THE VIRTUAL PANOPTICON IN CHINA: SURVEILLANCE THROUGH THE SECURITISATION OF THE INTERNET

XIAOXUE JIANG MARTIN
ABSTRACT

The essay comments on the debate of the CCP's increasing control over cyberspace since 2013. Specifically, it will argue that, through the securitisation of the internet and cyberactivity, the Chinese government has created a virtual panopticon. To make this case, the Copenhagen School's Securitisation Theory and Foucault's concepts of panopticism and disciplinary power will be explained and applied to the CCP's censorship and surveillance of the Chinese internet. Through securitisation of an issue and putting it in the realm of emergency politics, a government can legitimise exceptional measures that would not be possible under normal circumstances. Several examples of the securitisation of cyberspace will be discussed, such as the 2013 law that made the "spreading of false rumours online" a punishable act, as well as the establishment of the Cyberspace Administration to conduct dataveillance in 2014. More recently, homosexuality has been re-criminalised as "abnormal sexual activity" with the 2017 ban of LGBTQ content on the internet. The CCP's actions were all justified on the basis of national security, framed as a necessary act to protect Chinese citizens from alleged dangers to society. However, these developments are highly problematic as the freedom of speech is increasingly curtailed under rising authoritarianism. The consequence of this successful securitisation is that the CCP has created a virtual panopticon in cyberspace, effectively controlling people's online behaviour. First of all, like in a panopticon, surveillance feels constant and ubiquitous, with netizens' activities permanently visible online. Furthermore, the government's power is visible yet unverifiable, as it is not clear when the CCP is monitoring internet users' activities, nor exactly which activities are illegal. This leads to the internalisation of the CCP's values, as netizens and internet services engage in self-censorship to avoid punishment. The government therefore does not coerce, but discipline. Lastly, it does not matter who conducts the surveillance for the panopticon to function. Everyone can survey and be surveyed. In these ways, it is unsettling to see how efficiently the CCP has created its virtual panopticon.
1. INTRODUCTION

In 2017, for the third year in a row, China had the dubious honour of being named the “world’s worst abuser of internet freedom” by the NGO Freedom House (2018). It is not undeserved: in an impressive demonstration of its pervasive control over Chinese society, the Chinese Communist Party (CCP) has been worryingly successful in tightening and systematising its regulation over cyberspace and the internet over the last five years. The Party’s position on freedom of speech on the internet was succinctly conveyed by President Xi Jinping at the second World Internet Conference in Wuzhen, as he commented: “On the one hand, we should respect the freedom of expression. On the other, we need to create a fine cyberspace order following relevant laws” (Griffiths, 2015). What is problematic here is that the Party does not allow citizens to influence the legislation process, and its laws are designed to keep the Party in place. As such, in practice, cyberspace activity and discussion are allowed, as long as they adhere to party ideology, limiting true freedom of expression. Ironically, while President Xi held his speech about the Chinese understanding of the concept of freedom of expression at the Wuzhen World Internet Conference, Chinese free speech advocate Pu Zhiqiang was held in Beijing’s detention centre for posting tweets critical of the CCP on Twitter (Blake, 2015; Evans, 2015). Many Chinese netizens interpreted this as a warning to other dissidents, showing that critical voices on the internet are not tolerated and will be punished with jail sentences and fines. The CCP thus gives the illusion of free speech on the internet, while in actuality censoring and conducting surveillance in search of nonconformists. How does the CCP justify these actions? And what effects do they have on Chinese netizens?

