] "Envoy underscores China's progress in COVID-19 fight, efforts to meet development targets," *Xinhua*, March 4, 2020.
[190] Vivian Wang, "China's Coronavirus Battle is Waning. Its Propaganda Fight Is Not," *The New York Times*, April 8, 2020.
[191] "Some Countries Slow to Respond to Virus," *Global Times*, February 23, 2020.
[192] "US Political System Stymies Effective Virus Response," *Global Times*, February 26, 2020.
[193] Wang, "China's Coronavirus Battle is Waning. Its Propaganda Fight Is Not."

"use of modern technology."[194] The Chinese officials have been encouraging other countries to adopt strict measures, as China provided valuable lessons and experience in this pandemic fight.[195]

In response to the harsh critiques over its mishandling, China has been trying to shift the focus abroad and sending humanitarian assistance.[196] When European Union struggled to organize effective action, and the U.S. would halt funding to the World Health Organization,[197] China filled in the vacuum as a responsible leader and reliable partner. To save its damaged international image, China also exported or donated medical equipment, masks, and test kits to many countries, such as Pakistan, Serbia, Poland and Greece.[198] China's Red Cross sent a team of volunteer experts to Iran,[199] and Chinese intensive-care doctors arrived in Italy to help mitigate the crisis.[200] The effectiveness of such efforts overseas is unclear, yet for Chinese audiences, such narratives can seem compelling.

The Normalization of Extremes and Human Rights Implications

In an interview, Dr. Li said that "a healthy society should have more than one voice" before his death from COVID-19.[201] However, China's emergence response points to a different

194 Hernández, "China Spins Coronavirus Crisis, Hailing Itself as a Global Leader."
195 "Some Countries Slow to Respond to Virus," *Global Times*, February 23, 2020.
196 Hernández, "China Spins Coronavirus Crisis, Hailing Itself as a Global Leader."
197 Andrew Restuccia, "U.S. to Cut Funding to World Health Organization Over Coronavirus Response," *The Wall Street Journal*, April 14, 2020.
198 Steven Lee Myers, "China Pushes Back as Coronavirus Crisis Damages Its Image," *The New York Times*, March 6, 2020.
199 Ibid.
200 Eric Sylvers and Bojan Pancevski, "Chinese Doctors and Supplies Arrive in Italy," *The Wall Street Journal*, March 18, 2020.
201 Yew Lun Tian, "In 'People's War' on coronavirus, Chinese propaganda faces pushback," *Reuters*, March 13, 2020.

direction. The combination of surveillance technology and emergency power can significantly increase state capacity, challenging conventional human rights norms.

In order to mitigate the risk of infectious spread, law sets constraints for the exercise of coercive power over citizens and businesses.[202] While the application of emergency powers requires a specific time period, the scale and seriousness of the COVID-19 outbreak is testing the limits of state power. A successful vaccine is at least 12 to 18 months away, and natural immunity takes at least two years without overwhelming hospitals. The end point of this pandemic is unlikely to follow an absolute timeline but subjected to the development of science.[203] According to a U.S. federal government plan, the pandemic will last 18 months or longer and could include multiple waves, resulting in shortages of products and resources.[204]

The difficulty to set time limits for the state of emergency can pose greater challenges for human rights protections. As the Chinese government strived to justify its strict measures in crisis, it is likely that the extremes will become the new norm. Although lockdown was lifted in Wuhan, only people with "green code" on the smartphone app are allowed to leave the city. The health code or QR code for scanning is required before residents will be able to use public transport.[205] The electronic surveillance and neighborhood management have continued to regulate residents' movement, despite the expectations that business and daily lives are starting to get back to normal.[206]

[202] "Advancing the Right to Health," 41.
[203] James Gallagher, "Coronavirus: When Will the Outbreak End and Life Get Back to Normal?" *BBC*, March 23, 2020.
[204] Peter Baker and Eileen Sullivan, "U.S. Virus Plan Anticipates 18-Month Pandemic and Widespread Shortages," *New York Times*, March 17, 2020.
[205] "Coronavirus: People of Wuhan Allowed to Leave After Lockdown," *BBC*, April 8, 2020.
[206] Raymond Zhong and Vivian Wang, "China Ends Wuhan Lockdown, but Normal Life Is a Distant Dream," *The New York Times*, April 7, 2020.

If modern society has to coexist with the virus in the long-term, it is likely to tolerate a stronger state, the arbitrary and unchecked surveillance, and unclear boundaries between public and private sphere. Unconstrained surveillance interferes with the right to privacy, freedom of expression, and the right to equality. As the right to privacy is a qualified right, its interpretation is dependent on what constitutes public interest, and what remains a private matter. The UDHR pronounced that "no one shall be subjected to arbitrary interference in his privacy, home or correspondence." Any permissible limitations to the right to privacy and freedom of expression must be provided by the law and conform to the principle of proportionality. The restrictive measures must be "the least intrusive instrument amongst those which might achieve the desired result," and "proportionate to the interest to be protected."[207]

The nuances of restrictive measures make a huge difference for the poor, the vulnerable and marginalized groups. Yet in times of chaos and uncertainty, governments tend to prioritize public interest without considering delicate balancing. Vaguely defined legal powers are likely to defend surveillance and disregard the principle of proportionality. In its coronavirus response, China invested enormous resources to COVID-19, yet the progress was achieved with enormous costs.

