Faculty of Humanities and Social Sciences

Degree in International Relations

Final thesis

The role of technology in authoritarian regimes:

China's model of digital repression

Author: Lucía Rosell Taboada

Supervisor: Prof. Hutan Hejazi

Madrid, junio de 2023

Index

Abstract

This thesis explores the relationship between technology and authoritarianism, focusing on China's model of digital repression. It investigates the use of technology by the Chinese government to monitor and control its citizens, suppress dissent, and manipulate information and the implications of technological advancements for human rights, democracy, and global governance. Through a meticulous literature review, it examines theoretical frameworks, historical precedents, and case studies of technology-enabled authoritarian regimes. By analyzing primary and secondary sources, the thesis reveals specific technologies used by the Chinese government, such as surveillance systems, facial recognition, and social media platforms. It explores how information manipulation and online control consolidate state power and erode civil liberties. The research deepens understanding of the dynamics between technology and authoritarianism, particularly in China. It critically examines the implications of China's digital repression, addressing challenges and ethical considerations in studying technology within authoritarian regimes. Drawing lessons from China's model, it offers recommendations to safeguard human rights, promote digital freedom, and foster democratic principles. This research contributes to the discourse on technology's impact on authoritarian regimes and its broader societal implications.

Key words: technology, authoritarianism, digital repression, China, surveillance systems, artificial intelligence, human rights

Resumen

Esta tesis explora la relación entre tecnología y autoritarismo, centrándose en el modelo chino de represión digital. Investiga el uso de la tecnología por parte del gobierno chino para vigilar y controlar a sus ciudadanos, reprimir la disidencia y manipular la información, así como las implicaciones de los avances tecnológicos para los derechos humanos, la democracia y la gobernanza mundial. A través de una meticulosa revisión bibliográfica, examina marcos teóricos, precedentes históricos y estudios de casos de regímenes autoritarios facilitados por la tecnología. Mediante el análisis de fuentes primarias y secundarias, la tesis revela tecnologías y herramientas específicas utilizadas por el gobierno chino, como sistemas de vigilancia, tecnología de reconocimiento facial y plataformas de redes sociales. Explora cómo la manipulación de la información y el control en línea consolidan el poder del Estado y erosionan las libertades civiles. La investigación profundiza en la comprensión de la dinámica entre tecnología y autoritarismo, especialmente en China. Examina críticamente las implicaciones de la represión digital en China y aborda los retos y las consideraciones éticas que plantea el estudio de la tecnología en los regímenes autoritarios. Extrayendo lecciones del modelo chino, ofrece recomendaciones para salvaguardar los derechos humanos, promover la libertad digital y fomentar los principios democráticos. Esta investigación contribuye al discurso sobre el impacto de la tecnología en los regímenes autoritarios y sus implicaciones sociales más amplias.

Palabras clave: tecnología, autoritarismo, represión digital, China, sistemas de vigilancia, inteligencia artificial, derechos humanos

I. Introduction

a. Background and motivation

The use of technology for surveillance and control in authoritarian regimes is not a new phenomenon. Governments around the world have been using technology to monitor, censor, and manipulate their citizens for decades, from the printing press in 16th century Europe to radio propaganda in Nazi Germany (Tufekci, 2017). However, the rise of the internet and digital technologies has enabled these regimes to increase their level of control and surveillance, leading to what scholars have termed "digital authoritarianism" (Polyakova & Meserole, 2019). Defined in a Brookings Institution 2019 report as "the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations" (Polyakova & Meserole, 2019), as well as the public opinion (Shahbaz, 2018).

China has become a global leader in the development and implementation of digital authoritarianism. Its "Social Credit System" (SCS) and other forms of digital surveillance have allowed the Chinese Communist Party (CCP) to maintain its grip on power, despite being widely discussed in the media and policy circles (Shambaugh, 2007). The SCS is a government-led initiative that aims to use big data and artificial intelligence to assign a "social credit" score to each citizen based on their behavior, such as their financial transactions, online activity, and social interactions (Cho, 2020). Those with low scores can face a range of penalties, including travel restrictions, reduced access to public services, and social stigma (Mac Síthigh & Siems, 2019).

China's model of digital repression has significant implications for human rights, democracy, and global governance. The use of technology for surveillance and control raises serious concerns about privacy, free expression, and individual liberties, as well as the potential for abuse by those in power (Shambaugh, 2007). The SCS, in particular, has been criticized for its lack of transparency, its potential to discriminate against marginalized groups, and its potential to be used as a tool for political repression (Cho, 2020).

Furthermore, China's export of its model of digital repression to other countries, particularly through its "Belt and Road Initiative," has implications for global governance and the balance of power in the international system (Lew et al., 2021). The Belt and Road Initiative is a massive infrastructure project that seeks to connect China with other countries in Asia, Europe, and Africa through a network of roads, railways, ports, and

other infrastructure (Rogers, 2019). As part of this initiative, China has been exporting its digital technologies and expertise to other countries, particularly those with authoritarian regimes or weak governance structures (Lew et al., 2021). These include Egypt, Saudi Arabia, and Venezuela as Qiang (n.d.) asserts.

Despite the significant attention paid to China's model of digital repression in the media and policy circles, there is a relative lack of academic literature on the topic. This study seeks to fill this gap by providing a detailed and nuanced analysis of the role of technology in China's authoritarian regime and its model of digital repression. By examining the development, implementation, and impacts of China's digital surveillance state, this study aims to contribute to our understanding of the ways in which technology can be used for repression and control in authoritarian regimes, as well as its implications for international relations.

We must also remark that technology for surveillance has not only been used in authoritarian regimes but also in advanced democracies. The use of AI (artificial intelligence) surveillance is rapidly increasing all around the world with a total of "seventy-five countries, representing 43 percent of total countries assessed" deploying AI-powered surveillance in both lawful and unlawful ways according to the Artificial Intelligence Global Surveillance (AIGS) Index (2018)[1]. The group of countries present very different political systems ranging from "closed autocracies to advanced democracies" (AIGS Index, 2018).

b. Research questions and objectives

The primary research question of this thesis is: What is the role of technology in facilitating and reinforcing authoritarianism in China?

To address this research question, the following specific research questions have been formulated:

[1] The AIGS Index offers a comprehensive and factual overview of the current state of global AI surveillance, shedding light on the utilization of this technology by governments worldwide through three questions:

- Which countries have embraced AI surveillance technology?
- What specific types of AI surveillance systems are being implemented by governments?
- Which countries and companies are involved in the supply of such technology?

The index provides extensive details concerning seventy-five countries that have been identified through research as adopters of AI surveillance technology. It categorizes AI surveillance tools into the following subgroups: 1) smart city/safe city, 2) facial recognition systems, and 3) smart policing (Feldstein, 2019).

- What specific technologies are being used by the Chinese government to monitor and control its citizens, and how do these technologies function within the context of China's authoritarian regime?
- How does the Chinese government use technology to manipulate information and suppress dissent, and what are the implications of this for human rights and democracy in China?
- What are the challenges and limitations of studying the role of technology in authoritarian regimes, and how can these challenges be addressed in the context of research on China's model of digital repression?

In order to answer these research questions, this thesis has the following objectives:

To conduct a comprehensive review of the existing literature on the role of technology in authoritarian regimes, including case studies from China and other countries.

To analyze the specific technologies and tools that are being used by the Chinese government to monitor and control its citizens, including surveillance systems, facial recognition technology, and social media platforms.

To examine how the Chinese government uses technology to manipulate information and suppress dissent, including censorship, propaganda, and the manipulation of online discourse.

To assess the implications of China's model of digital repression for human rights and democracy, including the impact on freedom of speech, privacy, and the ability of citizens to hold their government accountable.

To evaluate the challenges and limitations of studying the role of technology in authoritarian regimes, including issues related to data access, censorship, and ethical considerations.

By addressing these research questions and objectives, this thesis aims to contribute to a deeper understanding of the complex relationship between technology and authoritarianism in China and to provide insights into the potential implications of this relationship for human rights and democracy in the country.

c. Methodology and scope

This study adopts a qualitative case study approach to examine the role of technology in China's authoritarian regime and its model of digital repression. In this study, China's digital surveillance state serves as the primary case, with a focus on the development,

implementation, and impacts of its model of digital repression. The methodology will encompass the selection and utilization of primary and secondary sources to address the research questions and achieve the research objectives.

The research on the role of technology in authoritarian regimes, particularly in the Chinese context, relies on primary sources to gather firsthand information and insights.

Secondary sources play a crucial role in providing a comprehensive understanding of the theoretical and empirical aspects of the research topic. Academic journals, books, scholarly articles, and reputable research reports will be extensively reviewed to establish the theoretical framework, examine historical precedents, and analyze the Chinese case study. These secondary sources will help contextualize China's model of digital repression within the broader international relations literature.

