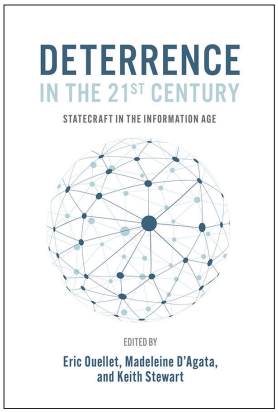
UNIVERSITY OF CALGARY
Press



DETERRENCE IN THE 21ST CENTURY: STATECRAFT IN THE INFORMATION AGE

Edited by Eric Ouellet, Madeleine D'Agata, and Keith Stewart

ISBN 978-1-77385-404-5

THIS BOOK IS AN OPEN ACCESS E-BOOK. It is an electronic version of a book that can be purchased in physical form through any bookseller or on-line retailer, or from our distributors. Please support this open access publication by requesting that your university purchase a print copy of this book, or by purchasing a copy yourself. If you have any questions, please contact us at ucpress@ucalgary.ca

Cover Art: The artwork on the cover of this book is not open access and falls under traditional copyright provisions; it cannot be reproduced in any way without written permission of the artists and their agents. The cover can be displayed as a complete cover image for the purposes of publicizing this work, but the artwork cannot be extracted from the context of the cover of this specific work without breaching the artist's copyright.

COPYRIGHT NOTICE: This open-access work is published under a Creative Commons licence. This means that you are free to copy, distribute, display or perform the work as long as you clearly attribute the work to its authors and publisher, that you do not use this work for any commercial gain in any form, and that you in no way alter, transform, or build on the work outside of its use in normal academic scholarship without our express permission. If you want to reuse or distribute the work, you must inform its new audience of the licence terms of this work. For more information, see details of the Creative Commons licence at: http://creativecommons.org/licenses/by-nc-nd/4.0/

UNDER THE CREATIVE COMMONS LICENCE YOU **MAY**:

- read and store this document free of charge;
- distribute it for personal use free of charge;
- print sections of the work for personal use;
- read or perform parts of the work in a context where no financial transactions take place.

UNDER THE CREATIVE COMMONS LICENCE YOU **MAY NOT**:

- gain financially from the work in any way;
- sell the work or seek monies in relation to the distribution of the work;
- use the work in any commercial activity of any kind;
- profit a third party indirectly via use or distribution of the work;
- distribute in or through a commercial body (with the exception of academic usage within educational institutions such as schools and universities);
- reproduce, distribute, or store the cover image outside of its function as a cover of this work;
- alter or build on the work outside of normal academic scholarship.

UNIVERSITY OF CALGARY
Press
press.ucalgary.ca

Acknowledgement: *We acknowledge the wording around open access used by Australian publisher,* **re.press**, *and thank them for giving us permission to adapt their wording to our policy* http://www.re-press.org

5

The Evolution of China's Information Exploitation of COVID-19

Anthony B. Seaboyer and Pierre Jolicoeur

Introduction

China is the single state actor producing the greatest volume of COVID-related disinformation. The effects of this targeting became increasingly evident with more waves of outbreaks unfolding as vaccination rates were insufficient. A major factor—but not the only contributing factor for the continuation of the pandemic—was disinformation-based vaccine reluctance. Some Western governments—such as the US government under the Trump administration—have undoubtedly also contributed to the COVID disinformation that Western audiences have consumed. But in terms of the amounts of COVID-related disinformation reaching Western audiences, China is the state actor that has most targeted the Western information space.

This chapter asks how China's messaging related to COVID has evolved during the pandemic. As COVID-related exploitation of the information space is part of China's information warfare operations, the chapter first describes China's general information warfare capabilities and how they evolved to show the context in which COVID-related messaging was exploited. It then looks into the role of information exploitation in China's political system and policies and the effects China's messaging is having. Based on this background, the chapter then describes five trends that can be observed in the evolution of China's COVID exploitation in the information space. The authors argue that the evolution can be described as moving from a limited quantity of defensive, unspecific, and rather vague posts, primarily directed at domestic audiences via local sources, to strategic, widespread, and very

specific and aggressive messaging increasingly targeting Western audiences through Western social media outlets.

What Are the Information Warfare Capabilities of China?

To understand the evolution of China's COVID-related exploitation of the information space, it is essential to consider the context in which these messaging operations are implemented. China's COVID messaging is part of its broader information warfare operations, which, in the early stages of the pandemic, initially primarily served the general goal of improving China's reputation both domestically and abroad. Information exploitation has played a very crucial role in China's political development in the past.

For decades China has focused on what it has described as "informationalization" by trying to catch up with Western development though information exploitation at all levels of the state—while at the same time attempting to control the very flow of all information—domestically and abroad. In an effort to simultaneously exploit information-based systems and control the flow of information, China developed a model for propaganda distribution and censorship that is unmatched in scale and, at some levels at least, such as censorship, also effectiveness.

Chinese information warfare (IW) capabilities can be divided into seven different categories: information operations (IO), cyber warfare, computer network operations (CNO), psychological operations, electronic warfare (EW), legal warfare, and space-based operations.[1]

Information Operations

The Chinese regime considers information operations to be at the core of IW, just as it considers IW to be at the core of informationalization (Anand, 2006). Chinese IO capabilities enable the implementation of the following strategies:[2] sabotaging information operation structures (Lovelace, 2015; Sabbagh, 2021); creating false situational impressions (Anand, 2006); launching surprise information attacks (Anand, 2006); weakening adversary information fighting capacity (Office of the Director of US National Intelligence, 2021; Spade, 2012); dispersing an adversary's forces, arms, and fires (Office of the Director of US National Intelligence, 2021); confusing or diverting the adversary (Ventre, 2014); information deception (Ellis, 2020; Ruwitch, 2021; Tsang, 2010); diverting an adversary's reconnaissance (Dell, 2017; Romo, 2021); targeting an adversary with false impressions or statements (Harold

et al., 2021); disrupting adversarial thinking (Cheng, 2021); forcing adversaries to believe what is true is false and what is false is true (Anand, 2006); information-based attacks exploiting collected information ("Hearing on China," 2021); information reconnaissance (Stokes et al., 2011); directing political, military, academic, and media assets as agents of influence (Bronskill & Bryden, 2021; Shaffer, 2017); intellectual property theft to access capabilities and technologies (Sobiesk, 2003); intercepting adversary signals (Sahay, 2016); mapping targeting information in foreign military, government, and civil infrastructure (Wortzel, 2010); influencing foreign media broadcasting—also through foreign media acquisition (Raska, 2015); influencing foreign information dissemination—also through distributor acquisition (Tromblay, 2017); propaganda production and dissemination abroad (Swanson, 2016); influencing foreign entertainment production and distribution (Tromblay, 2017); media broadcasting (Karásková, 2020; Quing & Schiffman, 2015); and social media exploitation (Cadell, 2017; Harold et al., 2021).