Xinhua said that a notable advantage of China's socialist system is to "concentrate resources to solve major problems,"[208] but the discussion on balancing tactics is lacking. The narrative of Chinese government obscures the distinctions between effective and draconian measures. In many instances, China's expansion of surveillance is disproportionate to the stated aim and infringes on the right to privacy. Rather, the sacrifice and trade-offs are rebranded as

[207] La Rue, 2013.
[208] "Xinhua Headlines: China's coronavirus battle offers valuable experience for future fights against epidemics," *Xinhua*, February 13, 2020.

necessary to pursue public health. The abusive use of surveillance blurs the boundaries between public goods and private interests yet reinforces the rigid dichotomy between security and liberty. It implies that security is unlikely to be sustained if a state respects freedom during emergencies. The reinforcement of state power may lead to a new security norm, which assumes that individual rights should be secondary to collective interests. As China has tried to export its model of handling the crisis, it challenges the conventional norms of public health and human rights.

In times of pandemic, China's surveillance has now touched on every aspect of private life. From taking a bus, eating out at a restaurant, to entering the apartment complex and office buildings, people would leave traces whenever they go. The QR code provides comprehensive documentary evidence of everyday activities, imposes certain categories, and shapes the distinctions of acceptable behaviors.[209] A public health crisis has accelerated collaboration between public and private sectors, which will likely lead to the establishment of a unified social credit system. The information collected for public health may be reused and exploited for other purposes. When exception becomes the rule, and emergency turns out to be ordinary, surveillance serves as a governance tool to maintain social order and create new norms.

[209] Lyon, 7.

Chapter 4: Huawei's Safe City: The Export of Technology and Narratives

In its 2018 annual report, Freedom House referred to China as the worst abuser of internet freedom.[210] Yet China's ambition goes beyond its domestic setting. Beijing has taken major steps to establish its standards and practices around the world. Huawei has become a dominant supplier of surveillance technologies, including facial recognition systems, big data platforms, and predictive policing algorithms.[211]

This chapter will examine the Huawei "Safe City" projects, the export of surveillance systems, and its human rights implications. As a major driver of surveillance worldwide,[212] China provides a cost-effective governance model that appeals to a variety of countries. With leading tech capabilities, Chinese companies have exported various surveillance tools, such as cameras, cables, software, and monitors. Currently there are no constraints or oversight on the global sale and transfer of surveillance technology, nor adequate safeguards against abuses of state power. Especially for countries with poor human rights records, the use of surveillance will likely exacerbate existing violations. As the surveillance technology proliferates, this chapter will look into its broader consequences in the international system, and what new norms and standards may emerge over the next ten years.

[210] "Freedom on the Net 2018.
[211] Ibid.
[212] Steven Feldstein, "The Global Expansion of AI Surveillance" (Carnegie Endowment for International Peace, September 2019).

China's Global Ambition

Through its Belt and Road Initiative (BRI), China has exerted growing economic and political influence across the globe. BRI plans to build a trade and infrastructure network connecting Asia with Europe, Africa, and beyond.[213] To improve regional cooperation, China has signed BRI cooperation documents with 137 countries and 30 international organizations as of November, 2019.[214] The focus has shifted from railways, ports and power plants to information and communications technologies. The BRI white paper calls for the Digital Silk Road, including the smart cities, data centers, the Internet of Things, and the construction of cable networks and satellites.[215]

Backed by government support, Chinese tech companies are expanding overseas, offering competitive price and quality services. Beijing has provided loans for governments that previously could not afford the telecommunications projects or surveillance system, especially in countries like Kenya, Laos, Uganda, and Uzbekistan.[216] Mostly driven by profits, the private enterprises also fit the bigger picture of China's strategic goals. They export next generation technologies, such as telecom infrastructure, AI surveillance, and training for local government officials.[217] For instance, Chinese AI firm CloudWalk has signed a deal with the government of Zimbabwe to collect biometric data and establish facial recognition software.[218]

[213] Li Xia, "Factbox: Key Takeaways on Belt and Road Initiative Development," *Xinhua*, April 2, 2019.
[214] "China Signs 197 B&R Cooperation Documents With 137 Countries, 30 International Organizations," *Xinhua*, November 15, 2019.
[215] "Vision and Actions on Jointly Building Silk Road Economic Belt and 21st Century Maritime Silk Road" issued by the National Development and Reform Commission, the Ministry of Foreign Affairs and the Ministry of Commerce of the People's Republic of China, March 2015.
[216] Feldstein, "The Global Expansion of AI Surveillance."
[217] Freedom on the Net 2018.
[218] Shan Jie, "China Exports Facial ID Technology to Zimbabwe," *Global Times*, April 12, 2018. https://www.globaltimes.cn/content/1097747.shtml

According to a report from Carnegie Endowment for International Peace, 75 out of 176 countries are actively using AI surveillance, including smart city or safe city platforms, facial recognition systems, and predictive policing.[219] Chinese companies including Huawei, Hikvision, Dahua, and ZTE supply AI surveillance technology in 63 countries, 36 of which have signed onto BRI.[220] The Freedom House report also identified 18 out of 65 countries that accessed AI surveillance developed by Chinese companies.[221]

The rise of Huawei paralleled China's economic expansion. With its cost-effective advantage and technical capacities, Huawei is projecting global influence. The company controlled 29% of the global telecommunications equipment market in 2018, followed by Nokia, Ericsson, and Cisco.[222] Huawei said that it has signed more than 30 5G commercial contracts with global carriers, and has shipped more than 40,000 5G sites across the world.[223] Although Huawei claims that it has no connections to the Chinese government and military, it has participated in numerous government infrastructure projects and received R&D and financial support from policy banks, such as the China Development Bank.[224]