The scope of this study is limited to the analysis of China's model of digital repression and its implications for international relations. While many other authoritarian regimes use technology for repression and control, such as Russia and Iran, this study focuses exclusively on China due to its unique combination of technological sophistication, scale, and export of its model to other countries. Furthermore, this study does not seek to provide a comprehensive analysis of China's domestic politics, economy, or foreign policy, but rather to examine the role of technology in authoritarianism and its implications for international relations.

d. Significance and contribution to the field

This study contributes to the growing literature on the intersection of technology and authoritarianism, particularly in the context of China's model of digital repression. The findings of this study will enhance our understanding of the ways in which technology can be used to suppress dissent and control society in authoritarian regimes. In addition, this study will shed light on the potential implications of China's model of digital repression for international relations, particularly with regard to issues of human rights, cybersecurity, and global governance.

One of the key contributions of this study is its focus on China's digital surveillance state and its model of digital repression, which has been widely discussed in the media and policy circles but has received relatively little attention in academic literature. By conducting a detailed and nuanced analysis of China's use of technology for repression

and control, this study seeks to fill this gap in the literature and provide a comprehensive understanding of the topic.

Another contribution of this study is its adoption of a qualitative case study approach, which allows for a detailed and in-depth analysis of the phenomenon under study. By using multiple sources of data and employing a systematic and transparent approach to data collection and analysis, this study seeks to enhance the validity and reliability of the findings and contribute to the methodological rigor of the field.

Finally, this study has important implications for policy and practice. By highlighting the ways in which technology can be used for repression and control, this study underscores the need for greater attention to issues of human rights and democracy in the development and deployment of technology. Furthermore, by examining the potential implications of China's model of digital repression for international relations, this study provides insights into the challenges and opportunities that arise from the intersection of technology and global governance.

II. Literature Review

a. Theoretical Framework: Technology and Authoritarianism

Authoritarianism is a form of government in which power is concentrated in the hands of a single leader or a small group of leaders who exercise control over all aspects of society. As argued by Linz & Stepan (1978), authoritarian regimes can be identified through some key features, such as the absence of meaningful political competition, and the suppression of civil liberties and political rights. They also noted that authoritarian regimes often emerge in situations where there is a crisis of legitimacy or a breakdown of the existing democratic order. Some other characteristics will be detailed above.

Firstly, the suppression of political opposition. Authoritarian governments typically restrict or eliminate political opposition through censorship, imprisonment, or violence. As noted by Levitsky and Ziblatt (2018), authoritarian regimes "silence, repress, and coerce those who dare to challenge their authority." In the context of technology, this can include the monitoring of online activities, the use of facial recognition technology, and the manipulation of social media platforms to stifle dissent (King, Pan, & Roberts, 2013).

Secondly, the control of media. Authoritarian governments often control the media, using it as a tool for propaganda and to shape public opinion. As stated by Diamond

(2015), “authoritarian rulers typically seek to monopolize the mass media as an instrument of control and manipulation.”

Thirdly, centralized power. Authoritarian regimes concentrate power in the hands of a single leader or small group of leaders. As Zakaria notes (1997), “the essence of authoritarianism is the concentration of power in the hands of a single individual or a small group.” This power control extends to all aspects of society, including the media, the legal system, and the use of force (Levitsky & Way, 2010). In the context of technology, this control can be extended through the use of surveillance and censorship tools, as well as the manipulation of information and communication channels (Levitsky & Way, 2010).

Fourthly, the restriction of political participation. Authoritarian regimes restrict political participation and deny citizens the right to choose their leaders through free and fair elections. As stated by Morse (2012), authoritarian governments create electoral authoritarianism, in which they maintain a façade of democracy while restricting political competition.

Lastly, the use of force. Authoritarian regimes often use force and violence to maintain control over their citizens. Authoritarian regimes are “often characterized by their willingness to use force to suppress opposition” (Davenport, 2007, p. 12).

Altogether, authoritarianism is marked by the concentration of power in the hands of a small group of leaders, the suppression of political opposition, the control of the media, limited political participation, and the use of force to maintain control. These characteristics have been observed in various authoritarian regimes throughout history and are still present in many countries today, such as the case of China.

Given technology’s key role in controlling the population and suppressing opposition in authoritarian regimes, it also becomes a helpful tool for the rise and persistence of these regimes around the world. The development and deployment of sophisticated surveillance technologies, social media platforms, and other digital tools have enabled authoritarian governments to monitor and control their populations more effectively than ever before. We must explore thus, three key concepts: digital repression, information control, and surveillance capitalism.

Digital repression refers to the use of technology by governments to monitor and control their populations, often through the use of sophisticated surveillance technologies and digital tools (Feldstein, 2021). This concept has become increasingly relevant in recent years, as authoritarian regimes such as China and Russia have invested heavily in developing and deploying advanced technologies for monitoring and controlling their populations. The use of facial recognition software, social media monitoring, and other forms of digital surveillance has enabled these regimes to exert unprecedented levels of control over their citizens, stifling dissent and limiting the space for political opposition (Feldstein, 2021). Within digital repression, we could categorize the concept into six different techniques according to Feldstein (2019) and shown in the chart above: surveillance, censorship, disinformation, cyber-attacks & hacking, internet shutdowns, and targeted arrests & violence.

Techniques of Digital Repression

Surveillance	Censorship	Disinformation	Cyber Attacks & Hacking	Internet Shutdowns	Targeted Arrests & Violence
AI surveillance (facial recognition systems, intelligent video surveillance, smart policing, smart cities/safe cities) ***Communications surveillance*** (internet/social media monitoring, mobile phone tapping/SIM registration, location monitoring, intrusion spyware, packet inspection, network interception, cable tapping, telecom surveillance) ***Surveillance laws*** (intelligence/ national security laws, data disclosure, data retention, data localization)	***Political & social content blocked/ filtered; use of friction & flooding*** ***Social media/ICT apps blocked*** ***Content removal*** ***Censorship laws/ directives:*** Religion/blasphemy Cyber crime False news Political/hate speech Lèse-majesté Security/terrorism Sedition Copyright infringement Defamation/libel Indecency/anti-LGBT ***Financial targeting of groups***	Government/ pro-government outlets peddle disinformation, false content Cyber trolling, social media manipulation/ harassment by pro-government actors (astroturfing, bots, sockpuppets, impersonation) Election manipulation (for example, data exploitation)	State-sponsored technical attacks which manipulate software, data, computer systems, or networks to degrade operational capabilities or collect information ***Categories:*** Attacks harming operational capacity Intrusion and surveillance attacks ***Illustrative Tools:*** Vandalism Distributed denial of service Man-in-the-middle Phishing Advanced persistent threat Spoofing Border Gateway Protocol	***Internet or electronic communications disrupted*** Total internet shutdowns Partial shutdowns (restricted website/ social media access, blackouts, slowdowns, throttling) ***Infrastructure restrictions*** (internet firewall; closed ICT infrastructure)	ICT user charged, arrested, imprisoned, or in prolonged detention for political/social content ICT user physically attacked or killed

(Feldstein, 2019)

Another key concept in the theoretical framework linking technology and authoritarianism is information control. Authoritarian regimes often use technology to control the flow of information within their societies, limiting access to independent media and suppressing dissenting voices (Zuboff, 2019). This can take many forms, from censorship of online content to the creation of alternative media outlets that present a skewed or heavily biased view of events. The use of social media platforms has also allowed authoritarian regimes to manipulate public opinion, through the use of fake news, targeted advertising, and other forms of digital propaganda (Feldstein, 2021).

A third key concept in the theoretical framework linking technology and authoritarianism is surveillance capitalism. This term refers to the practice of companies like Facebook and Google of collecting vast amounts of user data and using it to target advertising and shape user behavior (Zuboff, 2019). This has led to concerns about how these companies are able to manipulate public opinion and shape political discourse, particularly in the context of authoritarian regimes that use these platforms to spread propaganda and monitor dissent.

All in all, the theoretical framework surrounding authoritarianism and its relationship with technology highlights the potential dangers of unchecked technological development in the context of authoritarian regimes. Moreover, the use of digital repression, information control, and surveillance capitalism by authoritarian governments has enabled them to exert unprecedented levels of control over their populations, limiting the space for political opposition and stifling dissent. By understanding these theoretical concepts, we can better analyze the role of technology in contemporary authoritarian regimes with special emphasis on China and its potential implications for human rights and democracy.

b. Historical Examples of Authoritarian Regimes and Technology

The use of technology by authoritarian regimes to exert control over their populations is not a new phenomenon. Throughout history, authoritarian leaders have sought to use new technologies to monitor, manipulate, and suppress their citizens. This section of the literature review will examine several historical examples of authoritarian regimes and technology, including Nazi Germany, the Soviet Union, and North Korea.

Nazi Germany is perhaps one of the most notorious examples of an authoritarian regime that used technology to exert control over its citizens. Under the leadership of

Adolf Hitler, the Nazi regime used radio broadcasting, propaganda films, and other forms of media to shape public opinion and disseminate its ideology (Wistrich, 2013). The regime also developed advanced surveillance technologies, including wiretapping devices and secret police units, to monitor the activities of its citizens and suppress dissent (Friedman, 2013). These technologies were used to identify and persecute political opponents, Jews, and other groups deemed undesirable by the regime.