Once again, a quote by President Xi can serve as elucidation of the CCP’s logic. In April, he proclaimed: “Without web security there’s no national security, there’s no economic and social stability, and it’s difficult to ensure the interests of the broader masses” (Reuters, 2018). In this way, censorship and surveillance are rationalised and enabled by portraying them as necessary ‘invisible’ tools for so-called web security. Accordingly, the government’s omnipresent and all-seeing eye conditions netizens to self-censor and remain uncritical online. This essay will debate these findings and argue that, through the securitisation of the internet and cyberactivity, the Chinese government has created a virtual panopticon. It will be shown that this structure is used to discipline online behaviour to adhere to its censorship rules through the impression of constant and pervasive surveillance. To make this argument, the Copenhagen School’s Securitisation Theory will be applied, as well as Foucault’s concepts of panopticism and disciplinary power to the case study of the CCP’s control over cyberspace in China. The following sections will review previous literature on the CCP’s internet securitisation and its panoptic effects, highlight the concrete ways in which the Party has justified its progressive securitisation of the internet, and demonstrate how China’s cyberspace administration resembles a virtual panopticon. This essay will thus provide a theoretical basis to explain why the Chinese government has been successful in continuing to restrict free speech despite the advent of the internet.
2. LITERATURE REVIEW

As a controversial issue, the Xi administration’s intensifying practices of online surveillance and censorship have received considerable attention both in popular media and in academic literature. Optimistic beliefs as expressed in articles like Liu and Chen’s (2012) *Why China Will Democratize*, which pointed towards the internet as democratizing force, were crushed by the CCP’s repressive internet policies under the new President. Books like Economy’s (2018) *The Third Revolution: Xi Jinping and the New Chinese State* provide an overview of the growing cyberspace regulations. However, these works generally focus on placing these developments in the broader context of growing authoritarianism under President Xi, rather than on how they are justified by the Chinese government, as this essay does. One short article by Caster (2014), did remark the CCP established a link between social media and security regarding its law against ‘spreading rumours’, as does this essay. However, Caster did not explicitly draw the link to Copenhagen School’s Securitisation Theory, nor did he make explicit the mechanisms of securitisation move as elaborated upon in this essay. This work adds to Caster’s by explaining why the CCP made its first securitisation move, why it was effective, how it was followed by deeper securitisation of cyberspace over the following years, and what the effects on netizens’ behaviour were.

These panoptic results of self-censorship of internet surveillance in China were discussed as early as 2003, when Tsui warned of “the potential to have the internet turn into a full-blown Panopticon” (p. 66). Tsui, as well as Zhen in 2015, noted how the panoptic characteristic of the fear of being monitored by the government contributed to online self-censorship. This essay elaborates upon their observations by showing Tsui’s prediction indeed came true under the CCP’s newest internet regulations, and arguing this was enabled through securitisation of the internet. Furthermore, it will emphasise two other crucial panoptic factors that deepen the disciplinary power of the Chinese government: that non-governmental actors also participate in surveillance, and that the government’s power is visible, yet unverifiable. The next sections will present this argument.

3. SECURITISATION THEORY

Securitisation is a concept mainly associated with the constructivist Copenhagen School in Security Studies, consisting of scholars Waever, Buzan, and colleagues from the Copenhagen Peace Research Institute. They define securitisation as "shifting an issue out of the realm of 'normal' political debate into the realm of emergency politics by presenting it as an existential threat" (Peoples and Vaughan-Williams, 2010b: p.76). In other words, securitisation portrays an issue dangerous to such a degree that it has the potential to undermine national security, and poses it therefore does not belong in the a-securitised sphere of society. Normal politics need to be suspended in order to deal with the issue, which legitimises an actor to take exceptional measures, according to the Copenhagen School (Buzan et al. 1998; McDonald, 2008; Peoples and Vaughan-Williams, 2010b). For example, to prevent a life-threatening disease from spreading,
states have the legal authority to impose a quarantine and restrict freedom of movement, which under normal circumstances would be problematic. However, most issues are more ambiguous than this example in endangering national security. As securitisation can authorise controversial and far-reaching actions, it is important to understand the securitisation process.