How Has China's Information Warfare Capability Evolved?

INFORMATIONALIZATION

China's leadership has a long history of valuing information exploitation. The People's Liberation Army (PLA) has traditionally seen information as a key to victory (Pomerleau, 2017a, 2020)—to help improve China's standing and capabilities as a developing country, but also as a dictatorship needing to control information as a central element enabling the Chinese Communist Party (CCP) to stay in power (Cheng, 2016). As the world economy became more globalized and information more integrated with development, the CCP view of the relationship between information and power has evolved. Initially, the Chinese understanding of IW was based on Western concepts (Anand, 2006), though China soon moved toward evolving its own orientation of what Chinese analysts have named "informationalization":

> Informationalization is a comprehensive system of systems, where the broad use of information technology is the guide, where information resources are the core, where information networks are the foundation, where information industry is the support, where information talent is a key factor, where laws,

> policies and standards are the safeguard. (State Council Information Office, 2002)

Accordingly, threats to China's national security (where perceived) also have become informationalized as adversaries enjoy unprecedented access to national economies, populations and decision makers: "as the long-range missile allows an opponent to directly strike a nation without having to break through ground or naval defences, so too information outflanks traditional military forces" (Cheng, 2016, p. 1)—to which we might add borders and most kinds of traditional protections against adversaries. The CCP began to perceive information itself as a threat. It is capable not only of eroding the morale of the military or reducing the population's support for a mission, but internally can also lead to much better-organized uprisings and domestic challenges to party leadership. With the increased "informationalization" of Chinese society, the CCP adapted its definition of national security interests and its military and security apparatus to lead informationalized wars and defend against informationalized attacks. At the same time, the CCP determined that security in the age of informationalization requires a response both on the civilian side and in government institutions. "An informationalized society will create an informationalized military, while an informationalized military can be produced only by an informationalized society and economy," which leads to the need to prepare for informationalized warfare (Cheng, 2016, p. 2).

INFORMATION AS THE KEY TO DEVELOPMENT

In the 1950s, as a highly disadvantaged country, China perceived that access to technical and military information could be a means to improve its standing and capabilities (Cheng, 2016). At the time, the primary target for China's information and political warfare campaigns was Taiwan (then known as Formosa, the seat of the Nationalist Chinese government-in-exile), with operations attempting to exploit political, cultural, and social frictions inside Taiwan, undermine trust between varying political-military authorities, de-legitimize Taiwan's international position, and gradually subvert public perceptions in order to "reunite" Taiwan on Beijing's terms (Chan & Thornton, 2022; Raska, 2015). Since then, China has been broadcasting propaganda toward Taiwan through the "Voice of the Strait" radio. Soon, though, added value was seen in investing in information technology as a means to

improve China's economic situation. Heavy investment in information technology followed in order to improve China's standing as a developing country (Cheng, 2016). The goals then were not only to enhance communication between ground troops in the PLA and generally improve communication in China, but also to catch up to the development level of Western countries and transition toward an information economy.

INFORMATION AS A KEY TO EXPANDING NATIONAL POWER

As the leadership of China became interested in expanding its comprehensive national power, it identified that it could only do so if information technologies were incorporated and integrated into the broader society. To this end, Beijing refocused its informationalization activities from building an information economy to creating an information society (Cheng, 2016).

In 1999, the then vice-minister of science, technology, and industry for national defence, defined IW as the exploitation of information technologies to influence enemy decision-maker determination while protection China's systems (Ventre, 2016).

In 2002, the Sixteenth Party Congress formally recognized "informationalization" as essential for Chinese "comprehensive National Power" (Cheng, 2016). China's goal in using IW had by then evolved to be to "force the enemy to regard their goal as our goal, to force the opponent to give up the will to resist and end confrontation and stop fight by attacking enemy's perceptions and belief via information energy" (Anand, 2006, p. 785). Apart from defence, the Chinese leadership also identified that "modernization in all parts of society depends on the information sector" (Cheng, 2016, p. 6). Accordingly, the Tenth Five-Year Plan (2001–5) for the first time included national "informationalization" among China's top sixteen priorities (Cheng, 2016).

The 2004 "Historic Missions for the New Phase of the New Century," as introduced by the chairman of the Central Military Commission, declared that the PLA's support role in maintaining the nation's interests would, for the first time, also include the information domain. In 2005 the focus on information integration was formalized in the first "National Strategy for Informationalization Development for 2006 to 2020." The strategy requested the strengthening of information security systems and enhancing the use of information in China on all levels of society (Cheng, 2016). To enable sufficient training, an information warfare simulation centre was created for training the PLA. The centre uses high-tech simulation skills and

equipment to simulate information warfare and its environment (Anand, 2006). In 2007, after the Seventeenth Party Congress, five members of the Politburo (out of twenty-four) directly focused on the informationalization of Chinese society. This reflected not only a substantial slice of Chinese political power, as well as high-level attention to the role of information, but also the increasing dominance of military and security interests in the area of information. Consequently, in 2008, most of the information technology (IT) and aerospace sectors were consolidated into the Ministry of Industry and Information Technology. This super ministry also oversees the military industrial complex (Cheng, 2016).

Since 31 December 2015, the Strategic Support Force (SSF) is responsible for the PLA's space, cyber, and electronic warfare missions (Costello, 2016). The SSF's space unit is responsible for preparation and conduct of co-orbital counter-space missions, while its cyber and EW unit is responsible for jamming satellite communications and GPS signals, as well as computer network operations against space facilities and satellites (Costello, 2016). The establishment of the SSF suggests that information warfare, including space warfare, long identified by PLA analysts as a critical element of future military operations, appears to have entered a new phase of development in the PLA (Pollpeter et al., 2016). It unifies the PLA's space, cyber, and EW capabilities for the first time (DOD, 2017). The SSF may be the PLA's first effort to combine cyber reconnaissance, attack, and defence capabilities in one organization (Pomerleau, 2017a). This of course leads to a further blurring of the distinction between peacetime and wartime capabilities in that peacetime operations now include the defence of the electromagnetic space and cyberspace (Bing, 2017). It appears there is no longer any detectable difference between wartime and peacetime information management in China, as informationalization is now all about expanding the political power of the leadership. At the same time, any flow of unauthorized information is seen as a national security threat, and China's leadership may well perceive itself to be in a constant wartime environment.