The Soviet Union is another historical example of an authoritarian regime that made extensive use of technology to control its population. Under the leadership of Joseph Stalin, the Soviet government developed a vast network of informants and secret police units to monitor and suppress dissent (Davies, 1998). The regime also developed a highly centralized media system that allowed it to control the flow of information to the Soviet people (Ellul, 1964). This system included a government-controlled press, radio, and television, as well as strict censorship laws that limited access to independent sources of information.

North Korea provides a more contemporary example of an authoritarian regime that has made extensive use of technology to control its population. Under the leadership of the Kim family dynasty, the regime has developed an advanced surveillance state that monitors the activities of its citizens using a range of digital tools (Byman & Lind, 2010). These tools include facial recognition software, social media monitoring, and GPS tracking devices, which are used to monitor the movements and activities of citizens (Pearson, 2017). The regime has also developed a highly centralized media system that presents a heavily biased view of events and limits access to independent sources of information (Pearson, 2017).

As we can see, these historical examples highlight how technology has been used by authoritarian regimes to exert control over their populations. Whether through the use of propaganda, surveillance, or censorship, these regimes have sought to use technology to shape public opinion, suppress dissent, and maintain their grip on power. As such, it is important to examine how technology is being used by contemporary authoritarian regimes such as China, and the potential implications for human rights, democracy, and global governance.

III. China’s Model of Digital Repression

a. The role of technology in China’s authoritarian regime

China has become a leader and innovator in IT (information technology) and AI-based mass monitoring (Ding, 2018). The role of technology in China’s authoritarian regime is instrumental in consolidating state power and exerting control over its citizens. Digital surveillance and censorship tools in particular play a central role in enabling the Chinese government — the CCP — to monitor and suppress dissent, consolidate state power, and erode civil liberties (Heilmann & Stepan, 2016). This highlights the pivotal role technology plays in enabling the regime to monitor and regulate its citizens. The Chinese government extensively utilizes advanced surveillance technologies to monitor its citizens’ activities, both online and offline (Heilmann & Stepan, 2016). Moreover, China serves as an instance where the military is involved in the China Brain Project due to its incorporation of deep learning techniques to analyze user behavior through Baidu, the primary search engine in China (Ünver, 2018). This initiative aims to gather data and insights from Baidu search results with the assistance of advanced machine learning algorithms.

The implementation of China's SCS is a notable example of the role technology plays in reinforcing authoritarian control. The Chinese government’s policy for data access, illustrates two key elements of its overall AI strategy: its control over big technological businesses and its propensity for protectionism. In order to increase customer trust in online platforms, numerous well-known IT companies in China agreed to share data with the government in October 2016. The creation of a national “social credit system,” which some privacy activists contend may be used for vast monitoring reasons, was the goal of a bigger effort that included this program (Ding, 2018). The Chinese government wants to assert more control over these internet giants as AI-driven businesses companies continue to grow in importance. There have been proposals about internet regulators purchasing “special” stakes of 1% in these businesses (Yuan, 2017). These investments will grant Chinese government representatives’ seats on corporate boards and the authority to oversee content on the company’s online properties (Yuan, 2017). Ding (2018) emphasizes that technology, including surveillance cameras and data collection, is instrumental in monitoring individuals’ behavior and assigning social credit scores based on their compliance with government policies. He further argues that the SCS acts as a mechanism for social control and shaping citizens’ behavior.

Censorship of online content is another critical aspect of China's digital repression. Y. Wang (2020) highlights the impact of the Great Firewall, China's sophisticated internet censorship system, on controlling information flow and shaping public opinion. The government actively filters and blocks access to foreign websites and social media platforms, limiting citizens' access to alternative sources of information and maintaining a tight grip on the narrative. The watchdog group *Reporters without Borders* ranked China 179 out of 180 countries in its 2022 worldwide index of press freedom and labels the country as "the world's largest prison for journalists"; "its regime conducts a campaign of repression against journalism and the right to information worldwide" (Reporters without Borders, 2023). In its 2022 Freedom on the Net report, China was identified as "the world's worst environment for internet freedom for the eighth consecutive year" (Shahbaz et al., 2022).

The Chinese government's use of technology for censorship and control extends to social media platforms as well. Xu (2014) discusses the dynamics of social media censorship in China, noting that platforms such as Weibo actively moderate and suppress content that is deemed sensitive or critical of the regime. Scholars explain that this censorship operates through a combination of automated filtering algorithms and human intervention, effectively silencing dissenting voices and limiting the spread of information (King, Pan, & Roberts, 2013; Xu, 2014).

As Heilmann & Stepan (2016) point out, the Xi Jinping leadership has significantly strengthened online control after assuming office, resulting in the most effective and rigid control scheme to date. His government views information technologies as opening the door to pervasive mass surveillance. In order to properly enforce laws and regulations and to make people behave in accordance with the social standards established by the CCP, it has deployed information technology as a political instrument of automatic and real-time control (Polyakova & Meserole, 2019). The ultimate goal is to establish a community that is "civilized." Thus, the correlation between IT and authoritarianism is clear, IT serves as a valuable tool for the Chinese government to consolidate state power and exert control over its citizens through a repressing political system to "avoid potential subversion of its authority" (Xu, 2014).

In summary, the role of technology in China's authoritarian regime is instrumental in facilitating surveillance, censorship, and control. It empowers the government to monitor citizens, shape behavior through the SCS, control information flow through internet censorship, and silence dissent on social media platforms. These technological

mechanisms play a central role in reinforcing the regime's authoritarian rule and suppressing challenges to its authority.

b. The development of the Social Credit System

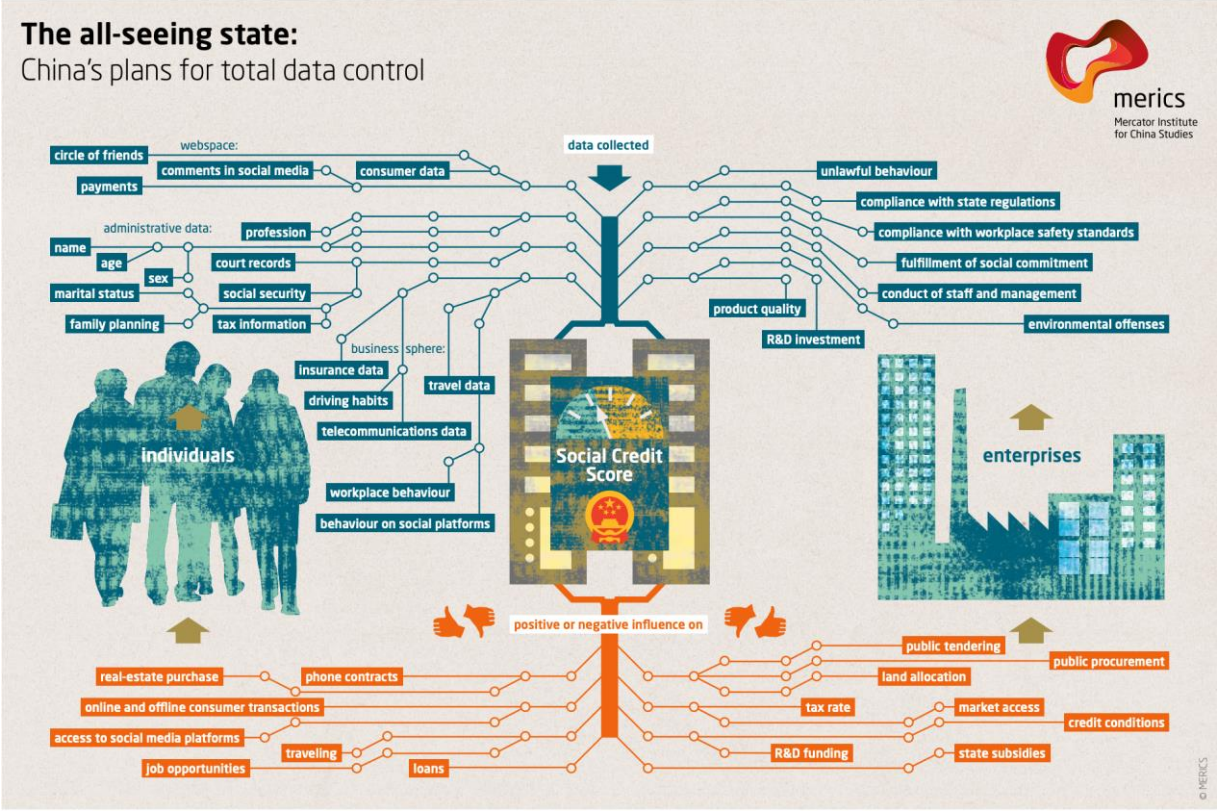
The SCS utilizes advanced technologies such as big data analytics, artificial intelligence, and surveillance systems to collect and process vast amounts of information about individuals and their behaviors. This includes financial transactions, online activities, social interactions, and more. The data is then analyzed and used to generate a comprehensive score that reflects an individual's or business's creditworthiness and social standing (Ding, 2018).

