KEEP YOUR EYES ON CHINA'S METAVERSE: ANOTHER TOOL FOR MAINTAINING ITS NATIONAL SECURITY

Ho Ting (Bosco) Hung, London School of Economics and Political Science Hong Kong

Abstract

While many people have been discussing the security implications of the development of the metaverse from a civilian or business perspective, very few discussions analyse the implications from a national security perspective. Thus, this article contributes to the security discussions by exploring how China can make use of the metaverse to maintain stability and international influence. This article argues that the metaverse provides an immersive and integrated environment, thus, facilitating the Chinese government's spread of propaganda and invasion of the privacy of netizens accessing China's Internet. This article will discuss China's emphasis on Internet security; then, this article discusses how the metaverse assists China in influencing people's mindsets and monitoring people's behaviours. Finally, this article discusses the implication of China's metaverse on individuals. As we sail into a new era of the digital world, everyone should maintain their independent thinking and be aware of their data security to enhance their resilience to government abuses.

Introduction

We are now stepping into a new era of the Internet. The international community has devoted unprecedentedly high attention to the three-dimensional integrated virtual space, the metaverse; the technological giant, Mark Zuckerberg, for example, decided to switch the focus of his technology conglomerate Facebook to the metaverse. He also rebranded the company's name as Meta and spent billions of dollars in 2021 to invest in the metaverse (Milmo, 2021). Other multinational corporations like Gucci and Coca-Cola have also jumped on the bandwagon and sold their non-fungible tokens (NFT) on metaverse platforms like Decentraland (Kim, 2021). Foreseeing a rapid expansion of the metaverse, analysts have even estimated that the metaverse could bring a nearly US$800 billion market opportunity (Kanterman & Naidu, 2021). This could provide a valid explanation to why so many enterprises are now trying to take a slice from the market of the metaverse.

Although the metaverse is widely considered the next evolution of social connection and a golden market opportunity, the Beijing government has interestingly shown its hesitance in developing this three-dimensional virtual space (Fly & Grünberg, 2022). The Chinese National Intellectual Property Administration has repeatedly rejected metaverse trademark submissions from companies like NetEase, iQiyi, and Xiaohonshu (Sundararajan, 2022). Besides, China's state media, *Securities Times* (as cited in Shen, 2021), warned that if people "blindly invest in such grand and illusionary concepts as the metaverse, they will be burnt in the end" (para. 15).

Still, the development of the metaverse appears to be irresistible because of the great potential and market interest. Despite repeated rejections of the metaverse trademark submissions and government warnings on making investments in the metaverse, metaverse filings by the business sector continued to increase. 16,000 metaverse-related trademark applications have been filed (Sundararajan, 2022), and extensive investments in the metaverse have been made (Baughman, 2022). Not only does the business sector find the market of the metaverse attractive, but the Chinese government has also recognised the potential of the metaverse. For instance, the Ministry of Industry and Information Technology has declared its interest in nurturing small-medium sized enterprises to enter the metaverse market to promote market digitalisation (Zhou, 2022). On a local level, the Shanghai Municipal Commission of Economy and Information Technology released the *14th Five-Year Plan for the Development of the Electronic Information Industry*, which considers the metaverse as one of four frontiers for exploration (Cheng, 2021; Nie, 2022). Other local governments like Hebei and Wuhan have also followed and made similar plans, while some governments also held seminars and discussions to speed up the development of the metaverse (Fly & Grünberg, 2022). China is, therefore, now making a greater engagement with the development of the metaverse.

While it appears that the metaverse is an online platform mainly for business or entertainment use, the metaverse does contain strategic value. Therefore, the international community cannot neglect the security implications of China's metaverse development, especially when China has increasingly voiced its concerns about Internet security in recent years. This can be seen by the case of the former General Secretary of the Chinese Communist Party, Hu Jintao, when he said,

> We do not merely want to focus on and safeguard the security of our territorial land, sea, and airspace. We also want to focus on and safeguard our security on the seas, in space, [and] in *cyberspace*, as well as the other dimensions of our national security. (Hu, 2004, as cited in Tanner & Mackenzie, 2015, emphasis added, p. 1)

Meanwhile, most people discuss the security implications of the metaverse from a business and technological perspective regarding civilian or corporate use (Amirulloh & Mulqi, 2022; Bogost, 2021; Deutsch et al., 2021; Hackl, 2020; Lloyd, 2021; Milmo, 2021; Regalado, 2021; Ravenscraft, 2022), instead of a political perspective regarding national use; therefore, the role of the metaverse in China's politics is not yet clearly examined. Also, to the best of my knowledge, there are limited attempts in linking the development of China's metaverse to China's past policies in maintaining security. This article, therefore, contributes to the discussion of cyber security by addressing how China's metaverse development can pose a risk to people's privacy, data, and thinking. Since the metaverse provides an immersive environment, China could utilise this platform to track individuals and spread its propaganda. Individuals should, therefore, be aware of their data in China's metaverse and always be critical and careful when receiving information when using China's metaverse.

This article starts by defining what the metaverse is and explaining what technologies or equipment could be involved in the metaverse. This provides a foundation for justifying how the metaverse could influence security in the following sections. The second section of this article explains China's emphasis on Internet security, thus justifying why the metaverse could become an arena for it to maintain national security. The third section of this article discusses how the metaverse could facilitate the spread of pro-China messages and influence people's mindsets. The fourth section of this article explores why China could use the metaverse to maintain its political security; this explains why users' privacy could be threatened in China's metaverse. Finally, this article draws on the previous sections to discuss the implications on individuals who could be exposed to China's metaverse. It concludes that we should stay alert about China's metaverse development because it can be a tool for China to maintain its national security. We should all enhance our resilience to prevent our mindsets from being unconsciously distorted by China's propaganda and prevent our data from being abused.

What is the metaverse?

Surprisingly, despite the global hype about the virtual space in recent years, the idea of the metaverse is rather old (Knox, 2022); the term metaverse was coined by Neal Stephenson (1992) in his science fiction novel *Snow Crash* as a portmanteau of "meta" and "universe." Subsequently, this term was used to describe a range of virtual world technologies and some large-scale multiplayer online role-playing games (Knox, 2022). At this stage, metaverse, however, simply represented an idea of a virtual world platform which was mostly related to online games. It is therefore understandable that the global community and firms were not excited to develop the "metaverse" at the time.

Nonetheless, with the development of virtual and augmented technologies, opportunities have arisen for technological firms to connect the virtual world with the real world using the metaverse with new technologies. Corporations realise how a parallel community to the physical world could encourage instant interactions and immersive experiences, thus changing the future of media, entertainment, socialisation, and business models. Recognising the huge business potential of the metaverse, more and more enterprises are eager to lead the development of the metaverse. In short, the metaverse, in the contemporary sense, could be framed as a three-dimensional shared virtual environment where people could connect, interact, and collaborate with others through virtual avatars in real time without being limited by geographical boundaries (Amirulloh & Mulqi, 2022; Kim, 2021).