What began in the 1980s as an effort to enable the PLA to move from a loosely connected body of soldiers on the ground now extends to outer space, the electromagnetic spectrum, and the information domain. Today China is still assumed to remain behind US capabilities and is therefore improving training and domestic innovation to achieve its cyber capability development goals (Pomerleau, 2017b). It has openly appreciated the effectiveness

of information and cyber warfare in recent conflicts and is continuing to make further significant investments in a more "informationalized" military. Its officially disclosed defence budget has increased on average by 8.5 per cent during the 2007–17 period, though the steady increases fell during the pandemic, due to China's economic downturn (DOD, 2017). China's focus, though, has shifted away from a primary focus on domestic interests to more global ones. Accordingly, its military modernization program has become more intent on supporting missions beyond China's periphery, including power projection through information warfare. The opening of China's first overseas military base in Djibouti is testament to the country's new ambitions (Lendon & George, 2017). There can be no doubt that China has placed a growing emphasis on cyber and information warfare, pursuits for which it is streamlining its forces (O'Connor, 2017).

China has been learning from Russia's 2014 annexation of Crimea and the reaction of the international community. Chinese policy seems to have moved away from opposing any sovereignty movements (such as in Tibet) to caring less about the perceptions of the international community and in many cases simply adopting Russian narratives and approaches (Saalman, 2016). China subscribes to the Russian treatment of the Ukraine crisis as a "great power competition" between Washington and Moscow (Saalman, 2016). China's tactics more and more seem informed by some of Russia's while often further developing them (Saalman, 2016).

HOW ARE NON-STATE ACTORS AND PROXIES USED?

In China, as in Russia, the aim of the country's leadership is to "weaponize" the whole society, both covertly and overtly. Besides the openly involved state actors like state media or individual government officials, unofficial media is forced to abide by the same strict rules regarding the handling of information and what can be published ("Complete list of blocked websites," 2021; DFRLab, 2020). Through the trust system, citizens are forced to police other citizens or face dire consequences. As such, there is hardly any meaningful differentiation between state and non-state actors among the population at large, though actual adherence to the rules varies significantly. Corruption is very widespread in all levels of society. In China, similar to Russia, there is a clear implementation of the weaponization of society, from schools to the arts, media, architecture, and science. The PLA directs, manages, or guides political, military, academic, media, and intelligence assets that either overtly

or covertly serve as agents of influence of the Chinese government (Anand, 2006).

There are many examples of how China uses proxies. The PLA even uses engagements with foreign militaries in order to enhance its presence and influence abroad, to bolster its image, assuage other countries' concerns about its rise, and to communicate its positions to foreign audiences (DOD, 2017).

A more direct example of China's exploitation of proxies is its manipulation of media and journalists. Official media sources in China are considered by the public to be experts on the position of the state and in manipulating public opinion (Cheng, 2016). But non-official media is thought to report slightly more from the perspective of the public and in a less biased way (Stockman, 2011). Actually, though, the so-called non-official media is only slightly less official as it acts under almost all of the same rules with only slightly more relaxed restrictions (Cheng, 2016). China's government uses unofficial media to disseminate propaganda from seemingly non-state sources. As a result, in 2021 Reporters without Borders ranked China 177 out of 180 countries for press freedom, and in 2017 it called China the "world's leading prison for citizen journalists" (Reporters without Borders, 2021a). There is no longer any independent commercial or private media in China today (Cheng, 2016). China is also aggressively exporting its state media networks, particularly to Africa, Southeast Asia, and eastern Europe, and in this sense very much follows the Russian model of exporting RT (formerly Russia Today) and its global, multilingual apparatus (Mwakideu, 2021; Sui, 2019).

The CCP's Central Propaganda Department (CPD) exercises close oversight of all Chinese media (including cultural products). The CPD regularly issues directives on news topics, dictating which topics should and should not be covered, and which specific perspectives should be allowed, encouraged, or forbidden (McGregor, 2010). These directives come with the threat of punishment, including fines, job dismissal, jail time, or even the closure of entire news outlet. Also, any interviews with experts must be approved by both the work unit leadership and the CPD. Not only are certain stories forbidden; if incidents are intended to be covered up, stories to divert attention are suggested and encouraged (Murphy, 2011). Foreign journalists are also used—even against their will—as proxies. Journalists, as part of their "professional conduct," are not allowed to speak about any kind of information, source material, or news product (Foreign Correspondents Club of China, 2014). Any foreign journalist interviewing a Chinese journalist must either

report the chosen narratives of the Chinese government or risk harming their Chinese colleague. Chinese journalists are generally not allowed to participate in any professional exchanges or co-operate in any form with foreign media. Even Chinese citizens who work for foreign media organizations are regularly harassed or arrested (Kockritz, 2015).

The Chinese government goes even further, forcing foreign journalists to report according to its agenda. To begin with, only a small number of foreign journalists are allowed to work in China (Foreign Correspondents Club of China, 2014). They are granted permission only after a very lengthy and strenuous process that effectively chills any desire to risk gaining the attention of the authorities. If a foreign journalist nevertheless publishes stories critical of the Chinese government, visas are no longer issued to journalists from that organization. For this reason, Bloomberg and the *New York Times* can no longer report from inside China. Imagine a foreign journalist, who may have had to learn Mandarin for many years, considering such critical coverage while contemplating the fact that they will subsequently never be able to work in China again. The chilling effect is obvious—as is the likely desire to maintain a good relationship with Chinese authorities—and this again enables potential proxy relationships. Furthermore, journalists applying for a visa to report on a specific story face the same challenges as they have to be invited by a China-based organization. This process effectively makes hosts responsible for the reporting of their foreign invitees and assures that visiting journalists refrain from reporting on any other topics during their stay (Cheng, 2016).

CNO grant funding is a good example of the blurred line separating the state and non-state actors with whom the Chinese government works. Government grant programs to support CNO-related research (offensive and defensive) aim at commercial IT companies as well as civilian and military universities. As Krekel et al. (2012) show, a review of PRC university technical programs, curricula, research foci, and funding for research and development in areas contributing to information warfare capabilities illustrates the breadth and complexity of the relationships between the universities, government and military organizations, and commercial high-tech industries countrywide.

In civilian academia, the government has created at least five national grant programs for information warfare research, and at the same time has also funded the PLA's informationalization programs. Fifty civilian

universities conducting information security research benefit from one or more national-level grant programs, reflecting a broad technology-development plan. There is considerable debate as to the extent and effectiveness of China's influence over foreign academic institutions, particularly when those institutions become accustomed to the funding provided by the Chinese government (Krekel et al., 2012).

The PLA relies strongly on China's commercial IT sector for research and development (R&D) of dual-use and military-grade micro-electronics and telecommunications. Rather than isolate certain state-owned IT firms as exclusively "defence" in orientation, the PLA, often operating through its extensive base of R&D institutes, alternately collaborates with China's civilian IT companies and universities and benefits as a customer of nominally civilian products and R&D. The military benefits from this arrangement because it receives access to cutting-edge research. This work is often carried out by Chinese commercial firms with legitimate foreign partners supplying critical technology and often sharing the cost of the R&D (Krekel et al., 2012).