As Ünver (2018) points out, the system works resembling its previous iterations that were trained on data related to criminal activities and national security threats, collecting, and organizing digital human actions. Disclosures made by Edward Snowden brought to light that the United Kingdom employed a comparable program called 'Karma Police,' which involved the correlation of vast amounts of user IP data with SMS metadata and social media records (Ünver, 2018). This laid the groundwork for one of the most extensive and concerning surveillance initiatives in European law enforcement.

Critics of the system raise concerns about privacy, surveillance, and the potential for abuse of power. They argue that the extensive monitoring and collection of personal data can infringe on individuals' privacy rights and enable the government to exert undue control over their lives. Furthermore, there are fears that the system could be used as a tool for social and political repression, suppressing dissent and rewarding conformity. Some even label it as an "Orwellian" project, and many newspaper articles even claim that it further reinforces China's totalitarian overtones (Mozur, 2019; Qiang, 2018; The Economist, 2016).

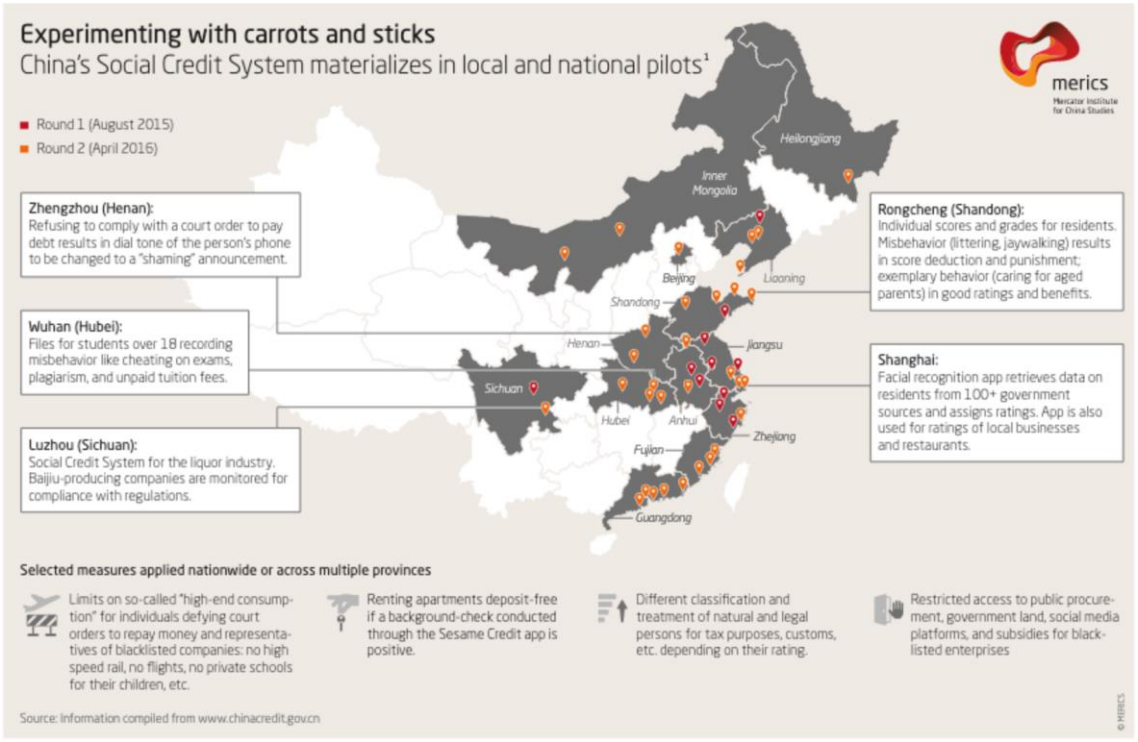
However, scholars such as Vincent Brussee (2021), analyst at the Mercator Institute for China Studies, leave aside the usual exaggerated claims of the system. He argues that it is quite fragmented and localized project, which can be seen as a "symptom of central authorities being unclear about goals and how to reach them". This provides local governments the freedom to carry out programs in innovative or self-serving ways, resulting in a variety of odd experiments, such as the purposeful inflation of data. The reason behind this is to, as Brussee (2021) points out, make the system appear more

effective than it actually is. The following illustration shows how the SCS works and how it collects data in order to create a score.



(Heilmann & Stepan, 2016)

Thus, it is important to note that the SCS national implementation is still at an early stage, with various local pilot programs and experiments being conducted across different regions and industries in China (Ohlberg et al., 2017). The full implementation and impact of the system are yet to be fully realized (Ding, 2018) but even so, the scope of this system is massive and will transform China's "legal, social, and economic environment significantly" (Ohlberg et al., 2017). Some examples of localized projects are the following:



(Ohlberg et al., 2017)

In conclusion, the Social Credit System (SCS) in China relies on advanced technologies to collect and process vast amounts of data on individuals, including financial transactions, online activities, and social interactions. This information is analyzed to generate comprehensive scores reflecting creditworthiness and social standing. Critics highlight concerns regarding privacy, surveillance, and potential abuse of power, expressing worries about infringement on individuals' rights and the system's potential for social and political repression. Some perceive it as reinforcing China's totalitarian tendencies.

However, scholars like Vincent Brussee emphasize that the SCS is a fragmented and localized project, indicating a lack of clarity in central authorities' goals and approaches. This allows local governments to experiment and implement programs in various ways, sometimes resorting to data manipulation to enhance the system's perceived effectiveness. It is worth noting that the SCS is still in the developmental stage, with ongoing pilot programs and experiments across different regions and industries in China. Therefore, the full implementation and ultimate impact of the system are yet to be fully understood.

c. The case of Xinjiang: discriminatory digital repression in China

The case of Xinjiang provides a compelling example of discriminatory digital repression within China's model of digital repression. Xinjiang, an autonomous region in northwest China, has been subjected to extensive surveillance and control measures implemented by the Chinese government (Cho, 2020). These measures involve the widespread use of advanced technologies, including facial recognition systems, biometric data collection, and predictive policing algorithms (Ünver, 2018). According to China's Ministry of Public Security (MPS), Xinjiang conforms the building of "the world's largest facial recognition database" (Ding, 2018).

One of the key aspects of the digital repression in Xinjiang is the targeting of the Uighur Muslim minority population (Cho, 2020). The Chinese government has framed its actions as counter-terrorism and deradicalization efforts, but critics argue that these measures amount to systemic discrimination and human rights abuses (Ding, 2018; Human Rights Watch, 2019). The surveillance technologies deployed in Xinjiang enable the Chinese authorities to closely monitor the activities and behaviors of Uighur individuals, resulting in an environment of constant surveillance and control.

The use of technology in Xinjiang goes beyond mere surveillance but rather it also serves as a basis for the "arbitrary and indefinite detention of Uighur minorities in political re-education camps" (Cho, 2020), where they are subjected to forced labor, political indoctrination, and cultural assimilation (Human Rights Watch, 2019). Technology plays a significant role in these camps, with reports suggesting the use of facial recognition systems and biometric data collection to track and monitor detainees (Human Rights Watch, 2019). The data collected through these technologies further strengthens the Chinese government's control over individuals, making it easier to identify and target individuals based on their religious or cultural affiliations.

The international community has expressed widespread condemnation of the discriminatory digital repression in Xinjiang (Clarke, 2019). Human rights organizations, governments, and activists have raised concerns about the violations of human rights, including the right to privacy, freedom of religion, and freedom of expression (Human Rights Watch, 2019). They argue that the Chinese government's actions in Xinjiang are not only a gross violation of basic human rights but also an example of how technology can be weaponized to target specific ethnic and religious groups.

As Clarke (2019) explains, international responses to the situation in Xinjiang have varied. Some countries and organizations have imposed sanctions and restrictions on Chinese officials and entities involved in the repression. Others have called for independent investigations and accountability for human rights abuses. However, challenges persist in addressing the issue effectively due to geopolitical considerations and China's economic and political influence.

The case of Xinjiang highlights the dangers and ethical implications of using technology for discriminatory purposes within an authoritarian regime. It raises questions about the responsible use of technology, the protection of human rights, and the need for international norms and regulations to govern the development and deployment of surveillance technologies. The ongoing scrutiny and condemnation of China's actions in Xinjiang serve as a reminder of the importance of upholding human rights and ensuring the ethical use of technology in the digital age.

IV. Impacts and Implications

a. Human rights violations and surveillance concerns

The development and implementation of advanced surveillance technologies in authoritarian regimes, such as China, have raised significant concerns regarding human rights violations and the erosion of privacy. Scholars have examined the implications of these technologies and highlighted the following key issues:

Human rights violations are a major concern when discussing the impact of advanced surveillance technologies in authoritarian regimes. The use of surveillance systems, including facial recognition, biometric data collection, and networked surveillance cameras, has led to mass surveillance that intrudes upon the right to privacy and personal freedom (Human Rights Watch, 2019). These technologies enable pervasive monitoring of individuals' activities, creating a culture of fear and self-censorship (Ünver, 2018).