To realise a seamless artificial connection between the physical world and the artificial world, technologies like virtual reality (VR) and augmented reality (AR) technology, sensors, holograms, and other equipment would be needed to create a more immersive user experience or mimic real interactions (Bogost, 2021; Di Pietro & Cresci, 2021; Rickli & Mantellassi, 2022). Besides digital assets or currencies, relevant technologies like NFTs have to be developed to facilitate payment and create a digital economy in the metaverse (Amirulloh & Mulqi, 2022; Nahar, 2022; Ravenscraft, 2022). These allow users to have a more immersive digital experience and a stronger connection with the virtual community.

China's Concern over Internet Security

In this section, I turn to discuss China's concerns over the Internet and its past measures used for controlling the online community so as to lay a foundation for the discussion on information restriction and surveillance in the metaverse in subsequent sections.

As an autocratic country, China has always been strongly concerned about its national security and the party's control over the country (Wuthnow, 2017). The Chinese government has also increased its mention of national security over time and it has explicitly stressed the country must defend its national unity, social stability, and party leadership (Tanner & Mackenzie, 2015). Nonetheless, the spread of foreign ideas like democracy, capitalism, and human rights could influence people's thinking and may induce them to overthrow communist rule to build up a Western system; opening up China to foreign countries can facilitate the spread of such thoughts, so this is unfavourable to the ruling party in the political sense. As Deng Xiaoping famously said, "If you open the window for fresh air, you have to expect some flies to blow in" (as cited in MacKinnon, 2008, p. 32). The Chinese government does recognise the potential adverse effects brought by connecting its country with the world in its rule.

The anxiety over the inflow of foreign ideas and ruling instability has been deepened by the introduction of the Internet because the exchange of information is no longer limited by time and geographical boundaries. It has become easier for people to discuss social issues and mobilise other people to participate in collective actions by launching campaigns or producing content with a few clicks on the keyboard and mouse (Chi, 2012; Qiang, 2019). Therefore, the Internet gives rise to the risk that the Chinese people can freely criticise the government, receive information about democracy, and become discontented with communist rule (Dong, 2012). Nevertheless, the Internet could also help China access foreign market information and build an international business network, which is vital to its economic development. Since China has to maintain its economic connections with the world to boost its competitiveness, it has no choice but to bring the Internet to China (MacKinnon, 2008). To maintain its national security and avoid the infiltration of these "flies," China, therefore, has to regulate and monitor the online world.

Regulations

First, China has explicitly issued regulations to govern the use of the Internet. The most remarkable one is the Computer Information Network and Internet Security, Protection and Management Regulations established in 1997. Section Four of Chapter 1 of the regulations clearly specifies that "[n]o unit or individual may use the Internet to harm national security, disclose state secrets, harm the interests of the State, of society or of a group, the legal rights of citizens, or to take part in criminal activities" (U.S. Embassy Beijing, 1998, as cited in Federation of American Scientists, n.d., para. 12).

Section Five further expands the prohibition of content that can be posted online:

(1) Inciting to resist or breaking the Constitution or laws or the implementation of administrative regulations;

(2) Inciting to overthrow the government or the socialist system;

(3) Inciting division of the country, harming national unification;

(4) Inciting hatred or discrimination among nationalities or harming the unity of the nationalities;

(5) Making falsehoods or distorting the truth, spreading rumors, destroying the order of society;

(6) Promoting feudal superstitions, sexually suggestive material, gambling, violence, murder[;]

(7) Terrorism or inciting others to criminal activity; openly insulting other people or distorting the truth to slander people;

(8) Injuring the reputation of state organs;

(9) Other activities against the Constitution, laws or administrative regulations. (U.S. Embassy Beijing, 1998, as cited in Federation of American Scientists, n.d., paras. 14-22)

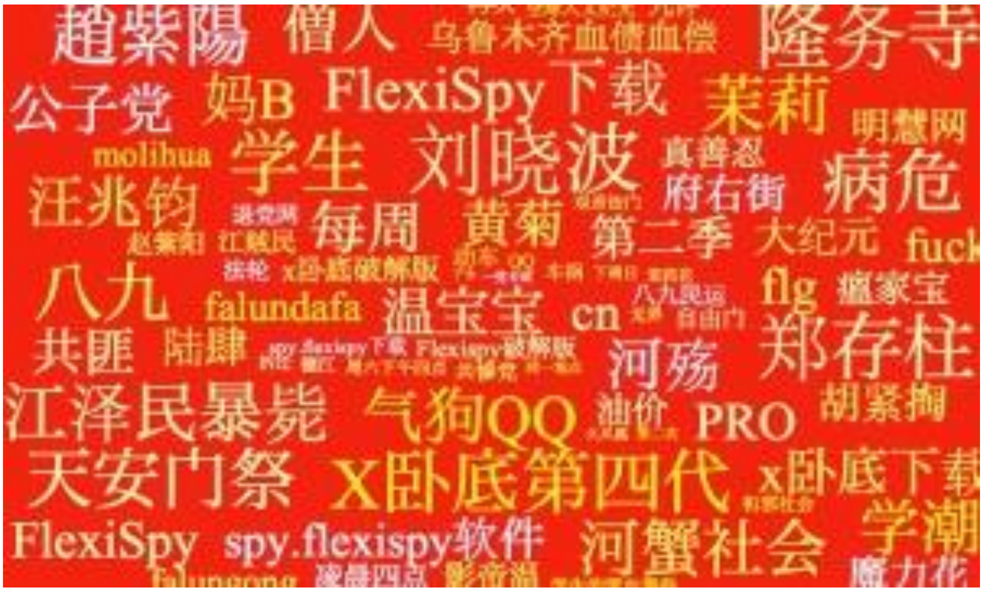
Accordingly, internet users cannot post, share, or discuss politically sensitive issues that could harm national or party interests. Otherwise, they can be made legally responsible for the publication (Chi, 2012). This has therefore laid a legal framework for the restriction of the use of the Internet, which also facilitates the future expansion of government control over the virtual community.

Automated Filtering Software

Second, China has widely used automated filtering software to remove anti-government content or content with offensive or politically sensitive keywords (敏感詞) in emails or on online forums (Endeshaw, 2004; Herold, 2018; Zhu & Fu, 2021). As discussed, the Internet facilitates timely discussions, so netizens could easily come together and discuss social issues. With the inflow of foreign information, the Chinese people could know more about the problems in China and may want to discuss or express their thoughts on these issues. To suppress these discussions or criticisms, China decided to use an effective mechanism: filtering posts containing certain keywords automatically; for example, posts containing words like “Falun Gong,” “Tiananmen incident,” and “Tibetan independence” are automatically removed (MacKinnon, 2008, p. 41). With such tight control over the Internet, China’s Internet has become a separate network from the global one (Brown, 2022; MacKinnon, 2008). The Chinese online community is filled with pro-China messages, whereas foreign ideas and anti-China content are filtered.