Huawei launched the "Safe City" solutions, aiming to revolutionize the public safety industry.[225] According to the company's 2019 annual report, Huawei has provided digital services for government customers in more than 100 countries and regions, such as Spain, Germany, Kuwait, Russia, Brazil, Peru, India and others.[226] It has helped more than 200 cities to

219 Feldstein, "The Global Expansion of AI Surveillance."
220 Ibid.
221 Freedom on the Net 2018.
222 Stefan Pongratz, "Key Takeaways - Worldwide Telecom Equipment Market 2018" (Dell'Oro Group, March 4, 2019).
223 Huawei Investment & Holding Co. Ltd. 2018 Annual Report.
224 Segal, *The Hacked World Order*, 165.
225 "Safe City White Paper: A Revolution Driven by New ICT" (October 2016). https://e.huawei.com/us/material/industry/safecity/255196f60b7c4d0aafc6310196253966
226 Huawei Investment & Holding Co. Ltd. 2019 Annual Report.

develop surveillance capabilities, cloud data centers, traffic-monitoring systems, and emergency communications.[227]

In response to security threats, such as terrorist attacks, natural disasters and crimes, "Safe City" offers an integrated communications platform to collect and analyze security-related information.[228] The technologies include video surveillance, visualized control and command, the Internet of Things, intelligence sharing and network analysis. This initiative intends to improve the efficiency of detection and emergency response, and develop the capabilities of social monitoring, predictive policing, and early warning. The "Safe City" is also incorporated into the categories of smart cities or public safety, all of which design a future based on big data, AI surveillance and cloud computing. As Huawei promotes on its website, "the good guys have to embrace the digital economy and form a network to fight against the network of bad guys."[229] The company holds that digital transformations will provide enormous benefits to protect public spaces and minimize any disruptions to normalcy.[230]

According to Huawei's promotion materials, the benefits of "Safe City" range from increased security, reduced crime rate, to better emergency response and a thriving economy.[231] Kyrgyzstan signs deals with Huawei to install cameras in airports or on streets to develop traffic-monitoring systems.[232] Uganda police confirmed that they are using Huawei's mass surveillance system to combat crime and boost security.[233] In Belgrade, the Serbian capital, the local

[227] Huawei case studies, https://e.huawei.com/en/case-studies?industry=public-safety
[228] "The Road to Collaborative Public Safety" (Huawei Technologies C., Ltd. 2016). https://e.huawei.com/us/material/industry/safecity/1fa708540cd944bda79a4dcf7bcacd73
[229] Ibid.
[230] Ibid.
[231] Huawei Annual Reports from 2015 to 2018.
[232] http://www.siluxgc.com/jejsst/kgNews/20180112/11487.html
[233] Madhumita Murgia and Tom Wilson, "Uganda Confirms Use of Huawei Facial Recognition Cameras," *Financial Times,* August 20, 2019, https://www.ft.com/content/e20580de-c35f-11e9-a8e9-296ca66511c9

government claims that Huawei's surveillance system helps reduce crime, as hundreds of cameras are able to identify and monitor individuals.[234]

Human Rights Concerns

The Center for Strategic and International Studies concludes the common characteristics of Huawei's markets as non-liberal, Asian or African, and middle income.[235] It is also observed that countries with authoritarian systems and low levels of political rights are investing heavily in AI surveillance techniques, such as advanced analytic systems, facial recognition cameras and sophisticated monitoring capabilities.[236] The East Asia and Pacific, the Middle East and North Africa have demonstrated robust investments, as well as South and Central Asia and Americas. [237] For states that prefer government control of information, China's model of governance appears attractive, as surveillance systems are exported to Ecuador, Venezuela, Bolivia and Angola.[238]

Surveillance technology has been spreading at a faster speed in all forms of governments, while liberal democracies have been the major users.[239] However, the scale and applications of surveillance technology are more likely to be scrutinized and restrained in democratic societies. For countries with poor human rights records, the governments may exploit the technology for mass surveillance and repressive policies.[240] There is limited external mechanism to safeguard human rights and suspend the global export of surveillance technology.

[234]"Chinese Facial Recognition Tech Installed in Nations Vulnerable to Abuse," *CBS News*, October 16, 2019.
[235] Jonathan E. Hillman & Maesea McCalpin, "Watching Huawei's "Safe Cities" (Center for Strategic and International Studies, November 2019),
[236] Feldstein, "The Global Expansion of AI Surveillance."
[237] Ibid.
[238] 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.
[239] Feldstein, "The Global Expansion of AI Surveillance."
[240] Ibid.

The surveillance industry largely relies on self-regulation. The tech companies have proposed ethical guidelines and principles when few regulations and oversight have been established. For instance, Microsoft published six principles to guide its facial recognition work, including fairness, transparency, accountability, non-discrimination, notice and consent, and lawful surveillance.[241] Google laid out its principles for artificial intelligence, asserting that the AI objectives should be socially beneficial, avoid creating or reinforcing unfair bias, incorporate privacy design principles, and be accountable to people.[242] In 2014, the UK government and Tech UK produced a guideline for tech companies when exporting cybersecurity capabilities. By developing due diligence processes and monitoring practices, tech companies can reduce the likelihood that the end user of cyber services may perpetuate human rights abuses.[243] All companies have the responsibility to respect human rights, seek to "identify, prevent and mitigate negative human rights impacts directly linked to its operations, products or services."[244]

Nonetheless, Huawei's ambiguity on privacy safeguard, data storage and accountability reflect great divergence to its Western counterparts. In the 2018 sustainability report, Huawei discussed its economic and social responsibility by focusing on digital inclusion, and security and trustworthiness.[245] Huawei also published an AI Security White Paper, yet with no references to human rights protections and procedures.[246] While Western companies have