According to the Copenhagen School, securitisation occurs through 'speech acts', in which an issue is being framed as a security matter by authoritative actors, mostly in the political sphere (Buzan et al., 1998; McDonald, 2008; Peoples and Vaughan-Williams, 2010b). As in Constructivist theory, discourse is crucial, as for securitisation there is always a speaker and an audience involved. Not all attempts at securitisation, or securitising moves, are successful: securitisation is an intersubjective process, a negotiation where a securitising move only succeeds when it is accepted by the intended audience. There are several facilitating or felicity conditions that contribute to the success of a securitisation move, such as the role and authority of the speaker. Furthermore, the Copenhagen School warns against overstretching the concept of security, as it has political and intellectual dangers. After all, securitisation allows a militarised mode of thinking that restricts open discussion and criticism of state actions, so that a certain agenda can be pushed through. In the name of security, a state can justify questionable 'emergency' practises that would otherwise be opposed, which is alarming if the securitisation actor has dishonest intentions. Overstretching the concept of security has intellectual consequences as well: if too many issues are labelled as a security matter, the idea of security loses its meaning and usefulness. Waever (1998) therefore calls for 'desecuritisation', or shifting securitised issues back into the normal political sphere, and urges critical analysis of securitisation moves.

4. SECURITISATION OF CYBERSPACE IN CHINA

Applying theory to practice, we can see how securitisation of cyberspace has transpired in China. The rise of cyberspace, social media, and the internet posed a new challenge to the Chinese government, empowering citizens in several ways (Tai, 2007; Robinson, 2013). With the World Wide Web, the information that flows from, to, and within China became much harder to control. The internet thus stimulated diversity of ideas and opinions diverging from the official Party line, endangering internal stability of the CCP rule. In immediate response to this challenge, in 2000, the Ministry of Public Security started the Golden Shield Project, often referred to as the Great Firewall, as a surveillance and censorship system based on online data (James, 2009; Deibert et al., 2011; Punyakumpol, 2011). Therefore, since the beginning of the internet in China, cyberspace has been politicised to be part of the political sphere. Cyberspace has also increasingly been securitised. Already in 2000, Chinese provinces started forming Internet Police Forces, who would "administrate and maintain order on computer networks" (Tai, 2007: p.99) by finding and censoring controversial web content for the Ministry of Public Security. This shows that the CCP has always imposed cyberspace regulations.
However, though developments like this set the stage for securitisation of cyberspace, they cannot be identified as true securitisation moves yet, according to the Copenhagen School's criteria, since cyberspace was not explicitly linked to security in a speech act (Peoples and Vaughan-Williams, 2010b). True securitisation of cyberspace only started under President Xi’s rule, when China passed a law against the spreading of rumours online in 2013. Circulating ‘false rumours’, of which the definition was left ambiguous, could now lead to detention and trial. According to Xinhua, the spreading of false rumours "mislead[s] the public and disrupt[s] social order", and "freedom of speech does not mean freedom to disseminate information" (Mengjie, 2013). Here, we can see how cyberspace activity was explicitly linked to security, justifying the limitation of the (Western interpretation of) freedom of expression in the name of social stability. This shows the dangers of securitisation, as opinions and information countering the CCP's view could now be framed as harmful rumours, and punished in the name of security ('China: New Ban on 'Spreading Rumors' About Disasters', 2015; Tokmetzis, 2016).

The securitisation movement intensified over the next years, as in 2014 when the Cyberspace Administration of China (CAC) was established under Lu Wei as the central cyberspace control agency to ensure ‘cybersecurity’ (Freedom House, 2018). Its powers were justified with a speech act by President Xi, as he stated that "national security no longer exists without network security" (Kaja and Luo, 2015). The CAC’s powers have expanded significantly since its creation. New cybersecurity laws in 2015 and 2016 enabled it to not only supervise and censor online content by requiring operators to comply and register users under their real names, but also to limit the overseas transfer and storage of personal information of Chinese citizens (Cheung, 2015; Kaja et al., 2015). Furthermore, it demanded that internet companies also monitor and censor their content themselves, with failure resulting in fines or forced closure. The new Counter-Terrorism Law also required internet services to give the CAC decryption keys and access to interface information if needed, allowing the government to access users’ data without difficulty (Carlson et al., 2016; Stratford and Luo, 2016). Another more recent example, is the re-criminalisation of LGBTQ expressions as ‘abnormal’ and ‘deviant’ sexual activity on the same level of sexual abuse and violence, with several attempts to ban gay content on the internet (Hernández and Mou, 2018; Shepherd, 2018). Cyberspace is now almost completely surveyed by the CCP, all in the name of counter-terrorism, protecting national security, and enabling quick response to security incidents (Economy, 2018). This would not be possible without the completion of securitisation of cyberspace, allowing freedom of speech to be increasingly curtailed under rising authoritarianism.