Figure 1

A cloud of sensitive words



Source: Museum Fatigue (2013)

Internet Police and Monitors

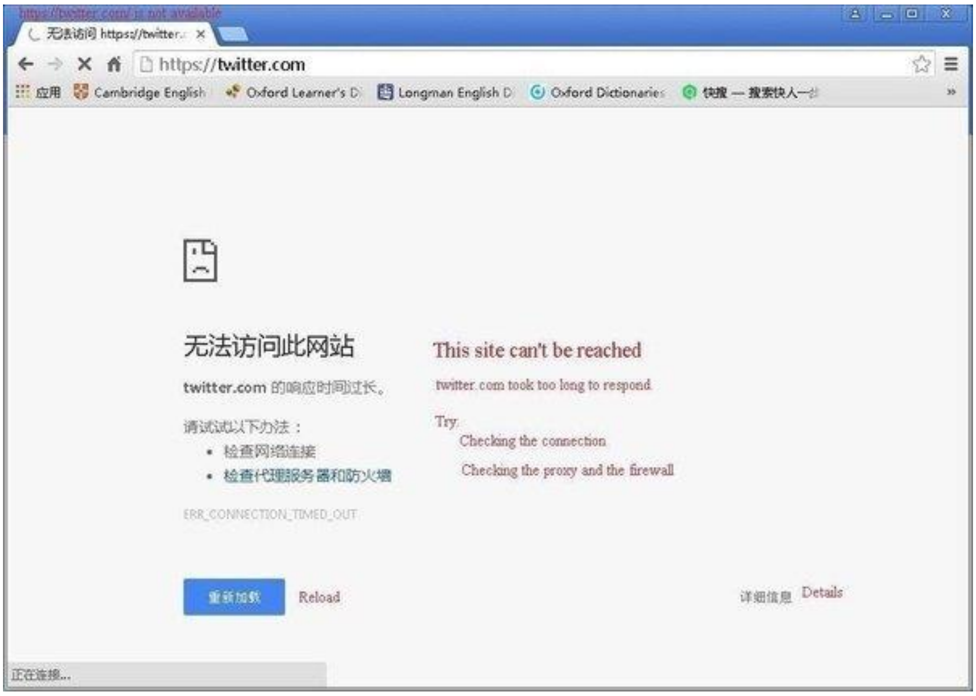
Third, China has established a team of Internet police and monitors to track netizens, monitor their behaviours, and impose punishments on critics of the government. While filtering software can help remove anti-China posts, it cannot deter people from posting such content; China needs another measure with a great deterrent effect in discouraging people from criticising the government. Therefore, the government closely monitors internet activities and tracks critics of the government using the Internet police, employed individuals, big data, and internet tools and services (Herold 2018; Qiang, 2019). The public security forces also leverage other established surveillance systems like DNA, voice and image recognition, and closed-circuit television to monitor the daily activities of these people (Dong, 2012; Qiang, 2019), then, the internet police will harass, arrest, and interrogate these anti-government forces (Endeshaw, 2004). A good example of this is when, in 2015, an 81-year-old writer was sentenced to jail because he wrote online essays to criticize the government (Wee, 2015). Besides, from 2014, the government has required users to register their accounts on video-sharing websites, instant messaging services like Weibo and WeChat, and other services; this allows the government to identify users and trace their digital footprint more easily (Herold, 2018). Accordingly, people are deterred from producing or spreading content unfavourable to government rule.

Cutting Netizens' Access to Certain Foreign Websites

Fourth, China has cut netizens' access to certain foreign websites. While China could remove anti-China content produced in its country and deter its people from producing such content, it could not control people outside its territory (Anderson, 2012). Therefore, the Chinese government has built the Great Firewall to block foreign websites by blocking IP (Internet Protocol) addresses, stopping the TCP (Transmission Control Protocol), injecting a fake DNS (Domain Name System) reply, and terminating HTTP (Hypertext Transfer Protocol) requests (Anderson, 2012; Ensafi et al., 2015). Notably, since June 1, 2014, Chinese netizens were no longer able to access Google, thus cutting the most direct access to the West (Zheng & Wang, 2020). Social media sites like Facebook and Twitter are also not accessible in China (Brady, 2017). This helps prevent Chinese people from accessing unfavourable foreign information, thus containing the spread, discussion, and exchange of foreign ideas.

Figure 2

Connections are reset when users try to access blocked sites



无法访问此网站

twitter.com 的响应时间过长。

请试试以下办法：

- 检查网络连接
- 检查代理服务器和防火墙

ERR_CONNECTION_TIMED_OUT

This site can't be reached

twitter.com took too long to respond

Try:

Checking the connection

Checking the proxy and the firewall

Source: Jeff Rajeck – Econsultancy (2017)

Producing Propaganda

Fifth, the government does not only make efforts in containing the spread of anti-China information, but it also actively produces pro-China propaganda to strengthen national unity and promote China on the Chinese Internet; China has been relying on its party media like People's Daily to mobilise support for the ruling party (Brady, 2017; Su, 2019). With the rise of social media, China turns to employing individuals to form an army of commentators, who are the so-called 50-cent Party or 50-cent Army (五毛黨, wumaodang), to leave pro-government comments and spread nationalist sentiment (Bolsover & Howard, 2019; Brady, 2017). This has manipulated public opinion and helped gather support for the government, thus maintaining social stability.

Summary

As reflected by the above measures, China has built up comprehensive infrastructures and strategies to manipulate information and defend its national security in the online sphere. Freedom of speech is absent in China's online community, while pro-government opinions are the dominating ones. Discussions are confined to politically insensitive or politically correct topics, whereas discussions that could jeopardise the ruling stability are suppressed.

Using Metaverse to Influence Your Mind

As shown by the second section, China has been extremely cautious about the influence of the internet on people's minds. In fact, in recent years, China has been eager to become an "Internet power" (网络强国), build an "online civilisation" (网络文明), and defend the Internet as a "spiritual home" (精神家园) of the Chinese citizens (Wang & Yu, 2021). This reflects that the Chinese government has considered the online community an important component in shaping people's minds (Baughman, 2022). China does not hesitate to make use of virtual tools to create a stronger sense of belonging or improve its reputation to enhance its international discourse power. By applying this logic, the metaverse will become another tool for it to exert its influence over its people and the international audience.