The extensive surveillance measures employed in authoritarian regimes undermine individual autonomy and restrict freedom of expression, assembly, and association (Reporters without Borders, 2023; Human Rights Watch, 2019). The fear of being monitored and punished for dissenting views or actions stifles open dialogue and critical discourse (Ding, 2018). As a result, citizens may refrain from expressing their opinions, leading to a chilling effect on democratic processes and public participation.

Furthermore, the collection and analysis of vast amounts of personal data raise concerns about data privacy and security. Authoritarian regimes often lack robust legal frameworks and oversight mechanisms to protect individuals' personal information (Heilmann & Stepan, 2016). This leaves citizens vulnerable to abuse and misuse of their data, including surveillance-based harassment, discrimination, and social control.

Scholars argue that the implementation of these surveillance technologies exacerbates social inequalities and discrimination (Xu, 2014). Biased algorithms and discriminatory profiling can disproportionately target marginalized groups, such as ethnic minorities (those present in Xinjiang) or political dissidents (Shambaugh, 2007). The lack of transparency and accountability in the use of these technologies further compounds these risks, as individuals have limited recourse to challenge or question the decisions made based on automated surveillance systems.

The international community has expressed concerns about the export of these surveillance technologies to other countries, as it can enable repressive regimes to enhance their surveillance capabilities and violate human rights on a global scale (Polyakova & Meserole, 2019). The transfer of surveillance technologies from authoritarian states to countries with weak democratic institutions can further undermine civil liberties and democratic values.

To address these concerns, scholars emphasize the importance of establishing robust legal and regulatory frameworks that safeguard individual rights and protect against the abuse of surveillance technologies (Cho, 2020; Ding, 2018; Heilmann & Stepan, 2016). It is crucial to strike a balance between security concerns and the protection of human rights, ensuring that surveillance measures are subject to judicial oversight, transparency, and accountability.

In conclusion, the widespread use of advanced surveillance technologies in authoritarian regimes raises significant human rights concerns and threatens privacy, freedom of expression, and democratic principles. Scholars emphasize the need for international cooperation, legal safeguards, and public awareness to mitigate the negative impacts of these technologies and protect individual rights in an increasingly digitized world.

b. Exporting the Chinese model of digital repression

Based on empirical evidence from the AIGS Index, it becomes evident that Chinese companies, particularly Huawei, hold a prominent position as major global providers of AI surveillance systems (Ding, 2018). China's concerted efforts to attain AI leadership and influence have led to its identification as a significant force driving "authoritarian tech" (Sherman & Morgus, 2018). While it is true that some Chinese exports of AI surveillance technology are destined for countries with a history of human rights violations like Zimbabwe and Venezuela, the transfers of such technology occur in a more diverse manner (Feldstein, 2019).

China's export of surveillance technology extends not only to authoritarian regimes but also to liberal democracies. Similarly, companies based in democratic countries, including the UK, and the US, France, Germany, Israel, South Korea, and Japan, are actively involved in selling equipment to oppressive regimes (Feldstein, 2019). For instance, Saudi Arabia has engaged multiple entities such as Huawei, Google, BAE, NEC, Amazon, and Alibaba in establishing various surveillance and smart city projects (Huawei, 2019a).

The AIGS Index reveals that repressive countries rarely rely on a single source for such technology. In countries like Thailand, policymakers prioritize "foreign policy balancing" and avoid aligning too strongly with any particular side (Sherman & Morgus, 2018). However, Chinese companies face heightened scrutiny due to Huawei's dominant market position, extensive global reach, and its close collaboration with governments. Investigative reports have exposed instances where Huawei technicians assisted Ugandan and Zambian officials in spying on political opponents, exemplifying their involvement in government-led surveillance efforts (Biryabarema, 2019).

Additionally, Huawei's role in smart city projects, particularly in the area of public security, has experienced exponential growth. The company actively promotes its safe city model to national security agencies, often with the support of subsidized loans from China's Exim Bank (Huawei, 2019a). Consequently, countries like Mauritius, compelled by financing agreements, engage Huawei as the primary contractor to implement advanced surveillance measures (Huawei, 2019b).

It is worth noting that it is increasingly evident that Huawei operates with limited independence from the Chinese government (U.S. House of Representatives, 2012; Donnan & Oliver, 2014). According to reports, Huawei's leadership has strong ties to

China's security and intelligence agencies and has received significant subsidies from the Chinese government. Ren Zhengfei, the founder of Huawei, is said to have connections to Chinese intelligence. The CCP's creation of "party cells" inside of commercial businesses makes access and control much easier (Lin, 2018).

Furthermore, China's national security law enacted in 2015 requires the 2015 requires that businesses permit access to their networks to outside parties and respond to requests for source code or encryption keys (Feldstein, 2019). Research by Balding and Clarke (2019) reveals that a trade union committee, which is probably a stand-in for Chinese state ownership of the corporation, controls 99 percent of Huawei shares.

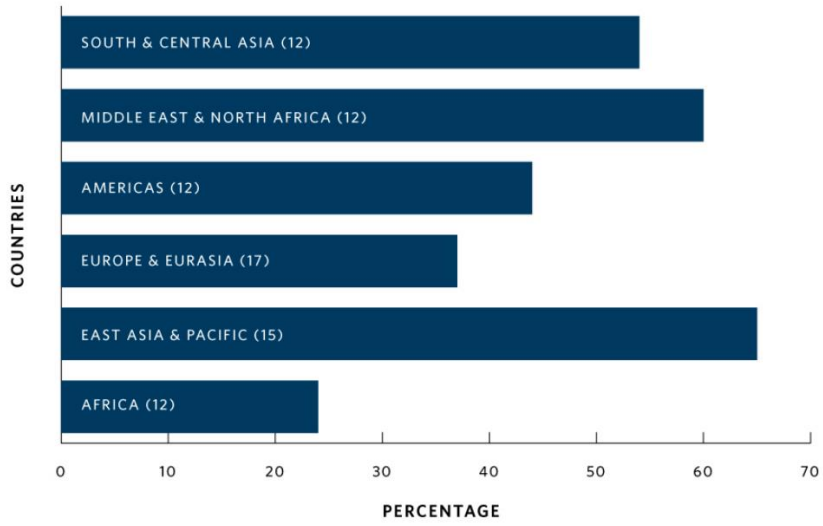
These factors highlight the complex landscape of technology and surveillance, where Chinese companies play a significant role but are not the sole actors involved in exporting authoritarian tech (Feldstein, 2019). Moreover, even though Chinese companies are increasingly active in selling advanced surveillance technology, the true intentions behind their actions remain puzzling. It is unclear to what extent companies like Huawei and ZTE are driven by their own economic interests or are simply carrying out the directives of the Chinese government. According to recent research interviews conducted by Feldstein (2019) in Thailand, there was not uncover any evidence of Chinese companies aggressively promoting advanced AI surveillance equipment or actively encouraging the government to develop sophisticated monitoring systems.

An official from Thailand's Ministry of Interior claims that although China has access to AI technology, they have not actively offered it. Instead, the Thai government would need to indicate interest in the technology and make specific demands for it. The concept of smart cities and safe cities also received skepticism. A prominent technology expert in Thailand, Somkiat Tangkitvanich, referred to the idea of a smart city as a joke. He shared a conversation he had with Thailand's ICT minister, who boasted about plans for a smart city in Phuket but revealed that it mainly involved providing free Wi-Fi and internet access to tourists (Feldstein, 2019). This serves as a valuable reminder that further on-the-ground research is necessary to discern reality from exaggerated claims in this domain.

Moreover, there is a strong correlation between China's strategic China's Belt and Road Initiative (BRI) projects and the widespread deployment of AI surveillance systems. As seen through the AIGS Index (2018), there is a substantial intersection between BRI and AI surveillance. Among the eighty-six countries involved in the BRI, thirty-six of them have a notable presence of AI surveillance technology. The following figure

showcases the number of countries per region that have adopted AI Surveillance as of 2018.

FIGURE 1
Percentage of Countries by Region Adopting AI Surveillance



NOTE: The numbers in parentheses indicate how many countries per region have adopted AI surveillance.

(Feldstein, 2019)

The "Freedom on the Net 2018" report drew attention when it revealed that eighteen out of the sixty-five countries assessed were utilizing AI surveillance technology supplied by Chinese companies (Shahbaz, 2018). A year later, according to the AIGS Index, that same group of countries has expanded to forty-seven, now implementing AI surveillance technology sourced from China (Shahbaz, 2018).