5. FOUCAULT’S PANOPTICON AND DISCIPLINARY POWER

The consequence of successful securitisation is that the CCP has created a virtual panopticon in cyberspace, effectively controlling people’s online behaviour. Panopticism is a concept developed by post-structuralist Foucault (1995), as he analysed the mechanisms of power (Simon, 2005; Peoples and Vaughan-Williams,
He believed that a new form of power relation had emerged since the 17th and 18th century, called 'disciplinary power', which relies mainly on surveillance. Here, the notion of the panoptic comes into play. Originally, the panopticon was developed by English philosopher Jeremy Bentham in 1785. It referred to a prison designed in a circle, with a watchtower in the middle that would be able to view every single cell. Inmates could not see each other or know whether they were being watched. With this set-up, in which power is always visible but never verifiable, the illusion of constant surveillance would prevent misconduct in the most efficient way with the least coercion and actual force. In a disciplinary society, panopticism is infinitely extended to all aspects of daily life. Through surveillance, or the possibility of it, individuals are classified and made to conform to the ruler’s norms. Furthermore, regardless who surveys, whether it be the government, strangers, or even friends, the power of the panopticon is not diminished. Each observer can be observed. Those within the pervasive panopticon are then trained to internalise discipline, not with the use of force, but by making the possibility of punishment always present.

As for the case study of cyberspace and surveillance and censorship, the CCP has been successful in creating a virtual panopticon to control its population. The Chinese government uses disciplinary power to engage in data surveillance, or the ’monitoring and ’mining’ of multiple forms of data [...] with the aim of identifying potentially 'risky' groups and individuals” (Peoples and Vaughan-Williams, 2010c: p.185). These actions are possible for the state, because it has been able to securitise cyberspace. And, just like in a panopticon, the goal of the government in doing this is to control people’s behaviour (Foucault, 1995; Tsui, 2003; Tokmetzis, 2016). The CCP perceives data surveillance as crucial for its regime’s stability. Like in Chinese offline media, freedom of expression had to be limited in cyberspace, and dissident opinions had to be identified and punished. Just like the prison panopticon, cyberspace surveillance is seemingly constant and ubiquitous. Netizens’ activities are permanently visible and punishable. Interestingly however, as King, Pan, and Roberts (2013) found, the CCP does not censor all cyberspace content critical of the state. Instead, censorship mainly focuses on the content that could spur social mobilisation, curtailing collective action. The lines between what is allowed and what is not are always blurred, indicating another clear characteristic of a virtual panopticon. Power is visible but unverifiable: it is not clear when the disciplinary power of the sovereign will be exercised, and it is ambiguous which cyberspace activities will and will not be punished. This uncertainty is used to control internet services and netizens, forcing them to first consider whether their activities are in line with the Party before conducting them.

This leads to another important panoptical characteristic of China’s securitisation of cyberspace, namely that the structure of the panopticon internalises the values of the sovereign in its subjects by making punishment always possible. The CCP has structured its cyberspace censorship in such a way that it does not have to use force constantly to ensure compliance. By punishing a small number of dissidents harshly and publicly, the CCP gives off a warning to all other netizens. This has led to self-censorship of web services and users, reducing public debate about political and social
issues: "The idea is that if you're never quite sure when, why and how hard the boom might be lowered on you, you start controlling yourself, rather than being limited strictly by what the government is able to control directly" (James, 2009). This applies to companies as well, as the CCP considers them responsible for their online content. Since they can be fined or shut down if their censorship is not deemed sufficient, internet services themselves also become more cautious and self-aware (Tsui, 2003; Tokmetzis, 2016; Chong, 2018). This connects to the last panoptic characteristic of our case study: that the disciplinary power of the panopticon is not dependent on who conducts the surveillance. Internet services monitor and censor their own content, netizens censor themselves, but also other netizens. Friends warn each other when cyberspace activity is perceived too risky, as association with dissidents is also dangerous. With China's new developing social credit system giving every citizen a score dependant on criminal offences, online activity, and even the online activity of friends, self-censorship and surveillance of other will become even more common. After all, dissident online activity could lead to a bad score, which will affect citizens’ ability to receive a loan, get a job, and will even influence the search for a romantic partner (Hatton, 2015). Thus, through the securitisation of cyberspace, enabling dataveillance, the CCP has successfully created a virtual panopticon.