Censorship

As reflected by the first section, the metaverse is a strong virtual network breaking down time and geographical boundaries to connect people. This, however, also means that people of different countries, cultures, values, and thinking could come into each other quickly and easily (Amirulloh & Mulqi, 2022). Rapid exchange of ideas could, therefore, take place on the metaverse between Chinese citizens and the international community. The Chinese government, however, will not like to see such exchanges happening because Chinese citizens could absorb or even accept more foreign information or knowledge. This would threaten its national security and shake its political stability as it was demonstrated in the second section. Considering China's strong concern about national security, the Beijing government will surely impose tight control over the metaverse. Similar censorship on the Internet will be introduced to the metaverse to avoid the spread of anti-government messages (Gandolfo & Hamilton, 2022). Therefore, China's metaverse will be an isolated metaverse, having limited connections with foreign metaverses.

Manipulating Information and Controlling Thoughts

We also need to recognise that the metaverse provides a powerful tool for the government to manipulate information and control people's thoughts. Humans understand the world and persuade others by leveraging stories, speeches, and symbols (Jobson & Hartley III, 2022). If the information contains emotional content, for instance, inducing people's nationalist sentiment by exaggerating China's economic success or foreign bullying behaviours of sanctions, then people will be less rational in analysing and reacting to the sources (Zhuravskaya et al., 2020); it is easier to influence their minds. The metaverse provides an immersive digital experience that deepens and extends experiences; therefore, fostering such persuasion. For example, the metaverse adopts 3D graphics and is supported by VR headsets, AR glasses, or even holograms that can enhance the visual experience and provide multi-sensory feedback (Deutsch et al., 2021; Di Pietro & Cresci, 2021; Robertson & Peters, 2021). People do not only receive static images or texts, but they also engage in vibrant interactions to access and exchange information. This could make the messages and interactions richer and more fascinating, as well as reinforce the emotional elements, thus facilitating the manipulation of people's thoughts.

Interconnected Network

Moreover, the metaverse offers a synchronous environment facilitating timely interactions, where users feel that they are close to other people instead of being separated by miles (Newton, 2021). With a strong network between individuals in the three-dimensional virtual space, the spread of propaganda will also become faster and more efficient (Rickli & Mantellassi, 2022). Therefore, users will be exposed to, and interact with, pro-government content more frequently, thus confirming pro-government thoughts and isolating anti-government users (Mølmen & Ravndal, 2021). This could trap people in a pro-China sphere and unconsciously influence people's mindsets more effectively. Therefore, as Rickli and Mantellassi (2022) argue, "state-run disinformation campaigns and propaganda would therefore also become more powerful. States could therefore utilise metaverses to manipulate behaviours and alter users' norms to their (i.e. states') advantage" (p. 9).

Echo-chamber Phenomenon

Such manipulations are further reinforced by the echo chamber phenomenon under the aforementioned censorship. Censorship filters out anti-government information and forcefully feeds the users with pro-government content only repeatedly. Netizens are also unable to communicate with people holding anti-government views within the Chinese metaverse. This could gradually "brainwash" users into believing that supporting the government is the prevailing trend, thus shaping their thoughts that they should support the government as well. An echo chamber is subsequently formed under which people repeatedly consume pro-government information only, strengthening their pro-government beliefs (Mølmen & Ravndal, 2021; Wang & Qian, 2021). Since people hold confirmation bias, which means they tend to accept and consume information conforming to their beliefs, they will continue to select pro-government information (Jobson & Hartley III, 2022; Zollo et al., 2017). Meanwhile, with the declining exposure to anti-government information, people will also become more reluctant to access information criticising the government. A cycle would be then formed under which people consume more pro-government content and less anti-government content. A metaverse with censorship could, therefore, push people to only one side of the political spectrum, which is becoming extremely pro-government.

Effects

From the above, we can see that the metaverse can act as a powerful tool for China to maintain its national security by disseminating and manipulating pro-China messages; the metaverse complements past efforts in maintaining internet security to strengthen national unity and obedience to the party. People have very limited opportunities to access information criticising the ruling party, while their exposure to pro-government propaganda increases in the metaverse. The metaverse also reinforces the effectiveness of propaganda by creating an immersive and memorable user experience; therefore, the metaverse can help the Chinese government strengthen its national cohesion and maintain its control over the country.

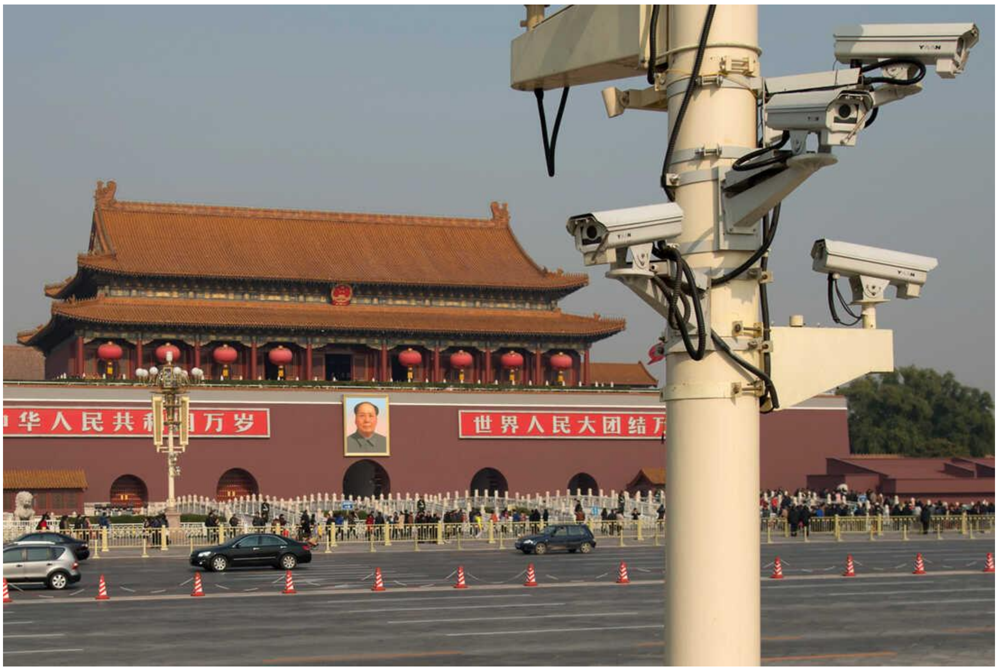
Moreover, the development of China's metaverse can also have an impact on external aspects because it is not only used by Chinese citizens but also by the international community. Considering the metaverse's strong power in manipulating thoughts, China will use the metaverse to carry out its expansion and achieve its ideological ambitions in the virtual world (Gandolfo & Hamilton, 2022). By spreading propaganda repeatedly, foreign visitors can be influenced to learn more about China, embrace Chinese values, or hold a more pro-China stance (Edney, 2012). China can also utilise the metaverse to display interactive content or fake information to emphasise or exaggerate China's strengths, national power, and values (Honrada, 2022), particularly, China possesses a large number of cultural relics and has a long history, which are attractive to the international audience (Edney, 2012; Fliegel & Kříž, 2020; Zhu, 2022). The Chinese government can use the metaverse to produce appealing content to promote its culture and history, and thus, enhance its popularity in other countries. For example, China can display the picturesque views of Jiuzhaigou (九寨溝), play birds' humming voices, and create the smell of flowers there to provide multi-sensory content to stress the beauty of China's natural environment. This would help capture foreigners' hearts and minds, thus improving China's image and enhancing its soft power; this way, the metaverse can help China build up a pro-China force in foreign countries and facilitate its subsequent expansion in both the virtual and real world.