[241] "Six Principles for Developing and Deploying Facial Recognition Technology," Microsoft Corporation, December 2018. https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2018/12/MSFT-Principles-on-Facial-Recognition.pdf
[242] "Artificial Intelligence at Google: Our Principles." https://ai.google/principles/
[243] "Assessing Cybersecurity Export Risks" (Tech UK). https://www.techuk.org/images/CGP_Docs/Assessing_Cyber_Security_Export_Risks_website_FINAL_3.pdf
[244] Ibid.
[245] Huawei Investment & Holding Co., Ltd. 2018 Sustainability Report. https://www-file.huawei.com/-/media/corporate/pdf/sustainability/2018/2018-csr-report-en.pdf?la=en-us
[246] "AI Security White Paper" (Huawei). https://www-file.huawei.com/-/media/corporate/pdf/trust-center/ai-security-whitepaper.pdf

concerns over freedom and human rights, Chinese firms operate with less scrutiny and regard for corporate social responsibility.[247]

Huawei comes up with a risk-free solution for modern cities. With comprehensive video surveillance, facial recognition, and big data analytics, the local government and police department will be able to respond and predict, thus preventing any threats and disruptions. Digital transformations are essential for managing risks and maintaining public safety. Yet according to a CSIS report, the benefits of Huawei's safe city solutions are questionable, difficult to verify and even appear exaggerated in some cases.[248] There is a gap between Huawei's promotional materials and reality.[249] For instance, Huawei claims that from 2014 to 2015, the project in Kenya "helped decrease the crime rate by 46% in the areas within the project's scope."[250] However, according to Kenya's National Police Service reports, there was a smaller decrease in crime rates in 2015 in Nairobi, one of the cities where "Safe City" equipment was installed. In 2017, Nairobi also saw an increase in reported crimes to higher than pre-installation levels.[251]

States promote the narrative of public safety, yet there is limited discussion to strike the balance between security and liberty, what are the costs of smart cities projects, and to what extent such trade-offs are lawful, legitimate and necessary. The use of facial recognition and other AI software has raised criticisms and concerns among political opponents and rights activists, who are vulnerable to targeted surveillance.[252] It is reported that Huawei technicians

[247] Ibid.
[248] Hillman and McCalpin, "Watching Huawei's "Safe Cities."
[249] Ibid.
[250] Zhang Aixue, "Protecting Enchanted Kenya," Huawei, March 14, 2016. https://e.huawei.com/en/case-studies/global/2016/201603141435
[251] Hillman and McCalpin, "Watching Huawei's "Safe Cities."
[252] Murgia and Wilson, "Uganda Confirms Use of Huawei Facial Recognition Cameras."

helped African governments spy on their political opponents, including intercepting their encrypted communications and social media, and using cell data to track their location.[253] In countries with weak human rights records, the unchecked sale and export of surveillance capability will likely exacerbate existing violations and deter street protests.

The Politics of Surveillance

Huawei is a private company but maintains close ties with the Chinese government. While Huawei helps promote the security norms through the export of surveillance technology, China plays an essential role by deepening economic and political connections with other states. With its emphasis on sovereignty and stability, China develops an alternative security norm which is likely to shape liberal human rights values.

China tries to advocate a state-centric approach of global governance in cyberspace. Compared to the U.S. private-sector-led model, China calls for a multilateral approach with the United Nations taking a leading role in Internet regulation. As China's Ministry of Foreign Affairs asserts, countries are all equal members of the international community entitled to equal participation in developing cyberspace rules through international governance mechanisms and platforms.[254] This approach would prioritize the interests of governments over companies and civil groups, allowing China to mobilize the votes of developing countries.[255]

[253] Joe Parkinson, Nicholas Bariyo and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," *The Wall Street Journal*, August 5, 2019.
[254] "International Strategy of Cooperation on Cyberspace" (Ministry of Foreign Affairs of the People's Republic of China, March 1, 2017). https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml
[255] Segal, "When China Rules the Web."

The Chinese government identified several problems in cyberspace, such as "unbalanced development, inadequate rules and inequitable order."[256] Seeking to challenge the status quo, China not only exerts influence through international political institutions, but also relies on growing economic power. By forming close economic ties with many countries along the Belt and Road, China has seen some successes to mobilize support on the global stage.

For instance, a group of 37 countries submitted a letter to the UN Human Rights Council in defense of China's Xinjiang policies, days after a group of 22 nations calling on China to end its mass surveillance and arbitrary detention. The signatories justified China's efforts in the letter, maintaining that "vocational educational camps and training centers" are a series of "counterterrorism and deradicalization measures."[257] The countries criticizing China are dominated by Western states, mostly in Europe, while those defending China are largely African and Middle Eastern nations, such as Egypt and Saudi Arabia.[258] The Chinese government has also organized different forums to impart norms. In 2019, China held the World Internet Conference in Wuzhen, covering topics such as artificial intelligence, big data, and 5G networks. The senior officials called for increasing efforts to "protect the security and order of cyberspace."[259]

Citing national security concerns, the U.S. has initiated a global campaign against Huawei yet received mixed responses from its allies.[260] Japan, Australia, and New Zealand are following the U.S.'s lead. Germany refuses to exclude Huawei,[261] while the United Kingdom