This enables the state to enjoy the latest commercial off-the-shelf telecommunications technology available through China's access to foreign joint ventures and international markets. The close relationship between some of China's—and the world's—largest telecommunications hardware manufacturers creates a potential vector for state-sponsored or state-directed penetration of international supply chains for micro-electronics (USCC Research Staff, 2011).

This has played out in the debate over Huawei's development of 5G networks, or the outright banning of Huawei's involvement in joint ventures in several countries, such as Japan, the United Kingdom, and Australia (Panettieri, 2021).

What Effect Has Been Achieved in Operations?

Domestically, the government has succeeded in eradicating any truly independent media in China. It is increasingly difficult for Chinese citizens to access "unauthorized" information—from either domestic or foreign sources. However, at least up until the recent blocking of the use of VPNs (virtual private networks), Chinese citizens have been very creatively circumventing government censorship by, for example, reading foreign media. So as to have debates on issues that are censored, citizens use code words that are very difficult for the government to censor.

After the death of Nobel laureate and famous dissident Liu Xiaobo of cancer in a state prison (due to the government's denial of medical treatment), his name became a targeted keyword, and Weibo blocked all mentions of him since 13 July 2017 (Si, 2017). Simultaneously, the "RIP" abbreviation, and even the candle emoticon, were blocked (Hernandez, 2017). Instead, citizens used the image of an empty chair, or simply the years of Liu's lifespan (1955–2017), to reference the dissident. He was also referred to by way of the phrase "someone died today," while others referred to the thunder and lightning storms that day in Beijing as a sign of "heavenly disquiet" (Mitchel et al., 2017). So while the Chinese government manages to control most communication, it is far from able to silence all dissenters in China or effectively block out ideas from other cultures.

Netizens posting videos and other content describing the most deplorable conditions in Chinese hospitals at the beginning of the pandemic represent further examples of dissidents circumventing the PRC's influence efforts (Ruan et al., 2022). The sheer number of code words and euphemisms that exist for sensitive content make it impossible for the government to achieve full censorship (Si, 2017)—unless it wishes to ban every image of a chair. It appears also that China's sensors are starting to realize, at least to some extent, that full censorship is not possible (nor particularly desirable). China's digital firewall, known as the "Golden Shield," was created to "protect" the Chinese population from the influence of unauthorized information from external and internal actors (Cheng, 2016). It appears, though—despite its efforts to drastically reduce what the general public can access—that the government is always a few steps behind when it comes to patching holes that have been found and exploited by citizens interested in real information. With some effort, it is still possible to access independent information in China. It is, however, increasingly difficult to do so—particularly without being noticed by the authorities.

China has undoubtedly succeeded in infiltrating the computer systems of foreign governments around the world to extract information from diplomats or members of the economic or defence industries. They have also successfully targeted defence contractors and succeeded in stealing proprietary information, such as plans of for high-tech military systems such as aircraft (Pomerleau, 2017b).

One of the most prominent Chinese successes in this regard was the 2015 hack of the US Office of Personnel Management database, which saw

the personal data of over 22 million federal employees breached (Nakashima, 2015). This hack included the fingerprints of 5.6 million US federal employees, enabling unprecedented exploitation of personal information (Associated Press, 2015). China is clearly capable of penetrating the computers that control vital national and military infrastructure, reconnoitering them electronically, and mapping or targeting nodes in the systems for future penetration or attack and planting malicious code to facilitate future entry (Wortzel, 2014).

China has also been successful in using its economic strength to inject itself into Western media, providing the ability to directly influence Western information dissemination and thereby influence foreign government decision making. The Chinese government has purchased telecoms, media companies, movie production companies, and even video game companies, which can all be used to disseminate Chinese propaganda through Western organizations. China can effectively diminish the impact of films that it deems to be counter to its interests, such as those portraying China as an aggressor or glorifying protest and civil disobedience. Ownership of distribution and production capabilities gives China increased influence on what Western audiences see. These acquisitions not only lead to heightened Chinese influence but also to the degradation of Western interests through the production and dissemination of hostile propaganda by (for example) Hollywood companies.

In the field of video games, China has succeeded in acquiring Riot Games, Epic Games, and Cryptic Studios. Similar to movies, video games can be designed to propagate desired messages. The positive treatment of China in virtual combat settings or the incorporation of Chinese mythology into a game's narrative could make effective use of high-end technology for perception management (Tromblay, 2017).

China has also succeeded—at least initially—in forcing a highly reputable publishing house, Cambridge University Press, to remove from its Chinese website 315 articles from *China Quarterly*, a journal published by Cambridge (Link, 2017). Immediate and extensive protest from Western academics led Cambridge to reverse its decision. China's response to this decision was very telling; speaking through the state-controlled daily paper the *Global Times*, the government offered the following rejoinder:

> It's no big deal if a few barely-read *China Quarterly* articles cannot be found on China's Internet. The real issue is that the fundamental principles of the two sides are in conflict, and the

> question is: Whose principles are a better fit for today's world? This is not a matter of "each to his or her own"; it is a contest of strength. In the end time will tell who's right and who's wrong. ("China Quarterly debate," 2017)

China sees itself in a contest for information dominance—no longer just domestically, but globally as well.

The Evolution of China's COVID-19 Exploitation

From the very beginning of the pandemic, China began spreading disinformation related to the virus. As early as 31 December 2019, Chinese government officials tried to deflect attention from reports on the origin of the virus and aimed to cast doubt on claims that the source of infection was in China (Kinetz, 2021). After facing increasing criticism and scrutiny for China's response to the virus, the country's officials took the lead in spreading disinformation related to the virus. Since the beginning of the pandemic China has been the single largest state actor spreading COVID-19-related disinformation targeting Western audiences. However, the forms, style, quantity, and targeting of such messaging has evolved since the beginning of the pandemic.

Initially, the main focus of narratives spread by China were directed at creating a positive image of the country, depicting as decisive in its actions against the virus and competent in meeting the challenge presented by the emerging pandemic (DFRLab, 2020). Positive events in the PRC's dealing with the virus where also exploited for propaganda to improve China's overall image domestically and abroad ("SARS hero follows leads," 2020). This initial messaging was basically an adaption of the main pre-pandemic focus of Chinese state propaganda, which aimed to establish a highly favourable image of the country while distracting from commentary critical of the Chinese government. While some messaging initially was directed at casting doubt as to the origin of the virus, as well as distracting from growing criticism of the country's handling of the pubic health crisis, the majority represented a continuation of information operations strategies already in use, such as downplaying, undermining, and/or discrediting any narratives that seemed undesirable to the PRC's leadership. Also, when positive messaging did not seem sufficient to cover up or distract from undesired foreign criticism, PRC messaging aimed at diminishing the credibility of China's geopolitical rivals (DFRLab, 2020).