Secretly Collecting Your Data

To maintain its control over citizens, apart from using disinformation and propaganda, China has also collected people's sensitive data and carried out mass surveillance. In 2005, the Chinese government began establishing a CCTV (closed-circuit television) surveillance system called the Skynet Project (天网工程) (Feldstein, 2021). Later in 2015, China initiated the Sharp Eyes project (锐眼工程) to further expand the coverage of CCTV surveillance and facial recognition technologies which were widely incorporated into the surveillance network (Qiang, 2019). In 2019, more than 200 million monitoring CCTV cameras were installed in China, which is 300% higher than the number of CCTV cameras deployed in the United Stated (Feng, 2019). Besides facial recognition, China also actively develops voice-recognition surveillance; the Ministry of Public Security collaborates with a local company iFlytek to develop voice-recognition software for *stability maintenance* (Qiang, 2019). The Chinese government also launched an extensive programme of building up a DNA database for surveillance and repression, especially for racial minorities like Uighurs in Xinjiang (Qiang, 2019; Cyranoski, 2020). Last but not least, in 2014, China launched the notorious Orwellian project of establishing a Social Credit System (社會信用體系) to induce its citizens to behave according to national interests. People’s behaviours like political activities, socialization, and purchase history are recorded and they affect their credit scores (Wong & Dobson, 2019). People’s credit scores can affect the outcome of their applications for financial services, personal loans, jobs, visas, hotel rooms, schools, etc. (Ding & Zhong, 2021; Kostka, 2019; Qiang, 2019); well-behaving citizens (in the government’s eyes) can enjoy benefits like being able to book a hotel room without leaving a cash deposit (Hatton, 2015), and poorly-behaved citizens (in the government’s eyes) can risk facing a travel ban (Ding & Zhong, 2021). In short, people’s personal data are no longer a “secret” to the government. The Chinese government has been infringing people’s privacy and data security by expanding its surveillance network.

Figure 3

Security cameras in Beijing



Source: Frank Langfitt – NPR (2013)

Figure 4

Zhima Credit of Alibaba's Ant Financial

Source: Rene Raphael and Ling Xi – The Nation (2019)

Meanwhile, the development of the metaverse deepens such concerns. This is because the metaverse's nature inevitably makes data easily traceable. While physical interactions are not quantified as numbers of data, interactions on the metaverse could be converted into statistical information because they are virtual (Rickli & Mantellassi, 2022). We can also use sensors, headsets, or other equipment to record the data for quantification. The government can then monitor and evaluate the data to exercise its control over its people (Cheung & Chen, 2021).

Admittedly, it takes time to develop such quantifying and sensory technologies to a sophisticated level and incorporate them into metaverse use. Particularly, brain-reading is a complicated matter which mankind only knows little about it (Regalado, 2021). However, we cannot ignore the effect of a sharp rise in investment in relevant technologies in recent years to the development of the metaverse. Therefore, in the future, the Chinese government could possibly collect behavioural data of its citizens or other Internet users on the metaverse for political purposes like mass surveillance, which has been carried out for years.

Tracking Expressions, Body Movements, and Brain Activity

First of all, the metaverse would allow the Chinese government to track people's expressions, body movements, and brain activity, thus monitoring people's political thoughts and activities. The metaverse heavily relies on headsets, goggles, sensors, and other equipment to create an immersive and personalized digital experience. These types of equipment, however, could allow the government to track people's body movements and physiological responses to stimuli. For example, headsets and sensors can monitor users' brain activity and read brain waves, while goggles can track eye movements to evaluate one's engagement with the information (Di Pietro & Cresci, 2021; Hamilton, 2022; Regalado, 2021; Rickli & Mantellassi, 2022). These feedbacks could provide information on a person's attention span, interests, concerns, and priorities. In addition, sensors can detect one's finger and facial movements (Ghaffary, 2021; Hamilton, 2022). By recording and analysing one's projection of voice and its tone, we can also know one's personality or attitude (Fly & Grünberg, 2022), such body language, facial expressions, and characteristics of voices reflect one's emotional state; therefore, showing one's views on the displayed issues. Applying this in politics, the government could know whether a person is concerned about political information, or whether the person has a specific attitude towards certain political matters. It could also be use the collected data to adapt the information to feed users with moderated content so as to control their mind.

Language

Second, China can use the metaverse to analyse people's use of language in their interactions, thus monitoring people's political stances. Apart from analysing one's tone and body language using sensors, we can also obtain one's view on an issue by examining the language used in verbal messages (e.g. voice recordings or live broadcasts) or text messages. The metaverse provides a digital platform for people to express themselves or interact with others, so inevitably, it processes or stores data about people's use of language (e.g. in their social media posts, voice messages, and interactions between people on the metaverse). The government can use artificial intelligence or automated software to extract some anti-government or politically sensitive keywords. The Chinese government could then identify potential rivals or opposition forces using the metaverse so that it can carry out timely interventions to repress these anti-government individuals or groups.

Stalking people

Third, China can use the metaverse to analyse people's consumption and socialising behaviour, thus knowing people's interests and values; in the physical world, it is time-consuming and costly to spy or stalk people because physical constraints exist. Stalkers have to stay close to their targets, follow them, and travel to different locations (Di Pietro & Cresci, 2021); however, the online world makes tracking much easier (Deutsch et al., 2021). Particularly, the metaverse establishes an interconnected economy and community, which records more data and makes it traceable. Through monitoring one's digital assets and purchases in online stores, the government can identify one's consumption habits. Through tracking one's behaviour in socialisation and social media, the government can know more about users' social circles. Therefore, China could track one's daily life more easily on the metaverse and grasp a more comprehensive understanding of one's habits, thus also facilitating the implementation of the Social Credit System for pressuring people to comply with national interests. For instance, the government can know whether a person supports products made in China or boycotts products produced by firms complying with Western sanctions; people's privacy thus becomes vulnerable in the metaverse.

Physiological characteristics

Fourth, the metaverse can help China collect personal information on one's physiological characteristics, thus facilitating surveillance. The equipment, such as headsets or sensors, used to support metaverses collects users' biometric data: heartbeat rates, facial features, and vocal features. By collecting and processing people's biometric data, the government could obtain more information on the digital representation of one's physiological characteristics. This provides more training data for machine learning to facilitate the identification of individuals in both the physical and virtual community (e.g. facial recognition or voice recognition). Together with the aforementioned political data collected on the metaverse (e.g. tone, language), it becomes easier for the government to identify and capture individuals with an anti-government stance, thus contributing to a strengthened surveillance network.