[256] "International Strategy of Cooperation on Cyberspace," Ministry of Foreign Affairs of China.
[257] Catherine Putz, "Which Countries Are for or Against China's Xinjiang Policies?" *The Diplomat,* July 15, 2019.
[258] Ibid.
[259] "6th World Internet Conference Opens in China's Zhejiang," *Xinhua*, October 20, 2019.
[260] Nikos Chrysoloras and Richard Bravo, "Huawei Deals for Tech Will Have Consequences, U.S. Warns EU," *Bloomberg*, February 7, 2019.
[261] Joanna Kakissis, "Despite U.S. Pressure, Germany Refuses to Exclude Huawei's 5G Technology," *NPR*, March 20, 2019.

allows access to non-core 5G networks.[262] In May 2019, the U.S. escalated its battle by adding Huawei to an export blacklist. The U.S. companies would be barred from supplying technology to Huawei without a license.[263] Huawei's smartphones will no longer have access to some Google mobile services, including the operating system, Android.[264] In October 2019, the Trump administration added 28 Chinese organizations to a United States blacklist over human rights concerns, blocking them from buying American products.[265] The lists include Hikvision and Dahua Technology, two of the world's largest manufacturers of video surveillance products, as well as companies that specialize in artificial intelligence, voice recognition and data.[266]

When there is no agreed upon international regulations and framework to regulate the global sale and transfer of surveillance technologies, China's leading role in telecommunications industry will likely exacerbate human rights violations and undermine democratic values. For China, exporting surveillance technology is a way to reinforce the sovereign and controlled vision of the Internet, and reshape the norms and principles of Internet governance.[267] China is likely to continue to export its policy of authoritarian cyber controls, giving countries the capability to regulate and censor their own Internet.[268]

[262] Michael Holden, Jack Stubbs, "Britain to Allow Huawei Restricted Access to 5G Network," *Reuters*, April 24, 2019.
[263] Kate O'Keeffe, John D. McKinnon and Dan Strumpf, "Trump Steps Up Assault on China's Huawei," *The Wall Street Journal*, May 15, 2019.
[264] Julia Carrie Wong, "The Drama Surrounding Google and Huawei's New Phone – Explained," *The Guardian*, August 31, 2019.
[265] Ana Swanson and Paul Mozur, "U.S. Blacklists 28 Chinese Entities Over Abuses in Xinjiang*," The New York Times*, October 7, 2019.
[266] Ibid.
[267] Justin Sherman, Robert Morgus, "Authoritarians Are Exporting Surveillance Tech, And With it Their Vision for the Internet," Council on Foreign Relations, December 5, 2018.
[268] Stewart M. Patrick, Ashley Feng, "Belt and Router: China Aims for Tighter Internet Controls with Digital Silk Road," Council on Foreign Relations, July 2, 2018.

Conclusion

A defining feature of modernity is the emergence of nation-states and the growing recognition of individual rights. The Declaration of Independence in 1776 held "these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights." However, truth, ideas or norms were not necessarily self-evident, but went through a contested process as a range of actors fought for legitimacy. State practices influence norms, and norms provide justifications for state behaviors. To secure life, liberty and security, it is crucial to engage with diverse stakeholders and reassert the appeal of human rights norms and practices.

As the government increases its power and capacity, it often leads to "a contraction of traditional individual rights, freedoms, and liberties."[269] To some extent, human rights discourse and movements have aspired to limit the excessive intervention from states. Since World War II, the international legal regime has been established in the spirit of restoration rather than revolution.[270] The 1948 UDHR reflected some of the attempts to balance a diverse range of interests, protecting human rights for individuals while acknowledging the significance of community and sovereignty. In a contemporary context, states are not the only guarantor of rights, but subjected to both domestic and supranational pressures. On the international level, bilateral and multilateral relations, international organizations, judicial institutions, and civil societies all participate in a dynamic process of redefining human rights.

This thesis examines the role of surveillance technology in expanding the power of states, and how the changing dynamics of state-citizen relationship may affect human rights norms and

[269] Oren Gross and Fionnuala Ní Aoláin, *Law in Times of Crisis* (Cambridge University Press, 2006): 9.
[270] Samuel Moyn, "On the Genealogy of Morals," *The Nation*, April 16, 2007.

practices. As a governance tool, China's surveillance system reflects a growing obsession to certainty and a decreasing tolerance of ambiguity. It cultivates an assumption that the more information a government gathers, the better predictive analysis they can create. By identifying threats among its citizens, the surveillance system ultimately aims for a risk-free society. As knowledge becomes power, modern policing tends to collect infinite data, generate predictions, and take preventive measures. Nonetheless, this vision of security is often achieved at the expense of individual rights. To maintain the legitimacy of its polity, China has acted as a norm entrepreneur and developed a security narrative. The benefits of surveillance technology are often exaggerated yet the costs are downplayed. In a gradual and intangible way, the intrusive use of surveillance is capable to shape and control the behaviors of citizens.

The universal values of liberty and equality are not timeless but embedded in specific temporal and geographical contexts. Even similar texts can connote different meanings and serve particular political agenda. In the aftermath of major disasters and crisis, the echoes of liberty and universalism may seem less appealing compared to security and survival. In response to perceived threats, the fear and frustration of uncertainty may provoke the government to take some draconian measures. As a result, states are likely to encourage the false dichotomy between security and liberty, without assessing the effectiveness, necessity and proportionality of certain policies. At the same time, human rights progress may encounter backlash and reversal, especially the right to privacy and fundamental freedoms.