Naturally, nations with authoritarian regimes and restricted political freedoms are investing substantially in AI surveillance methods, getting inspiration from the Chinese model (Ding, 2018). Governments in East Asia, South and Central Asia, the Gulf and Africa are adopting sophisticated monitoring tools, facial recognition cameras, and powerful analytic systems (Feldstein, 2019). However, it is noteworthy that even liberal democracies in Europe are rapidly adopting automated border controls, predictive policing, safe city initiatives, and facial recognition systems (Feldstein & Kot, 2023). In this regard, it is remarkable how many case studies on safe city surveillance, as showcased

on Huawei's website, pertain to municipalities in Italy, Germany, Spain, and the Netherlands (Huawei, 2022).

We could sustain that China's export of its digital repression model normalizes and legitimizes such practices globally. By exporting technologies and promoting their effectiveness, China undermines international norms and standards on human rights and digital freedom (Deibert, 2015). This normalization makes it increasingly challenging for international actors to condemn and counter digital repression practices effectively.

The export of the Chinese model of digital repression has far-reaching impacts, perpetuating authoritarianism, limiting freedom of expression, facilitating human rights violations, and stifling civil society. To address these challenges, international cooperation is crucial. Efforts should focus on raising awareness, advocating for human rights, promoting responsible technology transfer, and establishing global frameworks to protect digital freedoms and ensure ethical use of surveillance technologies.

In conclusion, the exportation of China's model of digital repression holds significant implications for global dynamics. Empirical evidence, as demonstrated by the AIGS Index, highlights the prominent role of Chinese companies, particularly Huawei, as major providers of AI surveillance systems worldwide. Notably, this exportation extends beyond authoritarian regimes, as even liberal democracies engage in the sale and implementation of advanced surveillance technology. While Chinese companies face scrutiny due to Huawei's dominance and close collaboration with governments, they are not the sole actors involved in exporting authoritarian tech. Complex factors, such as the influence of the Chinese government, national security laws, and corporate control, contribute to this landscape. Furthermore, the correlation between China's Belt and Road Initiative (BRI) projects and the widespread deployment of AI surveillance systems emphasizes the far-reaching impact of China's influence. It is crucial to recognize the normalization and legitimization of digital repression practices globally, which undermines international norms on human rights and digital freedom. To address these challenges, international cooperation, awareness raising, human rights advocacy, responsible technology transfer, and the establishment of global frameworks are imperative to safeguard digital freedoms and ensure ethical use of surveillance technologies.

c. International reactions and responses

As Runde et al. (2020) sustain China's growing importance in the Indo-Pacific, pose challenges to the consolidation of democracy in the region. They claim that China has been a key factor in the democratic regression in the region that is expected to worsen due to the impact of the COVID-19 pandemic. For instance, in countries with weak democratic institutions, the pandemic's economic and social pressures may create an environment susceptible to corruption, eroding public trust in democratic governance. This vulnerability is further exploited by China, who has strategically utilized various methods to regain its global influence and reshape the narrative surrounding the COVID-19 pandemic. These efforts include the implementation of disinformation campaigns through digital and social media platforms and the propagation of vaccine-related propaganda. Given the global impact of the pandemic, China has discovered a number of ways to assert its power. Firstly, it has employed a strategy known as "mask diplomacy," whereby it has actively distributed personal protective equipment (PPE) to other countries, aiming to garner sympathy and goodwill (Chen & Molter, 2020). Secondly, disclosed information on their response to the pandemic in a selective manner, portraying it as evidence of the success of their political system (Qiang, 2018). This portrayal seeks to enhance China's international image. Lastly, as nations seek to implement surveillance measures for contact tracing and quarantine purposes, China has the opportunity to export its digital surveillance tools to other countries, potentially further expanding its reach and influence (Runde et al., 2020).

There have been several instances in Taiwan of Chinese influence utilizing false information on COVID-19 to undermine authorities and scientists, tearing Taiwanese society apart in the process. For instance, claiming anonymous members of the Taiwanese parliament, the Chinese mounted a coordinated social media campaign alleging a massive cover-up of illnesses and fatalities. The purpose of the campaign was to "sow distrust in Taiwanese healthcare institutions" (Runde et al., 2020). Coordinated disinformation campaigns have also taken place in China and spread via Weibo (Runde et al., 2020). Therefore, by utilizing the possibilities afforded by COVID-19, the Chinese government has the capability and incentive to use disinformation techniques against democratic societies.

In the interest of human rights and national security, the United States has fought against Chinese technology giants (Runde et al., 2020; M. Wang, 2021). But we must

remember that the United States and its tech companies also have a "checkered history with the very ideals they claim to uphold" (M. Wang, 2021). In this regard, we also have to bear in mind that as Cho (2020) sustains there is an important role of cultural difference on the matter and the fact that Chinese concept of privacy is different from Western political and legal philosophy. Traditional Confucian philosophy prioritizes morality over respect for individual rights (Cho, 2020; Huang, 2014). Privacy is often related to family intimacy or shameful secrets (H. Wang, 2011). In fact, Chinese law treats the right to privacy primarily as a right to protect one's reputation (H. Wang, 2011).

China's growing influence in the Indo-Pacific region and its response to the COVID-19 pandemic have posed challenges to democratic consolidation. China strategically utilizes disinformation campaigns, "mask diplomacy," selective disclosure of pandemic response, and the export of digital surveillance tools to regain global influence. Instances of Chinese influence using false information on COVID-19 highlight the divisive impact of disinformation on democratic societies. The United States has taken a stance against Chinese technology giants, but it is important to acknowledge the complex history of upholding ideals. Cultural differences also play a significant role, with the Chinese concept of privacy differing from Western philosophy. Navigating these challenges requires protecting human rights and democratic principles while considering cultural nuances.

d. The future of technology and authoritarianism

Many scholars argue that advancements in technology, particularly in the areas of surveillance, artificial intelligence, and big data analytics, provide authoritarian regimes with powerful tools to tighten their grip on power (Ding, 2018; Polyakova & Meserole, 2019; Sherman & Morgus, 2018). These technologies enable more sophisticated methods of social control, monitoring, and censorship, allowing regimes to suppress dissent, stifle opposition, and maintain social stability. Scholars highlight the potential for increased surveillance, predictive policing, facial recognition, and social credit systems as instruments of control (Polyakova & Meserole, 2019; Sherman & Morgus, 2018). In the case of China, Heilmann & Stepan (2016) even claim that the country is moving towards a dictatorship supported by IT, where the Chinese leadership's potential for central power and control is strengthened by the growing use of IT technologies.

On the other hand, some scholars such as Xu (2014) suggest that technology can also pose challenges to authoritarian rule. Digital connectivity and social media platforms provide avenues for citizens to express dissent, mobilize collective action, and challenge government narratives. The spread of information and the ability to bypass traditional media gatekeepers can empower citizens and expose state propaganda. Scholars emphasize the role of technology in facilitating social movements, citizen journalism, and the dissemination of alternative narratives (Runde et al., 2020). In fact, proxy servers, virtual private networks (VPNs), and microblogging sites like Weibo have evolved into the principal platforms for Chinese citizens to express dissent or discuss taboo topics (Xu, 2014). According to Jason Q. Ng, specialist on Chinese media censorship and author of *Blocked on Weibo*, "Over the years, in a series of cat-and-mouse games, Chinese Internet users have developed an extensive series of puns—both visual and homophonous—slang, acronyms, memes, and images to skirt restrictions and censors" (Xu, 2014).

As we can see, technological advancements can have both positive and negative implications. Thus, we can highlight the dual-use nature of many technologies, which can be harnessed for both oppressive and liberating purposes. This creates a complex and dynamic landscape where the same technology can be used by both authoritarian regimes and pro-democracy activists. We must understand the contextual factors, socio-political dynamics, and human agency; crucial in determining the ultimate impact of technology on authoritarianism.

As we have previously explored, the Chinese government exports its model of digital repression to other authoritarian regimes. So, we must take into account the global diffusion of digital repression practices. Authoritarian regimes share strategies, techniques, and technologies, creating a "digital authoritarian playbook" (Khalil, 2020). Scholars argue that the exchange of information and tools among autocratic governments enables the replication and spread of repressive practices worldwide (Heilmann & Stepan, 2016). In consequence, we need to stress the importance of international collaboration and coordination to address the challenges posed by this global diffusion.

Ethical considerations and policy implications should be central to scholarly discussions on the future of technology and authoritarianism. We need to emphasize robust legal frameworks, human rights protections, and transparency in the development and use of technology. We should also call for ethical guidelines for tech companies, export controls on surveillance technologies, and international norms to prevent the abuse of technology by authoritarian regimes. The role of civil society, academia, and

international organizations is also important to monitor and advocate for digital freedom and human rights.

Overall, scholars highlight the complex and evolving nature of the relationship between technology and authoritarianism. While technology can amplify repressive practices, it can also empower individuals and challenge autocratic rule. Understanding the dynamics, impacts, and policy implications of technology in the context of authoritarianism is an ongoing area of research that seeks to shape the future trajectory of technology and safeguard democratic values.

V. Conclusion

a. Summary of findings

This study has delved into the role of technology in authoritarian regimes, with a specific focus on China's model of digital repression. By examining the various aspects of China's approach to controlling and monitoring its citizens through technological means, important insights have been gained regarding the impact and implications of such measures.