As reports about the virus became more widespread, PRC officials aimed at suppressing reports of outbreaks of the virus, which led also to large-scale muzzling of data reporting (to the World Health Organization and to inquisitive news media), and even the arrest of whistle-blowers and doctors reporting on cases of illness related to the virus.

While PRC broadcasting originally confirmed the Wuhan's Huanan Seafood Market as the place at which the virus first emerged (Pan, 2020), the main messaging soon shifted to spreading disinformation about this question (DFRLab, 2020). At the same time vast censorship efforts were introduced aiming at deleting any online content that contained keywords relating to the outbreak—particularly after doctors tried to warn the public about the then unknown virus. For example, WeChat broadly censored coronavirus-related content, including criticism of the government, rumours and speculative information on the epidemic that were deemed undesirable, and even neutral references to the Chinese government's handling the outbreak (Ruan et al., 2022). The key focus of messaging and censorship campaigns became the control of available social media content in China relating to the virus (Crete-Nishihata et al., 2020).

Messaging subsequently focused on how the West was weaponizing COVID rumours to harm China (Shi, 2020). At the same time, rumours were deliberately spread by PRC sources to deflect from undesirable information that showed, for example, the deficiencies in the PRC's pandemic response (DFRLab, 2020). Social media posts by Chinese officials at this time raised doubts about the effectiveness of the vaccines then being developed by Western-based multinational pharmaceutical companies (Shi, 2020).

PRC officials then tried to claim that independent, established sources form other countries had also identified that the United States was behind the virus. In February 2020 the *People's Daily* claimed that a "Japanese TV report sparks speculations in China that COVID-19 may have originated in US" ("Japanese TV report," 2020). Additionally, PRC sources started to disseminate the narrative that COVID was actually a bio-weapon (DFRLab, 2020). In March 2020, messaging claiming that the outbreak could have originated in the United States was being widely distributed. In much larger numbers than before, content was posted to Western social media sites by China's Foreign Ministry officials and China's foreign diplomatic mission staff. Many such posts subsequently directly asked for readers to share the original posts (Zhao, 2020).

Chinese sources started posting on Western social media more aggressively—even though these platforms were blocked in China, as was the case, for example, with Twitter[3]—trying to more effectively target Western audiences. On Twitter, China's official diplomatic user accounts more than tripled from May 2019 to May 2020, going from 40 to 135 in just one year. Narrative production doubled and turned more aggressive and conspiratorial as well (Watts, 2020). These narratives started to target US audiences directly—for example, by claiming that the "CDC was caught on the spot" and that the US Army had brought the epidemic to Wuhan (Zhao, 2020).

Chinese narratives then started to become more specific in claiming a US origin for the virus. Chinese sources even went as far as to claim that COVID was imported to China through a batch of lobsters from Maine (Solon et al., 2021).

Tying into pre-existing conspiracy theories, social media posts connected to China's government started claiming that COVID originated in Fort Detrick, in the US state of Maryland, before it was spread to China by the US military. Between May and October 2021, over a thousand tweets, videos, and articles linked to Chinese accounts claimed that Fort Detrick was the origin of the virus (Aghekyan & Shafter, 2021).

Google News searches for "Fort Detrick" in August and September of 2021 were dominated by Chinese sources. Conspiracy theory narratives related to Fort Detrick reached a peak in August 2021, when they dominated even Google's Top Stories feature as well as Bing News results, with the *Global Times* and the *China Daily* appearing in the top results (Aghekyan & Shafter, 2021). At the same time, four of the six top videos on YouTube in searches for "Fort Detrick" came from Chinese media channels, while the remaining two also promoted Beijing-friendly talking points. In a further attempt to claim that other countries were responsible COVID, in 2022 China spread narratives on social media claiming that Beijing's first Omicron case came to China from Canada (Tunney, 2022).

This domination of news feeds and search engine results hints at the extent to which China had increased its narrative output, as well as its focus on spreading content targeted at Western audiences—a markable difference in output and target audience from the beginning of the pandemic. The following six trends can be observed in China's evolution of COVID exploitation in the information space.

From Defence to Offense

Messaging related to COVID has evolved from defensive posts covering up and distracting from the deficiencies and inhuman measures employed in the PRC's COVID response to offensive narratives aggressively claiming in large, international information campaigns that the United States is responsible for the origin of the outbreak.

NON-SPECIFIC TO SPECIFIC

Initial narratives spread by China were often not specific in their claims. The goal was initially to crowd out undesirable information and generally post content that made China appear in a positive light. Over time, the posting intentionally grew more specific, such as when the virus was claimed to have originated in the United States, rather than just raising doubt about reports indicating China as the origin. More recently, Chinese sources claim to have identified the exact location in the United States at which the virus was produced, and even that it was allegedly imported to China via a delivery of Maine lobsters.

VAGUE TO AGGRESSIVE

Initial posts where comparatively vague in their claims, often merely casting doubt on unfavourable reporting. Following the declaration of a global pandemic by the World Health Organization, China's messaging became increasingly aggressive toward Western actors (the United States in particular), even demanding information from US authorities based on nothing more than claims from conspiracy theories.

LOW TO HIGH OUTPUT

The sheer volume of messaging related to COVID increased significantly over the course of the pandemic. Both due to the proliferation of international criticism of China's handling of the virus and because COVID dominated the attention of audiences, which opened up opportunities for exploitation related to other messaging agendas.

INCREASED OUTPUT IN WESTERN SOCIAL MEDIA OUTLETS

While social media posts were initially directed primarily at domestic audiences in China, the PRC's messaging soon started to target Western audiences more directly. Increasingly, Western media outlets were targeted—for

example, via posts in the online comment sections of the BBC, the *Washington Post*, and other major news outlets, as well as on Western social media.

Overall, based on the above examples, China's exploitation of COVID in the information space can be described as evolving in the following general directions: from a limited quantity of defensive, unspecific, rather vague posts primarily directed at domestic audiences via local sources to strategic, very specific and aggressive messaging targeting Western audiences through Western social media outlets.