Although surveillance technology poses a new set of challenges, the security norms have been a recurrent narrative. Kathryn Sikkink comes up with the term "counter-norm," which

refers to the anti-terrorism discourse to justify the use of torture.[271] The U.S. officials attempted to reinterpret the norm in the context of the "war on terror," rejecting previously accepted norms on the prohibition of torture.[272] Combating terrorism was used as a pretext for human rights violations, such as the practice of torture during interrogation and detention without trial.[273] "Enhanced interrogation techniques" were interpreted as permissible and necessary counterterrorism measures due to the state of emergency.[274]

Similarly, China has achieved some successes in promoting the security norms and justifying the use of surveillance technology. The Chinese officials push for an arbitrary notion of security and a blurred boundary between public and private spheres. Given the effectiveness of contact tracing, the unprecedented reach of "health code" is permitted during a pandemic. While the Chinese government primarily uses surveillance system for the purpose of public security, the state of emergency is likely to accelerate the transition from "Skynet" to the "social credit system," a unified and comprehensive surveillance system combining both public and private sectors.

Through the export of surveillance technology, political alliances, and socialization in international organizations, China also aims to export the security norm and obtain a wider acceptance for its governance model. In a contested process for legitimacy, China's alternative narrative has emerged to challenge the liberal and universal ideologies. Huawei's "Safe City" project and the norms of security have appealed to some illiberal states with poor human rights

[271] Kathryn Sikkink, "The United States and Torture: Does the Spiral Model Work?" in *The Persistent Power of Human Rights: From Commitment to Compliance*, ed. by Thomas Risse, Stephen C. Ropp, and Kathryn Sikkink (Cambridge: Cambridge University Press, 2013): 145-146.
[272] Ibid.
[273] Anna Di Lellio and Emanuele Castano, "The danger of 'new norms' and the continuing relevance of IHL in the post-9/11 era," *International Review of the Red Cross* 17, no.900 (December 2015): 3.
[274] Ibid.

records. A system designed for public security can be misused to target activists, journalists, political dissidents, and other vulnerable groups. The conflicts of norms are likely to increase the fragmentation in cyberspace, as well as the difficulty to reach international consensus on surveillance regulation.

The questions then arise as to, will this security norm be adequate to justify the expansion of surveillance and state power? To what extent the restrictions of individual rights can be considered as lawful and legitimate intervention? What solutions could counter such security narratives, and how can international human rights framework respond to new risks and challenges?

Regarding the prohibition against torture, Sikkink analyzes the spiral model to understand the power of human rights and U.S. response to pressure.[275] She suggests that the government must have "some form of vulnerability to internal and external pressures" to allows for the possibility of some behavioral change.[276] Due to their wealth and power, the hegemons are less materially vulnerable and often respond to accusations and pressures with repression and denial. Yet the democratic nature of the U.S. political system indicates that the opposition from media, NGOs, and judicial branches could have an impact on government behaviors.[277]

Therefore, to address the potential abuses of surveillance technology, substantial pressures from Chinese citizens and international community may also create some conditions for change. First, democratic countries should work together and push for consensus on the export control of surveillance technology and human rights protection. The United States, the European Union members, Australia, Canada and other like-minded countries may find it

[275] Sikkink, "The United States and Torture."
[276] Ibid.
[277] Ibid.

reasonable to reject the enormous trade-offs of security norms and intrusive surveillance systems. For instance, the Wassenaar Arrangement requires which military and "dual-use" goods should be subjected to licensing and has 41 participating states. It also includes several surveillance technologies within its list of controlled items.[278] More efforts could be invested in assessing the implications of new surveillance technology and incorporating the "dual-use" products to the existing regimes of international export control, in particular the sophisticated monitoring tools. Private companies are encouraged to integrate human rights due diligence into their export program and identify the risks associated with the end-users and human rights violations.

Check and balances are essential to restrain the use of surveillance. Governments should enact data privacy legislation and develop comprehensive policies to safeguard human rights, and if possible, impose sanctions on companies complicit in human rights abuses. Judicial institutions, NGOs, media, and other independent oversight should be cautious about public-private collaboration, and demand transparency and accountability of the objectives, procedures, and mechanisms of surveillance systems. Otherwise, an overpowering partnership between public and private sectors may have a chilling effect on civil liberties and fundamental human rights.

International organizations, human rights courts, NGOs and think tanks can also play a significant role in updating international human rights framework. Research and investigations are crucial to evaluate existing mechanisms and their applicability in global surveillance industry. The UN Guiding Principles on Business and Human Rights, the OECD Guidelines for Multinational Enterprises, and OECD Due Diligence Guidance on Responsible Business

[278] "The Global Surveillance Industry" (Privacy International, July 2016).

Conduct can provide basic guidelines to review the capabilities of surveillance technology and their potential for human rights abuses.

Moreover, civil societies should initiate discussions and dialogues regarding the tactics of balancing, the conditions of human rights restrictions, and the validity of government's justifications. Awareness of the risks posed by surveillance and security norms is key to call for surveillance regulations. Human rights lawyers, scholars, and activists can also think in creative and practical ways on how to reassert the appeal of human rights norms, such as stabilizing the regime and protecting democracy. Despite its flaws and limitations, international human rights framework remains one of the most promising approach to constrain the abusive power of surveillance and states.

Bibliography

Abbott, Kenneth W., and Duncan Snidal. “Hard and Soft Law in International Governance.” *International Organization* 54, no. 3 (2000): 421–56.

“Advancing the Right to Health: The Vital Role of Law.” World Health Organization, 2017.

Alston, Philip, and Ryan Goodman. *International Human Rights: The Successor to International Human Rights in Context*. Oxford, United Kingdom: Oxford University Press, 2013.

Amoore, Louise. *The Politics of Possibility: Risk and Security beyond Probability*. Durham, NC: Duke University Press, 2013.