6. CONCLUSION

To make my argument, I have shown through several examples that cyberspace has been securitised in China, enabling dataveillance and censorship. These actions have been justified on the basis of national security, framed as necessary to protect citizens from harm. The consequence of this successful securitisation is that the CCP has created a virtual panopticon in cyberspace to effectively control users’ online behaviour. First of all, like in a panopticon, surveillance feels constant and ubiquitous, with netizens' activities permanently visible online. Furthermore, the government's power is visible yet unverifiable, as it is not clear when the CCP monitors users' activities, and exactly which activities are illegal. This leads to the internalisation of the CCP's rules, as netizens and internet services engage in self-censorship to avoid possible punishment. The government therefore does not coerce, but discipline. Lastly, it does not matter who conducts the surveillance for the panopticon to function. Everyone can survey and be surveyed. In these ways, it is unsettling to see how efficiently the CCP has created its virtual panopticon. As President Xi Jinping said: “Cyberspace is not a place [that is] beyond the rule of law” (Phillips, 2015).
BIBLIOGRAPHY


Hatton, C. (2015) 'China's 'social credit': Beijing sets up huge system', BBC News,


ABOUT THE AUTHOR

Xiaoxue Jiang Martin is currently enrolled in the M.A. International Relations at Leiden University, where she focuses on China’s International Political Economy. Previously, she completed her B.A. at University College Maastricht, where her semester abroad at National Taiwan University kindled her fascination with contemporary China’s complex history, politics, and economy. She subsequently completed the Research Master Asian Studies at Leiden University, during which she spent another semester abroad at the Chinese University of Hong Kong. Her research focused on Sino-American relations during the Obama administration.
PUBLISH WITH THE MAPPING CHINA JOURNAL
ABOUT THIS JOURNAL

This peer-reviewed Journal is explicitly aimed at publishing work written by Bachelor and Master students and all interested PhD students in their early stages of their dissertation with an interdisciplinary background in Area Studies, Political and Social Science or in International Relations who have been working on or want to work on China and who are looking to publish their first research for a wider audience.

ABOUT MAPPING CHINA

Mapping China is a young professional network and NGO dedicated to a political science based analysis of contemporary China. We are the first network in Germany with the purpose of connecting young scholars of modern China from different universities in Germany and beyond. We are also the first think tank to offer young China watchers a publication platform for their own academic work specifically on China in order to engage in an academic discussion within a wider audience early on in their academic career. Kindly note that Mapping China publishes work in both German and English and does not translate any original work.

JOURNAL SUBMISSION GUIDELINES

The Mapping China Journal (MCJ) accepts submission of research papers and essays of original scholarly articles by students on all levels, including students at the early stages of their PhD and recent graduates that engage in scholarly discussion. More information about the Journal itself can be found here.

MCJ does not accept any work that has been published before or is set to be published elsewhere. This includes previous self-publishing of the author and articles that are mainly based on previously published manuscripts. Submission of a manuscript implies that the author is committed to publishing with MCJ if the manuscript is accepted. By submitting, authors attest that their work is entirely their own. Authors ensure proper acknowledgement and citation. Please read Statement of Publication Ethics for further information.

Additionally, authors wishing to publish work that has been submitted and graded as part of a University degree should make sure that their University guidelines allow publication. This sole responsibility lies with the author.