INCREASED CO-OPERATION WITH RUSSIA ON DISINFORMATION CAMPAIGNS

In the early phases of China's COVID exploitation in the information space there was little evidence of co-operation between China and Russia on disinformation campaigns. During the later phases of China's COVID information exploitation efforts, however, this changed, with the two countries showing an increasing level of co-operation in the dissemination of similar narratives and circular disinformation amplification becoming more common (Lucas et al., 2022). China and Russia started co-operating on multiplying the effects of their COVID disinformation campaigns by coordinating the distribution of narratives claiming that COVID is a biological weapon created in the United States and that China and Russia are responding more effectively to the pandemic (Jozwiak, 2020). This trend continues in other contexts today as China openly backs other Russian positions, such as narratives related to Russia's February 2022 invasion of Ukraine. Both actors co-operate on information space exploitation more than ever (Standish, 2023). Increasingly there is now evidence for the formation of a disinformation alliance between China and Russia (Bandurski, 2022).

Conclusion

This chapter asked how China's messaging related to COVID has evolved during the pandemic. After describing the role of information in the recent development of the political system in China, and the regime's general information warfare capabilities, the chapter described six trends that can be observed in the evolution of China's COVID information space exploitation. A transformation can be observed from a limited quantity of defensive, unspecific, rather vague posts, primarily directed at domestic audiences via local sources, to strategic, widespread, very specific and aggressive messaging targeting Western audiences through Western social media outlets. Finally,

we have observed the emergence of a disinformation alliance with Russia. For more definitive conclusions these observations will need to be substantiated with much larger research projects that can process a far greater volume of PRC-influenced posts.

While domestic narrative distribution did lead to substantial effects in China, where many citizens have been convinced that there is little merit to Western criticism of the PRC's dealing with the virus, internationally the impact is different. Despite mass messaging on alleged Chinese successes in dealing with the virus, and China's influence growing in some regions, like the Gulf, during the pandemic (Gurol-Haller & Saggar, 2023), few among these messages' Western audience seem convinced (Pierson, 2023; "Wuhan lab leak theory," 2021). Instead, it appears that despite the increasing output and sophistication of such messages, and the more direct targeting through Western media outlets and social media, Western audiences remain largely skeptical of China's handling of the virus and seem not to have been convinced by PRC online influence campaigns. This impression has not changed with China's declaration of a "decisive victory" over COVID in February 2023. While China claims to have created "a miracle in the history of human civilization," having had the lowest COVID death rate in the world (Hawkins, 2023), many countries, as well as the World Health Organization (Rigby & Tétrault-Farber, 2023), instead believe that Chinese leaders have been under-reporting the country's COVID deaths (Orr & Munroe, 2023), and that they have exploited the COVID response to accumulate power and increasingly establish a totalitarian political infrastructure in China (Xuecun, 2023).

NOTES

1 In research debates, there is no clear agreement on which of these seven components belong to IW, or if it even makes sense to separate some of them as they have impacts in most of the other areas. This selection is based largely on China-specific perceptions of IW based on the work of Vinod Anand (2006, 2014).

2 As can be seen in the list of examples, the means of delivery have evolved since 2006 but the strategies remain mostly consistent.

3 Twitter is "officially" banned in China but is widely consumed in China via VPN access. Algorithm-based content filters are, however, used in China to prevent the trending of certain words, phrases, or hashtags, or to block access to prohibited content.

REFERENCES

Aghekyan, E., & Shafter, B. (2021). *Deep in the data void: China's COVID-19 disinformation dominates search engine results.* German Marshall Fund of the United States. https://securingdemocracy.gmfus.org/data-void-china-covid-disinformation

Anand, V. (2006). Chinese concepts and capabilities of information warfare. *Strategic Analysis, 30*(4), 781–97.

Anand, V. (2014, 21 April). PLA's information warfare capabilities on an upward trajectory. *Vivekananda International Foundation*. https://www.vifindia.org/print/2123

Associated Press. (2015, 23 September). US government hack stole fingerprints of 5.6 million federal employees. *The Guardian*. https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints

Bandurski, D. (2022, 11 March). China and Russia are joining forces to spread disinformation. *Brookings Institution*. https://www.brookings.edu/techstream/china-and-russia-are-joining-forces-to-spread-disinformation/

Bing, C. (2017, 22 June). How China's cyber command is being built to supersede its US military counterpart. *Cyberscoop*. https://www.cyberscoop.com/china-ssf-cyber-command-strategic-support-force-pla-nsa-dod/

Bronskill, J., & Bryden, J. (2021, 23 June). Feds ask court to keep documents related to scientists' firing under wraps. *CTV News*. https://winnipeg.ctvnews.ca/feds-ask-court-to-keep-documents-related-to-scientists-firing-under-wraps-1.5482962

Cadell, C. (2017, 11 August). China investigates top local social media sites in push to control content. *Reuters*. https://www.reuters.com/article/us-china-cyber/china-investigates-top-local-social-media-sites-in-push-to-control-content-idUSKBN1AR07K

Chan, K., & Thornton, M. (2022, 19 September). China's changing disinformation and propaganda targeting Taiwan. *The Diplomat*. https://thediplomat.com/2022/09/chinas-changing-disinformation-and-propaganda-targeting-taiwan/

Cheng, D. (2016). *Cyber dragon: Inside China's information warfare and cyber operations*. Praeger.

Cheng, D. (2021). An overview of Chinese thinking about deterrence. In F. Osinga & T. Sweijs (Eds.), *NL ARMS Netherlands annual review of military studies 2020* (pp. 177–200). Asser Press. https://doi.org/10.1007/978-94-6265-419-8_10

China Quarterly debate a matter of principle. (2017, 20 August). *Global Times*. Retrieved 31 August 2017 from http://www.globaltimes.cn/content/1062304.shtml

The complete list of blocked websites in China & how to access them. (2021, 19 October). *VPNMentor.com*. https://www.vpnmentor.com/blog/the-complete-list-of-blocked-websites-in-china-how-to-access-them/

Costello, J. (2016). *The Strategic Support Force: Update and overview.* Jamestown Foundation. https://jamestown.org/program/strategic-support-force-update-overview/

Crete-Nishihata, M., Dalek, J., Knockel, J., Lawford, N., Wesley, C., & Zhou, M. (2020, 25 August). *Censored contagion II: A timeline of information control on Chinese social media during COVID-19*. Citizen Lab. https://citizenlab.ca/2020/08/censored-contagion-ii-a-timeline-of-information-control-on-chinese-social-media-during-covid-19/

DFRLab (Digital Forensic Research Lab). (2020). *Countering Chinese disinformation reports*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/dfrlab-china-reports

DOD (Department of Defense). (2017, May 15). *Annual report to Congress: Military and security developments involving the People's Republic of China*. Office of the Secretary of Defense.