Summary

In essence, one must bear in mind that China has built a long-standing and invasive state surveillance system of massive scale. Since the metaverse facilitates the gathering of information, it can end up becoming a tool for expanding the surveillance system and exacerbate the gross invasion of privacy and data security. No matter whether we are chatting with our friends, shopping in online stores, or discussing business projects with our clients, all of our activities in the digital sphere can be watched by the government. Even if we are just yawning or stretching our body in front of the sensor, the government can also creepily monitor our body movements. Thus, in China's metaverse, every netizen will be put under surveillance, and privacy will become empty words.

Implication on individuals

As shown by the previous sections, everything individuals read or come across in the Chinese metaverse may be fabricated or only reflect a part of the truth to mobilise support for China. Users should, therefore, acknowledge the risk that China can possibly use the metaverse to distort people's understanding of China and reactions to the country's behaviour, thus shaping users as a pro-China force, which voluntarily and eagerly spreads pro-China messages or carries out pro-China actions. Since the metaverse facilitates a distortion of cognitive abilities, we can hardly rely on our individual cognitive abilities or critical thinking to analyse information or make decisions, especially in China's metaverse (du Cluzel, 2020). Therefore, individuals, regardless of being a Chinese citizen or not, must remain extremely cautious when they connect themselves with China's fascinating yet dangerous three-dimensional space.

Meanwhile, the level of distortion depends on how resilient we are when receiving biased information. To prepare for confronting disinformation on the metaverse, netizens must sharpen their resilience to cognitive distortion. We have to develop an ability to collect information from multiple sources to identify fake information. This helps us obtain diverse viewpoints and prevent ourselves from falling into the trap of manipulated content (West, 2017) It is also of utmost importance for us to remain calm when receiving content that is misleading, spreads rumours, or aims to trigger our emotions by using offensive language. Even if the source provides fascinating graphics or involves motivating language, we have to keep in mind that the information may not be credible, so we should still strive to analyse the information critically.

Admittedly, it is insurmountably difficult to perfectly distinguish a scarce piece of true news from a sea of fake news, especially when the government is the creator instead of the regulator. However, the more fake news we avoid consuming, the less likely our perception of issues will be distorted. Thus, individuals should persevere to fight against manipulated content on China's metaverse, which is strictly censored and monitored by the government authority.

The same principle applies to privacy and data security. China can be secretly collecting our personal information on the metaverse, so we should stay alert to what information can be stored in the online community. If the metaverse platforms explicitly ask for our consent to submit certain personal information or biometric data, we have to think about whether it is necessary. For instance, if a metaverse platform asks us to submit our brain activity to analyse our emotions to enhance our user experience, we may consider rejecting the request to safeguard our privacy. Even if such measures cannot completely protect us from data theft or infringement by the government, at least we are minimising the amount of unnecessary sensitive data we submit to the government for unlawful or unjust purposes like surveillance.

Conclusion

This article has attempted to link the development of the metaverse to China's past policies in maintaining national security so as to demonstrate that China can build up a metaverse to serve its own national interests. Considering China's strong emphasis on Internet security, this article predicts that censorship and surveillance could be introduced to the three-dimensional community to construct a metaverse with Chinese characteristics. Our mindsets are susceptible to the Chinese government's intervention, while everyone's behaviour is closely monitored. People's independent thinking and privacy are, therefore, at risk in China's metaverse. As a result, this article aims to warn the general public to be careful when accessing China's metaverse to avoid getting abused.

This article, however, has some inherent limitations that need further enquiry and research. I acknowledge that China’s metaverse development is still at a beginning stage, so guidelines or policies were still absent at the time of writing. Currently, there is no evidence justifying that China has decided or expressed its intention to use the metaverse as a tool for maintaining its national security. More investigations are needed to examine China’s political intention in developing the metaverse. Besides, this article mainly relies on theoretical discussions on cognitive abilities and the metaverse. It is hoped that more in-depth neuroscientific and psychological empirical research can be conducted to understand how significantly an immersive digital experience in a metaverse can distort one’s understanding of an issue.

Nonetheless, this article aims to explore the possibility that China can use the metaverse for malicious purposes. Instead of calling for a halt to the development of the metaverse or opposing this ground-breaking technological development completely, this article aims to serve as an alert that the international community must keep its eyes on the development of China’s metaverse and relevant security issues. Although it takes time to develop a metaverse and relevant technologies, it is time for us to pay attention to their development and voice out our concerns about their security problems. As we sail into a new digital era, individuals must also maintain independent thinking and be aware of their data security to prepare for any challenges brought by immersive and interconnected digital experiences on their mind and security.

References

Amirulloh, M. F. N., & Mulqi, M. (2022). Know more metaverse as the technology of the future. *International Journal of Research and Applied Technology (INJURATECH)*, *2*(1), 174-177. https://doi.org/10.34010/injuratech.v2i1.6915

Anderson, D. (2012). Splinternet behind the Great Firewall of China: Once China opened its door to the world, it could not close it again. *Queue*, *10*(11), 40-49. https://doi.org/10.1145/2390756.2405036

Baughman, J. (2022). Enter the battleverse: China's metaverse war. *Military Cyber Affairs*, *5*(1), Article 2. https://digitalcommons.usf.edu/mca/vol5/iss1/2

Bogost, I. (2021, October 21). The metaverse is bad. *The Atlantic*. https://www.theatlantic.com/technology/archive/2021/10/facebook-metaverse-name-change/620449/

Bolsover, G., & Howard, P. (2019). Chinese computational propaganda: Automation, algorithms and the manipulation of information about Chinese politics on Twitter and Weibo. *Information, Communication and Society*, *22*(14), 2063-2080. https://doi.org/10.1080/1369118X.2018.1476576

Brady, A-M. (2017). Plus ça change? Media control under Xi Jinping. *Problems of Post-Communism*, *64*(3-4), 128–140. https://doi.org/10.1080/107p58216.2016.1197779

Brown, T. (2022, March 4). Metaverse fever is high in China. Regulators are watching. *Barron's*. https://www.barrons.com/articles/china-metaverse-regulators-51646356278?tesla=y

Cheng, E. (2021, December 31). *Shanghai doubles down on the metaverse by including it in a development plan.* CNBC. https://www.cnbc.com/2021/12/31/shanghai-releases-five-year-plans-for-metaverse-development.html

Cheung, A. S. Y., & Chen, Y. (2021). From datafication to data state: Making sense of China's social credit system and its implications.