Through an analysis of existing research and case studies, it has become evident that technology plays a significant role in the consolidation and maintenance of authoritarian control in China. The Chinese government's implementation of advanced surveillance systems, internet censorship, and social credit systems has effectively created a comprehensive digital ecosystem of repression. These technological measures enable the government to monitor, track, and control the actions and behaviors of its citizens, suppressing dissent and maintaining social stability.

The findings of this study highlight the multifaceted nature of China's model of digital repression, which encompasses a range of technological tools and strategies. From the Great Firewall that restricts access to information to the widespread use of facial recognition technology for surveillance, China has established a sophisticated infrastructure that enables the state to exert control over its population.

Moreover, the study underscores the potential global implications of China's model of digital repression. As other authoritarian regimes observe and adopt similar tactics, the erosion of privacy, civil liberties, and freedom of expression becomes a concerning reality. The Chinese example serves as a cautionary tale, urging scholars, policymakers, and advocates to critically examine the impact of technology on governance and individual rights. It is important to note the substantial intersection between China's Belt

and Road Initiative (BRI) and AI surveillance. This indicates a strong correlation between China's strategic BRI projects and the widespread deployment of AI surveillance systems. Western democracies have also used these systems in both lawful and unlawful ways, where there is a particular influence of Chinese companies with Huawei standing out as a major provider of AI surveillance technology worldwide.

In conclusion, this study sheds light on the role of technology in authoritarian regimes, focusing on China's model of digital repression. By providing a comprehensive understanding of the various technological measures employed by the Chinese government, this research contributes to a broader discussion on the implications of digital repression for societies, governance, and human rights. It is crucial for policymakers and society as a whole to critically assess the trade-offs between security and individual freedoms in the age of technology-driven authoritarianism.

b. Implications for international relations and policy

Analyzing the export of the Chinese model of digital repression sheds light on the broader implications for global digital governance and human rights. It highlights the need for international collaboration to protect individuals' fundamental freedoms, counter digital repression, and establish ethical standards for the use of surveillance technologies in a way that respects human rights and democratic values. This section examines the key implications resulting from the spread of Chinese digital repression practices.

Firstly, China's export of its digital repression model reshapes power dynamics in international relations. As China provides recipient countries with surveillance technologies and establishes partnerships, it gains influence and leverage over these nations (Heilmann & Stepan, 2016). This grants China greater political and economic clout, potentially challenging the dominance of traditional Western powers and impacting global governance structures.

Secondly, the export of the Chinese model presents normative challenges in international relations. China's promotion and normalization of digital repression practices undermine established norms of human rights, privacy, and freedom of expression (Lin, 2018). This creates tension between countries upholding democratic values and those adopting or endorsing China's model. It also poses a challenge for the development of consistent global standards and regulations on digital governance.

Thirdly, the export of Chinese digital repression forces countries to navigate a delicate balance between economic interests and upholding democratic values. Many countries are attracted to China's economic investments, technological partnerships, and infrastructure projects, but at the same time, they must grapple with the implications of adopting repressive surveillance technologies (Cho, 2020). Policymakers face the challenge of safeguarding human rights while maintaining economic cooperation with China.

Fourthly, these practices pose a threat to global internet freedom. The widespread adoption of Chinese surveillance technologies by recipient countries creates a ripple effect, emboldening other authoritarian regimes to adopt similar measures (Sherman & Morgus, 2018). This trend undermines the free and open nature of the internet, curtailing digital rights and impeding the free flow of information across borders.

Lastly, addressing the implications of Chinese digital repression requires coordinated policy responses and international cooperation. Policymakers need to develop comprehensive strategies that safeguard human rights, promote digital freedom, and regulate the ethical use of surveillance technologies (Ding, 2018). Collaborative efforts among democracies, international organizations, and civil society groups are crucial to counter the spread of digital repression and protect the values of transparency, accountability, and respect for human rights.

We should also remark how the United States must reshape its strategy regarding AI and China. It should start leading by example for other nations. As M. Wang (2021) points out, the US must update its own surveillance policies, protect the security and privacy of its citizens, and work with partners to create international standards that respect human rights that internet corporations must follow.

The ongoing debate surrounding privacy and data protection has sparked arguments from both sides. Advocates of individual freedom emphasize privacy as a fundamental aspect, while businesses and security agencies raise concerns about regulatory costs and the effectiveness of law enforcement. In response, societal actors have been pushing the boundaries of personal data collection and utilization.

Currently, there is no global consensus on the regulation of data technologies. Around 30% of countries lack national data protection laws, and those that do often have limited coverage and broad exemptions (UNCTAD, 2016). Privacy guidelines issued by global and regional organizations often overlook the issue of government surveillance.

Interestingly, even the United States, home to major internet companies and advanced data technologies, lacks a comprehensive data protection law (Cho, 2020). Instead, it relies on a patchwork of sector-specific and state-level regulations.

The implications of China's model of digital repression for international relations and policy are multifaceted. They encompass power shifts, normative challenges, the delicate balance between economic interests and values, threats to global internet freedom, and the necessity of coordinated policy responses. Addressing these implications requires a collective effort to safeguard human rights, promote digital freedom, and uphold democratic values in the face of growing digital repression practices globally.

c. Limitations and future directions for research

While this thesis has provided valuable insights into the role of technology in China's authoritarian regime and its implications, it is important to acknowledge certain limitations and identify potential avenues for future research.

One significant limitation is the restricted access to comprehensive and up-to-date data on the development and implementation of repression practices. Due to the secretive nature of the regime and limited transparency, obtaining accurate and reliable information can be challenging. Future research could explore strategies to overcome these data limitations, such as leveraging alternative sources, conducting fieldwork in relevant regions, and fostering collaborations with local researchers and organizations.

China is a vast country with regional variations in the implementation and impact of digital repression. This thesis provides a broad overview, but further research could delve into specific regions or case studies to better understand the nuanced dynamics at play. Comparative studies between regions within China or with other countries adopting similar practices would contribute to a more comprehensive understanding of the subject matter.

Given the human rights implications of China's digital repression, future research should include a more in-depth analysis of the ethical considerations involved. This could involve examining the specific rights violations, such as privacy infringements, freedom of expression restrictions, and discriminatory targeting, and exploring the legal and normative frameworks that can be utilized to address these concerns.

The examination of the impact of digital repression on civil society organizations, social movements, and citizen resistance is another important area for future research. Understanding how individuals and groups navigate and respond to digital repression measures, including the adoption of countermeasures and circumvention strategies, can shed light on the resilience of civil society and potential avenues for promoting human rights and democratic values.

Comparative analysis with other digital authoritarian models, such as those observed in Russia, Iran, or North Korea, can provide valuable insights into the similarities and differences in their approaches and impacts. Understanding the variations in digital repression practices across different contexts can contribute to a broader understanding of the global dynamics of digital authoritarianism.

Addressing these limitations and pursuing future research in these areas will enhance our understanding of the role of technology in China's authoritarian regime and its wider implications. It will also contribute to the development of more effective policies and strategies to protect human rights, promote digital freedom, and counter the spread of digital repression globally.

VI. References

AIGS Index 2018. Carnegie Endowment for International Peace. (2018). https://carnegieendowment.org/files/AI_Global_Surveillance_Index1.pdf

Balding, C., & Clarke, D. C. (2019). Who owns Huawei? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3372669

Biryabarema, E. (2019, August 15). Uganda's cash-strapped cops spend $126 million on CCTV from Huawei. Reuters. Retrieved from https://www.reuters.com/article/us-uganda-crime-idUSKCN1V50RF.

Brussee, V. (2021, September 15). *China's Social Credit System is actually quite boring.* Foreign Policy. https://foreignpolicy.com/2021/09/15/china-social-credit-system-authoritarian/

Byman, D., & Lind, J. (2010). Pyongyang's Survival Strategy: Tools of Authoritarian Control in North Korea. *International Security, 35*(1), 44–74.

Chen, A., & Molter, V. (2020, June 16). *Mask diplomacy: Chinese narratives in the Covid era*. Stanford Cyber Policy Center: Freeman Spogli Institute for International Studies. https://cyber.fsi.stanford.edu/news/covid-mask-diplomacy

Cho, E. (2020, May 1). *The Social Credit System: Not just another Chinese idiosyncrasy | journal of public and international affairs*. Princeton University. https://jpia.princeton.edu/news/social-credit-system-not-just-another-chinese-idiosyncrasy

Clarke, M. (2019). China: Repression at home, extension abroad. In I. Kfir & G. Grice (Eds.), *COUNTERTERRORISM YEARBOOK 2019* (pp. 31–40). Australian Strategic Policy Institute. http://www.jstor.org/stable/resrep23114.7

Davenport, C. (2007). State repression and political order. *Annual Review of Political Science, 10*(1), 1-23.

Davies, R. W. (1998). *Soviet economic development from Lenin to Khrushchev*. Cambridge Univ. Press.