Ellis, S. (2020, 7 October). Here's what could happen if China invaded Taiwan. *Bloomberg.* https://www.bloomberg.com/news/features/2020-10-07/here-s-what-could-happen-if-china-invaded-taiwan

Foreign Correspondents Club of China. (2014, 12 September). *Position paper on working conditions for foreign journalists*. fccchina.org/2014/09/12/fccc-position-paper-2014/

Gurol-Haller, J., & Saggar, R. (2023, 17 April). China's renewed influence in the Gulf. *Chatham House*. https://www.chathamhouse.org/2023/04/chinas-renewed-influence-gulf

Harold, S. W., Beauchamp-Mustafaga, N., & Hornung J. F. (2021). *Chinese disinformation efforts on social media*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR4300/RR4373z3/RAND_RR4373z3.pdf

Hawkins, A. (2023, 17 February). China claims "decisive victory" over Covid amid doubt over figures. *The Guardian*. https://www.theguardian.com/world/2023/feb/17/china-victory-covid-deaths-virus

Hearing on China and US national security. (2021, 4 August). C-Span. https://www.c-span.org/video/?513854-1/hearing-china-us-national-security

Hernandez, J. C. (2017, 14 July). Chinese citizens evade internet censors to remember Liu Xoabo. *New York Times*. https://www.nytimes.com/2017/07/14/world/asia/china-liu-xiaobo-censorship-internet.html?mcubz=3

Japanese TV report sparks speculations in China that COVID-19 may have originated in US. (2020, 23 February). *People's Daily*. http://en.people.cn/n3/2020/0223/c90000-9661026.html

Jozwiak, R. (2020, 22 April). EU monitors see coordinated COVID-19 disinformation effort by Iran, Russia, China. *Radio Free Europe/Radio Liberty*. https://www.rferl.org/a/eu-monitors-sees-coordinated-covid-19-disinformation-effort-by-iran-russia-china/30570938.html

Karásková, I. (2020, 13 November). China's evolving approach to media influence: The case of Czechia. *The Diplomat*. https://thediplomat.com/2020/11/chinas-evolving-approach-to-media-influence-the-case-of-czechia/

Kinetz, E. (2021, 15 February). Anatomy of a conspiracy: With COVID, China took a leading role. *AP News*. https://apnews.com/article/pandemics-beijing-only-on-ap-epidemics-media-122b73e134b780919cc1808f3f6f16e8

Kockritz, A. (2015, 14 January). They have Miao. *Die Zeit*. https://www.zeit.de/feature/freedom-of-press-china-zhang-miao-imprisonment?utm_referrer=https%3A%2F%2Fwww.google.com%2F

Krekel, B., Adams, P., & Bakos, G. (2012, March). *Occupying the information high ground: Chinese capabilities for computer network operations and cyber espionage*. US-China Economic and Security Review Commission. https://info.publicintelligence.net/USCC-ChinaCyberEspionage.pdf

Lendon, B., & George, S. (2017, 13 July). China sends troops to Djibouti, establishes first overseas military base. *CNN*. http://edition.cnn.com/2017/07/12/asia/china-djibouti-military-base/index.html

Link, P. (2017, 5 September). Beijing's bold new censorship. *New York Review of Books*. http://www.nybooks.com/daily/2017/09/05/beijings-bold-new-censorship/

Lovelace, D. (2015). *The cyber threat*. Oxford University Press.

Lucas, E., Dubow, B., Lamond, J., Morris, J., Rebegea, C., & Zakem, V. (2022). Post-mortem: Russian and Chinese COVID-19 information operations. *Centre for European Policy Analysis*. https://cepa.org/comprehensive-reports/post-mortem-russian-and-chinese-covid-19-information-operations/

McGregor, R. (2010). *The Party: The secret world of China's Communist rulers*. Harper.

Mitchel, T., Wildau, G., & Feng, E. (2017, 14 July). China online censors rush to erase Liu Xiaobo tributes. *Financial Times*. https://www.ft.com/content/b6d56066-6847-11e7-8526-7b38dcaef614

Murphy, Z. (2011, 28 July). China struggles to censor train crash coverage. *BBC News*. http://www.bbc.com/news/world-asia-pacific-14321787

Mwakideu, C. (2021, 29 January). Experts warn of China's growing media influence in Africa. *Deutsche Welle*. https://www.dw.com/en/experts-warn-of-chinas-growing-media-influence-in-africa/a-56385420

Nakashima, E. (2015, 2 December). Chinese government has arrested hackers it says breached OPM database. *Washington Post*. https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html?utm_term=.3bb698ba57ee

O'Connor, T. (2017, 19 April). Chinese military prepares for new cyber focus, streamlined force. *Newsweek*. http://www.newsweek.com/chinese-military-prepares-massive-changes-new-cyber-division-586313

Office of the Director of US National Intelligence (2021, 9 April). *Annual threat assessment of the US intelligence community*. https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2204-2021-annual-threat-assessment-of-the-u-s-intelligence-community.

Orr, B., & Munroe, T. (2023, 16 February). China declares "decisive victory" over COVID-19. *Reuters*. https://www.reuters.com/world/china/china-declares-decisive-victory-over-covid-19-2023-02-17/

Pan, Z. (2020, 27 January). Experts confirm Wuhan seafood market was source of novel coronavirus. *CGTN*. https://news.cgtn.com/news/2020-01-27/Experts-confirm-Wuhan-seafood-market-was-source-of-novel-coronavirus--NAHPUtsPgA/index.html

Panettieri, J. (2021, 11 November). Huawei: Banned and permitted in which countries? List and FAQ. *Channel E2E*. https://www.channele2e.com/business/enterprise/huawei-banned-in-which-countries/

Pierson, D. (2023, 27 February). China dismisses latest claim that lab leak likely caused Covid. *New York Times*. https://www.nytimes.com/2023/02/27/world/asia/china-react-covid-lab-leak.html

Pollpeter, K., Chase, M., & Heginbotham, E. (2016, 2 May). *In with the old, out with the new? The creation of the Strategic Support Force and its implications for Chinese military space operations*. RAND Corporation. https://www.rand.org/paf/casi/research-topics.html

Pomerleau, M. (2017a, 22 March). Breaking down China's electronic warfare tactics. *C4ISRNET*. https://www.c4isrnet.com/c2-comms/2017/03/22/breaking-down-chinas-electronic-warfare-tactics/

Pomerleau, M. (2017b, 7 June). DoD's assessment of China's information capabilities. *C4ISRNET*. https://www.c4isrnet.com/2017/06/07/dod-s-assessment-of-china-s-information-capabilities/

Pomerleau, M. (2020, 1 September). China moves toward new "intelligentized" approach to warfare, says Pentagon. *C4ISRNET*. https://www.c4isrnet.com/battlefield-tech/2020/09/01/china-moves-toward-new-intelligentized-approach-to-warfare-says-pentagon/

Quing, K. G., & Schiffman, J. (2015, 2 November). Beijing's covert radio network airs China-friendly news across Washington, and the world. *Reuters*. http://www.reuters.com/investigates/special-report/china-radio/