Law & Social Inquiry, *00*(00), 1–35. http://doi.org/10.1017/lsi.2021.56

Chi, E. (2012). The Chinese government's responses to use of the internet. *Asian Perspective*, *36*(3), 387–409. http://www.jstor.org/stable/42704798

Cyranoski, D. (2020, July 7). China's massive effort to collect its people's DNA concerns scientists. *Nature*. https://doi.org/10.1038/d41586-020-01984-4

Deutsch, J., Nix, N., & Kopit, S. (2021, December 15). Misinformation has already made its way to the metaverse. *Bloomberg*. https://www.bloomberg.com/news/articles/2021-12-15/misinformation-has-already-made-its-way-to-facebook-s-metaverse

Ding, X., & Zhong, D. Y. (2021). Rethinking China's social credit system: A long road to establishing trust in Chinese society. *Journal of Contemporary China*, *30*(130), 630-644. https://doi.org/10.1080/10670564.2020.1852738

Di Pietro, R., & Cresci, S. (2021). Metaverse: Security and privacy issues. *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 281-288. https://doi.org/10.1109/TPSISA52974.2021.00032

Dong, F. (2012). Controlling the internet in China: The real story. *Convergence: The International Journal of Research into Media Technologies*, *18*(4), 403–425. https://doi.org/10.1177/1354856512439500

du Cluzel, F. (2020). *Cognitive warfare*. Innovation Hub. https://www.innovationhub-act.org/sites/default/files/2021-01/20210113_CW%20Final%20v2%20.pdf

Edney, K. (2012). Soft power and the Chinese propaganda system. *Journal of Contemporary China*, *21*(78), 899-914. https://doi.org/10.1080/10670564.2012.701031

Endeshaw, A. (2004). Internet regulation in China: The never-ending cat and mouse game1. *Information and Communications Technology Law*, *13*(1), 41-57. https://doi.org/10.1080/1360083042000190634

Ensafi, R., Winter, P., Mueen, A., & Crandall, J. R. (2015). Analyzing the Great Firewall of China over space and time. *Proceedings on Privacy Enhancing Technologies*, *2015*(1), 61-76. https://doi.org/10.1515/popets-2015-0005

Federation of American Scientists. (n.d.). *New PRC Internet Regulation.* Retrieved May 31, 2022, from https://irp.fas.org/world/china/netreg.htm

Feldstein, S. (2021). *The rise of digital repression: How technology is reshaping power, politics, and resistance.* Oxford University Press. https://doi.org/10.1093/oso/9780190057497.001.0001

Feng, C. (2019, December 9). China the most surveilled nation? The US has the largest number of CCTV cameras per capita. *South China Morning Post*. https://www.scmp.com/tech/gear/article/3040974/china-most-surveilled-nation-us-has-largest-number-cctv-cameras-capita

Fliegel, M., & Kříž, Z. (2020). Beijing-Style soft power: A different conceptualisation to the American coinage. *China Report*, *56*(1), 1-18. https://doi.org/10.1177/0009445519895615

Fly, Y. J., & Grünberg, L. (2022, March 30). What will China's metaverse look like? *The Diplomat*. https://thediplomat.com/2022/03/what-will-chinas-metaverse-look-like/

Gandolfo, R., & Hamilton, M. (2022, April 13). *How China will censor the metaverse.* SupChina. https://supchina.com/2022/04/13/how-china-will-censor-the-metaverse/

Ghaffary, S. (2021, November 24). *Why you should care about Facebook's big push into the metaverse.* Vox. https://www.vox.com/recode/22799665/facebook-metaverse-meta-zuckerberg-oculus-vr-ar

Hackl, C. (2020, August 2). Now is the time to talk about ethics and privacy in the metaverse. *Forbes*. https://www.forbes.com/sites/cathyhackl/2020/08/02/now-is-the-time-to-talk-about-ethics--privacy-in-the-metaverse/?sh=45a4a8c1ae6c

Hamilton, I. A. (2022, January 18). *Meta wants to track your eye movements and facial expressions as you roam the metaverse, patents suggest.* Business Insider. https://www.businessinsider.com/meta-metaverse-patents-track-eye-movement-facial-expressions-facebook-zuckerberg-2022-1?r=US&IR=T

Hatton, C. (2015, October 26). *China 'social credit': Beijing sets up huge system.* BBC News. https://www.bbc.co.uk/news/world-asia-china-34592186

Herold, D. K. (2018). Xi Jinping’s internet: Faster, truer, more positive and more Chinese? *China: An International Journal*, *16*(3), 52-73. https://muse.jhu.edu/article/703440

Honrada, G. (2022, April 21). *US, China race to militarize the metaverse.* Asia Times. https://asiatimes.com/2022/04/us-china-race-to-militarize-the-metaverse/

Jobson, K. O., & Hartley III, D. S. (2022). Achieving cognitive warfare superiority amidst accelerating change. *Phalanx*, *55*(1), 28–31. https://www.jstor.org/stable/27116806

Kanterman, M., & Naidu, N. (2021, December 1). *Metaverse may be $800 billion market, next tech platform.* Bloomberg. https://www.bloomberg.com/professional/blog/metaverse-may-be-800-billion-market-next-tech-platform/

Kim, J. (2021). Advertising in the metaverse: Research agenda. *Journal of Interactive Advertising*, *21*(3), 141-144. https://doi.org/10.1080/15252019.2021.2001273

Knox, J. (2022). The metaverse, or the serious business of tech frontiers. *Postdigital Science and Education*, *4*, 207-215.

https://doi.org/10.1007/s42438-022-00300-9

Kostka, G. (2019). China’s social credit systems and public opinion: Explaining high levels of approval. *New Media & Society*, *21*(7), 1565–1593. https://doi.org/10.1177/1461444819826402

Langfitt, F. (2013, January 29). *The use of security cameras such as these, looking out over Tiananmen Square in Beijing, is on the rise in China. Critics say the government is using them to discourage dissidents.* [Photograph]. NPR. https://www.npr.org/2013/01/29/170469038/in-china-beware-a-camera-may-be-watching-you

Lloyd, T. (2021, November 29). Facebook’s metaverse heralds a brave new underworld of metacrime. *The New Republic*. https://newrepublic.com/article/164497/facebook-metaverse-cybercrime-marc-zuckerberg

MacKinnon, R. (2008). Flatter world and thicker walls? Blogs, censorship and civic discourse in China. *Public Choice*, *134*, 31-46. https://doi.org/10.1007/s11127-007-9199-0

Milmo, D. (2021, October 28). Enter the metaverse: The digital future Mark Zuckerberg is steering us toward. *The Guardian*. https://www.theguardian.com/technology/2021/oct/28/facebook-mark-zuckerberg-meta-metaverse

Mølmen, G. N., & Ravndal, J. A. (2021). Mechanisms of online radicalisation: How the internet affects the radicalisation of extreme-right lone actor terrorists. *Behavioral Sciences of Terrorism and Political Aggression, .* https://doi.org/10.1080/19434472.2021.1993302

Museum Fatigue. (2013, March 10). *Sensitive words* [Photograph]. https://museumfatigue.files.wordpress.com/2013/03/china-banned-cloud-1.jpg