Deibert, R. (2015). Authoritarianism Goes Global: Cyberspace Under Siege. *Journal of Democracy, 26*(3), 64-78. 10.1353/jod.2015.0051

Diamond, L. (2015). Facing up to the democratic recession. *Journal of Democracy, 26*(1), 141-155.

Ding, J. (2018, March). *Deciphering China's AI Dream.* Future of Humanity Institute - University of Oxford. https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf

Donnan, S., & Oliver, C. (2014, March 27). EU commissioner attacks China's telecoms subsidies. *Financial Times*. Retrieved from https://www.ft.com/content/d6d0bcc6-b5cb-11e3-b40e-00144feabdc0

Ellul, J. (1964). The Technological Society. New York: Vintage Books.

Feldstein, S. (2019). Appendix 2: Taxonomy of Digital Repression. In *The Global Expansion of AI Surveillance* (pp. 29–29). Carnegie Endowment for International Peace. http://www.jstor.org/stable/resrep20995.12

Feldstein, S. (2021). *The rise of digital repression: How technology is Reshaping Power, politics, and resistance*. Oxford University Press.

Feldstein, S., & Kot, B. (2023). When Is It Permissible for Governments to Use Spyware? In *Why Does the Global Spyware Industry Continue to Thrive?: Trends, Explanations, and Responses* (pp. 6–8). Carnegie Endowment for International Peace. http://www.jstor.org/stable/resrep48430.5

Friedman, T. L. (2013). Thank You for Being Late: An Optimist's Guide to Thriving in the Age of Accelerations. New York: Farrar, Straus and Giroux.

Heilmann, S., & Stepan, M. (2016, June). *China's Core Executive: Leadership styles, structures and processes under Xi Jinping*. Mercator Institute for China Studies. https://merics.org/sites/default/files/2020-04/MPOC_ChinasCoreExecutive_web.pdf

Huang, P. C. (2014). Morality and law in China, past and present. *Modern China, 41*(1), 3–39. https://doi.org/10.1177/0097700414553923

Huawei. (2019a). *Yanbu: A smart industrial oil kingdom city*. Huawei Enterprise. https://e.huawei.com/es/publications/global/ict_insights/201708310903/manufacturing/201712061133

Huawei. (2019b). *Building a safe Mauritius, the inspiration for Heaven*. Huawei Enterprise. https://e.huawei.com/topic/leading-new-ict-ua/mauritius-safecity-case.html

Huawei. (2022, February 28). *Huawei debuts Giga Green site in Spain for Optimal Energy Efficiency and performance*. Huawei Enterprise. https://www.huawei.com/en/news/2022/2/Debut-Giga-Green-Site-MWC2022

Human Rights Watch. (2019, May 1). *China's algorithms of repression*. Human Rights Watch. https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass

Khalil, L. (2020). *Digital Authoritarianism, China and C0VID*. Lowy Institute for International Policy. http://www.jstor.org/stable/resrep27665

King, G., Pan, J., & Roberts, M. E. (2013). How censorship in China allows government criticism but silences collective expression. *American Political Science Review, 107*(2), 326-343.

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

Levitsky, S., & Ziblatt, D. (2018). How democracies die. Crown.

Lew, J. J., Roughead, G., Hillman, J., & Sacks, D. (2021, March). *Findings | China's Belt and Road: Implications for the United States*. Council on Foreign Relations. https://www.cfr.org/report/chinas-belt-and-road-implications-for-the-united-states/findings

Lin, Z. (2018, November 25). Chinese communist party needs to curtail its presence in private businesses. *South China Morning Post*. Retrieved from https://www.scmp.com/economy/china-economy/article/2174811/chinese-communist-party-needs-curtail-its-presence-private.

Linz, J. J., & Stepan, A. C. (1978). *The breakdown of Democratic regimes*. Johns Hopkins University Press.

Mac Síthigh, D., & Siems, M. (2019). The Chinese Social Credit System: A model for other countries? *The Modern Law Review*, 82(6), 1034–1071. https://doi.org/10.1111/1468-2230.12462

Morse, Y. L. (2012). The era of electoral authoritarianism [Review of Competitive Authoritarianism: Hybrid Regimes after the Cold War; Democratization by Elections: A New Mode of Transition; Voting for Autocracy: Hegemonic Party Survival and Its Demise in Mexico; Electoral Authoritarianism: The Dynamics of Unfree Competition, by S. Levitsky, L. A. Way, S. Lindberg, B. Magaloni, & A. Schedler]. *World Politics*, *64*(1), 161–198. http://www.jstor.org/stable/41428375

Mozur, P. (2019, December 18). China moves towards "digital totalitarian state" as surveillance technology continues to advance. *The Independent.* https://www.independent.co.uk/tech/china-technology-surveillance-network-totalitarian-state-spy-a9251971.html

Ohlberg, M., Ahmed, S., & Lang, B. (2017, December 12). *Central planning, local experiments*. Mercator Institute for China Studies. https://merics.org/sites/default/files/2020-04/171212_China_Monitor_43_Social_Credit_System_Implementation.pdf

Pearson, J. (2017, March 2). *North Korea uses sophisticated tools to spy on citizens digitally - report*. Reuters. https://www.reuters.com/article/us-northkorea-surveillance/north-korea-uses-sophisticated-tools-to-spy-on-citizens-digitally-report-idUSKBN1690DZ

Polyakova, A., & Meserole, C. (2019, August). *Exporting Digital authoritarianism*. Brookings. https://www.brookings.edu/research/exporting-digital-authoritarianism/

Qiang, X. (n.d.). *Chinese digital authoritarianism and its Global Impact*. Project on Middle East Political Science. https://pomeps.org/chinese-digital-authoritarianism-and-its-global-impact

Qiang, X. (2018, February 21). The rise of China as a digital totalitarian state. *The Washington Post.* Retrieved from

Reporters without Borders. (2023). *Worldwide Index of Press Freedom*. Reporters without Borders. https://rsf.org/en/index

Runde, D., Savoy, C., & McKeown, S. (2020). *Post-pandemic Governance in the Indo-Pacific: Adapting USAID's Strategy in the Face of Covid-19.* Center for Strategic and International Studies (CSIS). http://www.jstor.org/stable/resrep26382

Shahbaz, A. (2018). *Freedom on the Net 2018: The Rise of Digital Authoritarianism.* Freedom House. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

Shahbaz, A., Funk, A., & Vesteinsson, K. (2022). *Countering an authoritarian overhaul of the internet.* Freedom House. https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet

Shambaugh, D. (2007). China's Propaganda System: Institutions, Processes and Efficacy. *The China Journal, 57*, 25–58. http://www.jstor.org/stable/20066240

Sherman, J., & Morgus, R. (2018, December 5). *Authoritarians are exporting surveillance tech, and with it their vision for the internet.* Council on Foreign Relations. https://www.cfr.org/blog/authoritarians-are-exporting-surveillance-tech-and-it-their-vision-internet

The Economist Newspaper. (2016, December 17). China invents the Digital Totalitarian State. *The Economist.* https://www.economist.com/briefing/2016/12/17/china-invents-the-digital-totalitarian-state

The rise of digital authoritarianism. Freedom House. (n.d.). Retrieved March 19, 2023, from https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

Tufekci, Z. (2017). Twitter and tear gas: The power and fragility of networked protest. Yale University Press.

Ünver, H. A. (2018). *Artificial Intelligence, Authoritarianism and the Future of Political Systems.* Centre for Economics and Foreign Policy Studies. http://www.jstor.org/stable/resrep26084

United Nations Conference on Trade and Development (UNCTAD). 2016. Data Protection Regulations and International Data Flows: Implications for Trade and Development.

U.S. House of Representatives. (2012, October 8). *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE.* Permanent Select Committee on Intelligence. https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf

Wang, H. (2011). *Protecting privacy in China: A research on China's privacy standards and the possibility of establishing the right to privacy and the information privacy protection legislation in modern China*. Springer.

Wang, M. (2021, April 8). *China's techno-authoritarianism has gone global*. Foreign Affairs. https://www.foreignaffairs.com/articles/china/2021-04-08/chinas-techno-authoritarianism-has-gone-global

Wang, Y. (2020, September 1). *In China, the "great firewall" is changing a generation.* Human Rights Watch. https://www.hrw.org/news/2020/09/01/china-great-firewall-changing-generation

Wistrich, R. S. (2013). Hitler and the Holocaust. London: Routledge.

Xu, B. (2014, September 25). *Backgrounders media censorship in China*. Council on Foreign Relations. https://www.files.ethz.ch/isn/177388/Media%20Censorship%20in%20China.pdf

Yuan, L. (2017, October 12). Beijing pushes for a direct hand in China's Big Tech firms. *The Wall Street Journal*. https://www.wsj.com/articles/beijing-pushes-for-a-direct-hand-in-chinas-big-tech-firms-1507758314

Zakaria, F. (1997). The rise of illiberal democracy. *Foreign Affairs, 76*(6), 22-43.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: Public Affairs.