REGULATIONS FOR SUBMISSION

Mapping China regularly posts Call for Papers for the MCJ. Please refer to any conditions of those in the original Call for Papers. Additionally, Mapping China accepts submission through the online portal or after contacting info@mappingchina.org. Research papers should feature original analysis or research, include a section on theory and have a length of 6000 to 8000 words. Essays should discuss opinions on a
contemporary topic and have a length of three pages to 3000 words. Kindly include a cover page with the title of the submission, the author’s name, affiliation, email address and phone number. Additionally, kindly include a 150 to 250 words abstract for any work handed in.

PROCESS AFTER SUBMISSION

MCJ employs a double-blind peer review policy whereby research papers that pass the original in-house editorial assessment are sent to at least two expert referees for evaluation. Essays are sent to at least one expert for evaluation. Authors should therefore be careful to avoid any personal information in text or endnotes that might reveal their identity.

Authors should be prepared for multiple stages of review. First corrections might be necessary after in-house editorial assessment. Manuscripts are then either rejected before peer-review, after peer-review, accepted on the condition of revise and resubmit or accepted as is. In exceptional cases manuscripts might be accepted on condition of “rewrite and resubmit”. The whole process might take up to six months. Work that cannot be featured in the MCJ might still be published as part of the Mapping China Working Paper Series. Accepted authors for the MCJ will sign an author’s agreement with Mapping China e.V. All papers are reviewed based on their structure and coherency, theoretical quality, empirical quality, their research design and their analytical quality.

All accepted manuscripts are copyedited by MCJ for language and style. All changes will be tracked and approved by the author. The author will also receive the first galley proofs for inspection. At this stage, no changes are to be made in the text or notes, except for corrections of errors. Authors are responsible for obtaining permission from copyright holders where necessary – for example, stanzas of a poem, maps, photographs, illustrations, posters, tables, figures, or text exceeding the maximum length permitted by copyright law.

GENERAL MANUSCRIPT PREPARATION

• MCJ is using this Harvard Style Guide for citation. Please refer to it.
• Kindly use British English for texts written in English.
• Tables and figures may be included in the text and should be numerically ordered. They may contain captions.
• Any use of Mandarin Chinese is allowed and encouraged. Citation should be: pinyin in italics followed by characters followed by a direct translation in square brackets.
• Co-authored submissions are accepted. Kindly provide all authors’ details on the cover page.
• Research papers are accepted in both English and German.
• If the author is not a native English speaker, kindly ensure a high level of language
competency before submission. This means that the paper should be proofread by a native or almost-native English speaker. Papers whose arguments are not clear due to language cannot be accepted for the MCJ.

- Kindly use Times New Roman font with a text size of 12. Main titles should be in size 16, titles in size 14 and subtitles in 12. The text should be 1.5 spaced throughout. All paragraphs should be justified. Kindly only leave one space between sentences and after colons.

RESEARCH PAPER MANUSCRIPT PREPARATION

- Research Papers should have a length of 6000 to 8000 words.
- Mapping China encourages the use of qualitative and quantitative methodology. Research Papers should be theory-based, meaning that they derive their arguments and hypotheses from theory. A section on methodology or the findings of the paper should be included.
- Kindly use scientific language in all parts of the research paper.

ESSAY MANUSCRIPT PREPARATION

- Essays should have a length of minimum three pages and maximum 3000 words. Please contact info@mappingchina.org to discuss individual cases.
- Essays are arguments-based, meaning that they do not require a section on theory. Nonetheless, they should be based on current academic discourse. Essays are discussing opinions on a contemporary topic.
- The language of an essay is allowed to be more non-scientific.
- While essays are not subjected to the same level of academic requirements as research papers, authors should make sure to include a wide variety of research sources, including academic texts.

PHOTO CREDITS

Dragon in front of red background - Photo by Annie Spratt on Unsplash
Hashtag in front of pink background - Photo by Elena Koycheva on Unsplash
Globe - Photo by shuttersnap on Unsplash
Camera - Photo by Victor Garcia on Unsplash
Pedestrian Street Crossing - Photo by Ryoji Iwata on Unsplash
Skyline of Shanghai - Photo by Adi Constantin on Unsplash
Building with flagpoles - Photo by Lin Zhizhao on Unsplash
Women in front of skyline - Photo by Robert Bye on Unsplash