Nahar, P. (2022, May 6). Can there be a metaverse without cryptocurrencies? Here's what experts say. *The Economic Times*.

https://economictimes.indiatimes.com/markets/cryptocurrency/can-there-be-a-metaverse-without-cryptocurrencies-heres-what-experts-say/articleshow/91367768.cms?from=mdr

Newton, C. (Host). (2021, July 22). Interview: Mark Zuckerberg on Facebook’s metaverse [Podcast transcript]. In *The Vergecast.* The Verge. https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview

Nie, H. (2022, January 26). Why China’s buying into the ‘metaverse’ hype. *Sixth Tone.* https://www.sixthtone.com/news/1009494/why-chinas-buying-into-the-metaverse-hype

Qiang, X. (2019). The road to digital unfreedom: President Xi’s surveillance state. *Journal of Democracy*, *30*(1), 53-67. https://doi.org/10.1353/jod.2019.0004

Rajeck, J. (2017, April 2). *Twitter is one of the blocked sites* [Screen capture]. Econsultancy. https://econsultancy.com/the-great-firewall-of-china-2017-update-the-good-and-the-bad/

Raphael, R., & Xi, L. (2019, January 23). *Chinese women show the scores of their Zhima Credit of Alibaba's Ant Financial on their Apple iPhones in Hangzhou City on May 9, 2016* [Photograph]. The Nation. https://www.thenation.com/article/archive/china-social-credit-system/

Ravenscraft, E. (2022, April 25). *What is the metaverse, exactly? Everything you never wanted to know about the future of talking about the future.* Wired. https://www.wired.com/story/what-is-the-metaverse/

Regalado, A. (2021, July 14). Facebook is ditching plans to make an interface that reads the brain. *MIT Technology Review.* https://www.technologyreview.com/2021/07/14/1028447/facebook-brain-reading-interface-stops-funding/

Rickli, J-M., & Mantellassi, F. (2022, March 25). *Our digital future: The security implications of metaverses.* Geneva Centre for Security Policy. https://dam.gcsp.ch/files/doc/ssa-25-march-2022

Robertson, A., & Peters, J. (2021, October 4). *What is the metaverse, and do I have to care? One part definition, one part aspiration, one part hype.* The Verge. https://www.theverge.com/22701104/metaverse-explained-fortnite-roblox-facebook-horizon

Shen, X. (2021, November 1). Chinese state-owned think tank flags national security risks of metaverse, citing potential political and social problems. *South China Morning Post*. https://www.scmp.com/tech/tech-trends/article/3154447/chinese-state-owned-think-tank-flags-national-security-risks

Stephenson, N. (1992). *Snow crash.* Bantam Spectra.

Su, Y. (2019). Exploring the effect of Weibo opinion leaders on the dynamics of public opinion in China: A revisit of the two-step flow of communication. *Global Media and China*, *4*(4), 493–513. https://doi.org/10.1177/2059436419866012

Sundararajan, S. (2022, February 22). *Metaverse trademark applications reach 16,000 in China.* FX Empire. https://www.fxempire.com/news/article/metaverse-trademark-applications-reach-16000-in-china-906841

Tanner, M. S., & Mackenzie, P. W. (2015). *China's emerging national security interests and their impact on the people's liberation army*. Marine Corps University Press.

Wang, D., & Qian, Y. (2021). Echo chamber effect in rumor rebuttal discussions about COVID-19 in China: Social media content and network analysis study. *Journal of Medical Internet Research*, *23*(3), e27009. https://doi.org/10.2196/27009

Wang, S., & Yu, J. (2021, November 19). *Gungju Wangshang Meihao Jinshen Jiayuan* [Building a beautiful spiritual home online]. *People's Daily*. http://cpc.people.com.cn/n1/2021/1119/c64387-32286470.html

Wee, S-L. (2015, February 25). China convicts 81-year-old writer who criticized propaganda chief. *Reuters*.

https://www.reuters.com/article/cnews-us-china-rights-idCAKBN0LT0V620150225

West, D. M. (2017, December 18). *How to combat fake news and disinformation.* Brookings. https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/

Wong, K. L. X., & Dobson, A. S. (2019). We're just data: Exploring China's social credit system in relation to digital platform ratings cultures in Westernised democracies. *Global Media and China*, *4*(2), 220-232. https://doi.org/10.1177/2059436419856090

Wuthnow, J. (2017). China's new "Black Box": Problems and prospects for the Central National Security Commission. *The China Quarterly*, *232*, 886-903. http://doi.org/10.1017/S0305741017001308

Zheng, Y., & Wang, Q. (2020). Shadow of the great firewall: The impact of Google blockade on innovation in China. *Strategic Management*, *41*(12), 2234-2260. https://doi.org/10.1002/smj.3179

Zhou, D. (2022, January 24). *Gongxinbu: Peiyu Yipei Jinjun Yuanyujou deng Xinxin Linyu de chuangxinxin zhungxiaoqiyie* [Ministry of industry and information technology: Cultivate a group of innovative small and medium-sized enterprises that have entered emerging fields such as metaverse]. The Paper. https://www.thepaper.cn/newsDetail_forward_16426057

Zhu, Y. (2022). China's 'new cultural diplomacy' in international broadcasting: branding the nation through CGTN documentary. *International Journal of Cultural Policy*. https://doi.org/10.1080/10286632.2021.2022651

Zhu, Y., & Fu, K. (2021). Speaking up or staying silent? Examining the influences of censorship and behavioral contagion on opinion (non-) expression in China. *New Media & Society*, *23*(12), 3634–3655. https://doi.org/10.1177/1461444820959016

Zhuravskaya, E., Petrova, M., & Enikolopov, R. (2020). Political effects of the internet and social media. *Annual Review of Economics*, *12*(1), 415-438. https://doi.org/10.1146/annurev-economics-081919-050239

Zollo, F., Bessi, A., Del Vicario, M., Scala, A., Caldarelli, G., Shekhtman, L., Havlin, S., & Quattrociocchi, W. (2017). Debunking in a world of tribes. *PLOS ONE*, *12*(7), e0181821. https://doi.org/10.1371/journal.pone.0181821

Author Biography

Ho Ting (Bosco) Hung is a Politics and International Relations student at the London School of Economics and Political Science (LSE). Hung is a member of the International Team for the Study of Security Verona and the Research Director of the LSE Undergraduate Political Review. Recently, he presented at the Oxford Hong Kong Forum 2022 and was interviewed by Asharq News to provide a geopolitical analysis of China's political economy. Additionally, Hung has written for Oxford Political Review, International Policy Digest, Modern Diplomacy, The Geopolitics, and International Affairs Forum. Hung is interested mainly in Sino-US relations, Chinese politics, foreign policy analysis, gender, political economy, and human rights.

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University

Available from: https://jicw.org/