Aolain, Fionnuala Ni. “How Can States Counter Terrorism While Protecting Human Rights.” *Ohio Northern University Law Review* 45 (2019): 389–409.

Babu-Kurra. “How 9/11 Completely Changed Surveillance in U.S.” *Wired*, September 11, 2011. https://www.wired.com/2011/09/911-surveillance/.

“Backgrounder: Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era.” *Xinhua*, March 17, 2018.

Beech, Hannah. “Tracking the Coronavirus: How Crowded Asian Cities Tackled an Epidemic.” *The New York Times*, March 17, 2020.

Bergenfalk, Joel. “AI and Human Rights — An Explorative Analysis of Upcoming Challenges,” 2019.

Buckley, Chris. “Chinese Doctor, Silenced After Warning of Outbreak, Dies from Coronavirus.” *The New York Times*, February 6, 2020.

Buckley, Chris, and Steven Lee Myers. “As New Coronavirus Spread, China’s Old Habits Delayed Fight.” *The New York Times*, February 1, 2020.

Ceyhan, Ayse. “Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics.” *Surveillance & Society* 5, no. 2 (2008).
Chen, Yu-Jie, Ching-Fu Lin, and Han-Wei Liu. “Rule of Trust: The Power and Perils of China’s Social Credit Megaproject.” *Columbia Journal of Asian Law* 32, no. 1 (2018): 1–36.

Chin, Josh. “Twelve Days in Xinjiang: How China’s Surveillance State Overwhelms Daily Life.” *The Wall Street Journal*, December 19, 2017.

"China Passes New National Security Law Extending Control over Internet." *The Guardian*, July 1, 2015.

Cockerell, Isobel. "Inside China's Massive Surveillance Operation." *The Wired*, May 9, 2019. https://www.wired.com/story/inside-chinas-massive-surveillance-operation/.

"Coronavirus: Countries Enforce Mass Closures to Stem Spread." *BBC*, March 13, 2020.

Deibert, Ronald J. "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace." *Millennium: Journal of International Studies* 32, no. 3 (2003): 501–30.

Di Lellio, Anna and Emanuele Castano. "The danger of 'new norms' and the continuing relevance of IHL in the post-9/11 era." *International Review of the Red Cross* 17, no.900 (December 2015): 1-17.

"Enemies of the Internet Report 2012." Reporters Without Borders, March 2012.

Farrell, Henry, and Abraham Newman. "Will the Coronavirus End Globalization as We Know It?" *Foreign Affairs*, March 16, 2020.

Feldstein, Steven. "The Global Expansion of AI Surveillance." Carnegie Endowment for International Peace, September 2019.

Finnemore, Martha. *The Purpose of Intervention: Changing Beliefs about the Use of Force*. Ithaca, NY: Cornell University Press, 2003.

Finnemore, Martha, and Duncan B. Hollis. "Constructing Norms for Global Cybersecurity." *American Journal of International Law* 110, no. 3 (2016): 425–79.

Fisher, Max, and Emma Bubola. "As Coronavirus Deepens Inequality, Inequality Worsens Its Spread." *The New York Times*, March 15, 2020.

"Freedom on the Net 2015: Privatizing Censorship, Eroding Privacy." Freedom House, October 2015.

"Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy." Freedom House, November 2017.

"Freedom on the Net 2018: The Rise of Digital Authoritarianism." Freedom House, October 2018.

"General Comment No.29, States of Emergency (Article 4)." Human Rights Committee, July 24, 2001.
Gross, Oren, and Fionnuala Ní Aoláin. "International Human Rights and Emergencies." In *Law in Times of Crisis*, 247–325. Cambridge University Press, 2009.

Harari, Yuval Noah. “Why Technology Favors Tyranny.” *The Atlantic*, October 2018.

Hernández, Javier C. “China Spins Coronavirus Crisis, Hailing Itself as a Global Leader.” *The New York Times*, February 28, 2020.

Hillman, Jonathan E, and Maesea McCalpin. “Watching Huawei’s ‘Safe Cities.’” Center for Strategic & International Studies, November 2019.

“International Covenant on Civil and Political Rights,” December 16, 1966.

Johnston, Alastair Iain. "Learning versus adaptation: explaining change in Chinese arms control policy in the 1980s and 1990s." *The China Journal* 35 (1996): 27-61.

Keegan, Matthew. “Big Brother Is Watching: Chinese City with 2.6m Cameras Is World’s Most Heavily Surveilled.” *The Guardian*, December 2, 2019.

Kristof, Nicholas. “"I Cannot Remain Silent”.” *The New York Times*, February 15, 2020.

Kuo, Lily. “China Bans 23m from Buying Travel Tickets as Part of ‘Social Credit’ System.” *The Guardian*, March 1, 2019.

La Rue, Frank. “Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue.” United Nations General Assembly, Human Rights Council, April 17, 2013. http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

Lewis, James Andrew. “China’s Information Controls, Global Media Influence, and Cyber Warfare Strategy.” U.S. China Security and Economic Review Commission, May 4, 2017.

Lewis, James Andrew. “Cognitive Effect and State Conflict in Cyberspace.” Center for Strategic & International Studies, September 2018.

Lewis, James Andrew. “Defining Rules of Behavior for Force and Coercion in Cyberspace.” In *Confronting an “Axis of Cyber”? China, Iran, North Korea, Russia in Cyberspace*. Institute for International Political Studies, 2018.

Lewis, James Andrew. “Rethinking Cybersecurity: Strategy, Mass Effect, and States.” Center for Strategic and International Studies, January 2018.