Raska, M. (2015, December). China and the three warfares. *The Diplomat*. http://thediplomat.com/2015/12/hybrid-warfare-with-chinese-characteristics-2/

Reporters without Borders. (2021, 28 June). At least 22 newspapers "murdered" in the past five years. *RSF.org*. https://rsf.org/en/news/least-22-newspapers-murdered-past-five-years

Reporters without Borders. (2021). 2021 world press freedom index. *RSF.org*. https://rsf.org/en/ranking

Rigby, J., & Tétrault-Farber, G. (2023, 4 January). WHO says China data underrepresents COVID surge and deaths. *Reuters*. https://www.reuters.com/world/china/whos-tedros-concerned-by-china-covid-surge-calls-again-data-2023-01-04/

Romo, V. (2021, 24 March). Chinese hackers made fake Facebook profiles, apps to spy on Uyghur activists. *NPR*. https://www.npr.org/2021/03/24/981021257/chinese-hackers-made-fake-facebook-profiles-apps-to-spy-on-uyghur-activists.

Ruan, L., Knockel, J., & Crete-Nishihata, M. (2020, 3 March). *Censored contagion: How information on the coronavirus is managed on Chinese social media*. Citizen Lab. https://citizenlab.ca/2020/03/censored-contagion-how-information-on-the-coronavirus-is-managed-on-chinese-social-media/

Ruwitch, J. (2021, 28 October). Would the U.S. defend Taiwan if China invades? Biden said yes. But it's complicated. *NPR*. https://www.npr.org/2021/10/28/1048513474/biden-us-taiwan-china

Saalman, L. (2016). Little grey men: China and the Ukraine crisis. *Survival, 58*(6), 135–56.

Sabbagh, D. (2021, 23 September). Experts say China's low-level cyberwar is becoming severe threat. *The Guardian*. https://www.theguardian.com/world/2021/sep/23/experts-china-low-level-cyber-war-severe-threat

Sahay, R. K. (2016). *History of China's military*. Alpha Edition.

SARS hero follows leads on illness. (2020, 23 January). *China Daily*. http://en.people.cn/n3/2020/0123/c90000-9651455.html

Shaffer, L. (2017, 7 August). Pro-Beijing professor expelled from Singapore for being "agent" of foreign power. *CNBC*. https://www.cnbc.com/2017/08/07/pro-beijing-professor-expelled-from-singapore-for-being-agent-of-foreign-power.html

Shi, T. (2020, 18 February). Some in West weaponize rumors to attack China. *Global Times*. https://www.globaltimes.cn/content/1180041.shtml

Si, J. (2017, 21 July). *The Chinese language as a weapon: How China's netizens fight censorship*. Berkman Klein Center. https://medium.com/berkman-klein-center/the-chinese-language-as-a-weapon-how-chinas-netizens-fight-censorship-8389516ed1a6

Sobiesk, E. (2003, 1 March). *Redefining the role of information warfare in Chinese strategy*. SANS Institute. https://www.sans.org/white-papers/896/

Solon, O., Simmons, K., & Perrette, A. (2021, 21 October). China-linked disinformation campaign blames Covid on Maine lobsters. *NBC News*. https://www.nbcnews.com/news/china-linked-disinformation-campaign-blames-covid-maine-lobsters-rcna3236

Spade, J. (2012). *Information as power: China's cyber power and America's national security*. US Army War College.

Standish, R. (2023, 6 March). Disinformation wars: China, Russia, cooperating on propaganda more than ever, says report. *Radio Free Europe/Radio Liberty*. https://www.rferl.org/a/china-russia-cooperation-propaganda-marshall-fund/32305566.html

State Council Information Office. (2002). *Tenth five year plan for national economic and social development, informationalization key point special plan*. People's Republic of China. http://www.cia.org.cn/information/information_01_xxhgh_3.htm

Stokes, M. A., Lin, J., & Hsiao, R. L. C. (2011, 11 November). The Chinese People's Liberation Army signal intelligence and cyber reconnaissance infrastructure. *Project2049.net*. https://project2049.net/.../pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf

Sui, C. (2019, 1 November). China wants state media to peddle its "soft power" in Africa, but tech platforms are a better bet. *Quartz Africa*. https://qz.com/africa/1736534/china-daily-cgtn-fight-for-influence-in-africa-vs-bbc-cnn

Swanson, A. (2016, 24 September). China's influence over Hollywood grows. *Washington Post*. https://www.washingtonpost.com/news/wonk/wp/2016/09/24/chinas-influence-over-hollywood-grows/?utm_term=.56d914bac548

Tromblay, D. E. (2017, 22 May). No more fun and games: How China's acquisition of U.S. media entities threatens America's national security. *Small Wars Journal*. https://smallwarsjournal.com/jrnl/art/no-more-fun-and-games-how-china%E2%80%99s-acquisition-of-us-media-entities-threatens-america%E2%80%99s-nati

Tsang, S. (2010). *If China attacks Taiwan: Military strategy, politics and economics*. Oxford University Press.

Tunney, C. (2022, 17 January). Doctors say claim that Beijing's 1st Omicron case came from Canada isn't based on science. *CBC News*. https://www.cbc.ca/news/politics/china-allegations-mail-1.6318115

USCC Research Staff (2011, January). *The national security implications of investments and products from the People's Republic of China in the telecommunications sector*. US-China Economic Security Review Commission.

Ventre, D. (2014). *Chinese cybersecurity and defense*. Wiley.

Ventre, D. (2016). *Information warfare*. Wiley.

Watts, C. (2020, 15 May). *Triad of disinformation: How Russia, Iran, & China ally in a messaging war against America*. Alliance for Securing Democracy. https://securingdemocracy.gmfus.org/triad-of- disinformation-how-russia-iran-china-ally-in-a-messaging-war-against-america/

Wortzel, L. (2010, 10 March). China's approach to cyber operations: Implications for the United States [Testimony]. *US House of Representatives Committee on Foreign Affairs*. https://www.uscc.gov/sites/default/files/Congressional_Testimonies/LarryWortzeltestimony-March2010.pdf

Wortzel, L. (2014, March). *The Chinese People's Liberation Army and information warfare*. US Army War College Press. https://press.armywarcollege.edu/monographs/506

Wuhan lab leak theory: How Fort Detrick became a centre for Chinese conspiracies. (2021, 23 August). *BBC News*. https://www.bbc.com/news/world-us-canada-58273322

Zhao, L. (@zlj517). (2020, 12 March). *This article is very much important to each and every one of us. Please read and retweet it. COVID-19: Further Evidence that the Virus Originated in the US* [Tweet]. Twitter. http://archive.today/2020.03.13-114631/https:/twitter.com/zlj517/status/1238269193427906560