Lucas, Louise, and James Kynge. “Huawei Continues Global Push Despite Setbacks in West.” *Financial Times*, December 16, 2018.
Lyon, David. *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press, 1994.

Michel, Foucault. *Discipline and Punish: The Birth of the Prison*. New York: Vintage Books, 1995.

Mozur, Paul. "China's Internet Controls Will Get Stricter, to Dismay of Foreign Business." *The New York Times*, November 7, 2016.

Mozur, Paul. "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras." *The New York Times*, July 8, 2018.

Mozur, Paul, Raymond Zhong, and Aaron Krolik. "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags." *The New York Times*, March 1, 2020.

Myers, Steven Lee. "China Pushes Back as Coronavirus Crisis Damages Its Image." *The New York Times*, March 6, 2020.

"National Cyber Strategy of the United States of America." The White House, September 2018.
"Overview of China's Cybersecurity Law." KPMG China, February 2017. https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf.

Price-Smith, Andrew. *Contagion and Chaos: Disease, Ecology, and National Security in the Era of Globalization*. Cambridge, MA: MIT Press, 2009.

Purdeková, Andrea. "'Even If I Am Not Here, There Are So Many Eyes': Surveillance and State Reach in Rwanda." *Journal of Modern African Studies* 49, no. 3 (2011): 475–97.

"Report of the WHO-China Joint Mission on Coronavirus Disease 2019 (COVID-19)"." World Health Organization, February 16, 2020.

Rona, Gabor, and Lauren Aarons. "State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace." *Journal of National Security Law & Policy* 8, no. 3 (2016): 503–30.

Ruggie, John Gerard. "What Makes the World Hang Together? Neo-Utilitarianism and The Social Constructivist Challenge." *International Organization* 52, no. 4 (n.d.): 855–85.

"Safe City White Paper: A Revolution Driven by New ICT." Huawei, October 2016. https://e.huawei.com/us/material/industry/safecity/255196f60b7c4d0aafc6310196253966.

Segal, Adam. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York: PublicAffairs, 2016.

Segal, Adam. "When China Rules the Web." *Foreign Affairs*, September/October 2018.
Sender, Omri, and Michael Wood. "A Mystery No Longer? Opinio Juris and Other Theoretical Controversies Associated with Customary International Law." *Israel Law Review* 50, no. 3 (2017): 299–330.

Shah, Sangeeta, and Kevin Boyle. “Thought, Expression, Association, and Assembly.” In *International Human Rights Law*, edited by Daniel Moeckli, Sangeeta Shah, and Sandesh Sivakumaran, 257–79. Oxford: Oxford University Press, 2010.

Shih, Gerry. “In China’s Coronavirus Crisis, a Fleeting Flicker of Freer Speech.” The *Washington Post*, February 6, 2020.

Sikkink, Kathryn. “The United States and Torture: Does the Spiral Model Work?” in *The Persistent Power of Human Rights: From Commitment to Compliance,* ed. by Thomas Risse, Stephen C. Ropp, and Kathryn Sikkink (Cambridge: Cambridge University Press, 2013): 145-163.

Snowden, Frank M. *Epidemics and Society: From the Black Death to the Present.* Yale University Press, 2019.

“Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.” Human Rights Council, July 24, 2019.

“The Johannesburg Principles on National Security, Freedom of Expression and Access to Information.” ARTICLE 19, November 1996. https://www.article19.org/wp-content/uploads/2018/02/joburg-principles.pdf.

“The Right to Development: China’s Philosophy, Practice and Contribution.” The State Council Information Office of the People’s Republic of China, December 2016. http://www.scio.gov.cn/32618/Document/1534069/1534069.htm.

Tian, Yew Lun. “In ‘People’s War’ on Coronavirus, Chinese Propaganda Faces Pushback.” *Reuters*, March 13, 2020.

“Universal Declaration of Human Rights,” December 10, 1948.

Wang, Vivian. “China’s Coronavirus Battle Is Waning. Its Propaganda Fight Is Not.” *The New York Times*, April 8, 2020.

Wendt, Alexander. “Constructing International Politics.” *International Security* 20, no. I (1995): 71–81.

Wong, Chun Han. “Beijing Portrays President Xi Jinping as Hero of Coronavirus Fight.” *The Wall Street Journal*, March 8, 2020.

Wong, Julia Carrie. “The Drama Surrounding Google and Huawei’s New Phone – Explained.” *The Guardian*, August 31, 2019.

Wu, Tim. “Bigger Brother.” *The New York Review of Books*, April 9, 2020.

"Xi Focus: Xi Vows to Win People's War Against Novel Coronavirus." *Xinhua*, February 11, 2020.

Xi, Jinping. "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era." Presented at the The 19th National Congress of the Communist Party of China, October 18, 2017. http://english.qstheory.cn/2018-02/11/c_1122395333.htm.

"Xinhua Headlines: China's Coronavirus Battle Offers Valuable Experience for Future Fights against Epidemics." *Xinhua*, February 13, 2020.

"Xinhua Headlines: Seven Things China Has Done Right to Battle Coronavirus." *Xinhua*, March 13, 2020.

"Xinhua Insight: China Adopts New Law on National Security." *Xinhua*, July 1, 2015.

Zhong, Raymond, and Paul Mozur. "To Tame Coronavirus, Mao-Style Social Control Blankets China." *The New York Times*, February 15, 2020.

Zhong, Raymond, and Vivian Wang. "China Ends Wuhan Lockdown, but Normal Life Is a Distant Dream." *The New York Times*, April 7, 2020.

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.