Unleash the Dragon: China's Strategic Narrative during the COVID-19 Pandemic

Mark Bryan Manantan[1]

ABSTRACT

This article argues that the disruption of the coronavirus was a critical opportunity among states to draw compelling narratives and consequently negotiate their power status and level of influence based on their management of the outbreak. This argument will be explored through the Chinese Communist Party (CCP) at the height of the pandemic. The article investigates the evolution of the CCP's information warfare as an asymmetric capability from its early days of technological inferiority towards its ascendancy to great power status. It highlights the breakthrough of Chinese app TikTok in the US-dominated social media landscape and its potential impact in expanding China's strategic narrative. Using the proposed analytical tools—assets, tactics, and narratives—this article examines the whole of CCP approach aimed to shape the narrative in China's favor following the global outcry from its lack of transparency during the early stages of the pandemic set against the backdrop of its deepening strategic rivalry with the US. It concludes that the CCP will continue to capitalize on information warfare to promote the superiority of the Chinese model amid the eruption of unexpected global crises while depicting the decline of the Western-centric order.

INTRODUCTION

In the aftermath of the US Presidential Elections in 2016, an abrupt change in the cybersecurity policy community transpired. From the heavily focused debate about integrating 'deterrence' in cyberspace, the aperture shifted into combatting the increasing threats from the online environment caused by information warfare.[2] Overnight, social media companies like Facebook, Twitter, and Google found themselves under greater

Mark Bryan Manantan is currently the Lloyd and Lilian Vasey fellow at the Pacific Forum and concurrently, a non-resident fellow at the Center for Southeast Asian Studies at the National Chengchi University in Taiwan. Recently he was based at the Center for Rule-Making Strategies at Tama University in Tokyo, Japan, and the East-West Center in Washington DC as a 2020 US-Japan-Southeast Asia Partnership in a Dynamic Asia Fellow.

scrutiny for being weaponized by Russian sponsored hackers and troll operators to tamper US elections.[3] Four years after the Russian interference in American election, open and liberal societies are still grappling with the effects of information warfare only to be confronted with an unexpected global health crisis that will test the online information environment into a whole new level. Despite existing efforts like fact-checking or policing against coordinated and inauthentic behaviors in social media platforms,[4] the uncertainty brought by the COVID-19 pandemic served as the perfect catalyst which afforded authoritarian states like Russia and China to achieve a forward advantage in the online environment by launching information warfare to cause psychological distress. The disruptive effects of the current pandemic facilitated the acceleration of information warfare to win the battle for strategic narrative and ultimately expand influence while continuing to undermine trust among open and liberal societies across the globe.

This article examines the salience of information warfare as the weapon of choice during the unprecedented global pandemic among authoritarian countries. It argues that information warfare was instrumental to propel a strategic agenda, influence the prevailing debates, and even aggravate existing divisions to promote a state's own interests in international politics and undermining adversaries as majority of the international community strive to cope with the devastating impacts of COVID-19. This argument is explored through the Chinese Communist Party (CCP) and its sophisticated efforts to amplify its strategic narrative following the global fallout from its mismanagement of the coronavirus at the early onset of the pandemic, and, more broadly, to advance its interests on its on-going great power contest with the US. The CCP is no stranger in conducting covert operations to promote its strategic narrative as seen in Hong Kong and Taiwan, however, the COVID-19 pandemic has immensely threatened the

Party's international standing and credibility, thereby, this accelerated information warfare as the crux of its strategic response. An international survey revealed a rising anti-China sentiment since the Tiananmen massacre in 1989.[5] To arrest this, China employed a whole-of-CCP approach to distract the international community from focusing on China's lack of transparency and accountability and to exploit the inherent political and socio-economic divisions in international politics to assert its increasing influence amid a declining US hegemony.

Russia is the most prominent state actor using information warfare to achieve its political and strategic goals as shown during its extensive interference in the US Presidential elections, and the BREXIT referendum in 2016.[6] Trailing behind Russia is China which is increasingly becoming a central actor in the information warfare space, primarily asserting its influence as a rising power in the emerging post-liberal order. On the surface, it is convenient to assume that China could just be borrowing pages from Russia's information warfare playbook.[7] However, this paper contends that CCP's information warfare is more sophisticated than Russia influenced by its new-found great power status which demonstrates its dual identity in international politics as a disruptor and as a collaborator. Compared to Russia, which is beset with debilitating challenges primarily from its stagnant economy and regime instability, China's re-emergence is backed by its increasing political and economic power. China's increasing competitiveness in the emerging technological landscape makes it a formidable peer competitor of the US. This makes China a well-resourced state actor capable of launching information warfare that is even more sophisticated, potent, and pervasive than Russia's. China no longer relies solely on the established tech titans—Facebook, Twitter, YouTube, and Google—to conduct its information warfare. Instead it has successfully penetrated the US-dominated global social media landscape with its own rising digital native platforms like TikTok. As a true marker of its ambition to shape the contours of the Fourth Industrial Revolution, China has nurtured and developed its own tech platforms to capture a global audience. This provides the CCP with a myriad of possible options for experimentation on different information campaigns using various assets. On one hand, the CCP could utilize US social media apps to sow its strategic narrative and counter its critics, on the other hand, it can now employ TikTok and other rising Chinese apps for its information warfare operations and conduct censorship on content which does not align to the CCP's agenda.

This article develops a comprehensive analysis on China's unrelenting quest to advance its strategic narrative through information warfare by exploiting US and Chinese social media platforms. It also examines China's evolving information warfare tactics through its two-pronged approach of seeding and amplifying its strategic narrative while simultaneously conducting censorship in the context of the coronavirus pandemic. Data-gathering for this paper relied on desktop research and open-source information, particularly from policy papers and online articles that were published by various think-tanks and international media outlets which covered China's information warfare during the pandemic. To better explicate China's approach to its strategic narrative, the paper proposes three analytical tools namely: (1) assets, (2) tactics, and (3) narrative.

This entire article unfolds as follows: after this introductory section, the paper proceeds with a conceptual discussion on strategic narrative in the context of the brewing contestation in international affairs between the US and China, particularly the systemic challenges presented by the emerging post-liberal order to the current status quo supported by the US-led international rules-based order. It then dives deeper into the role of information warfare as the critical vehicle which allow states to drive discourse surrounding their respective strategic narrative in the online environment. The article moves to explain the CCP's unique approach on information warfare and the evolution of such capability in the context of its ascendancy to great power status to propel a narrative that serves its global interests. The next to last section explains the defining hallmarks of the CCP's strategic narrative playbook using empirical data by drawing from the proposed triad of analytical tools—assets, tactics, and narratives— as seen throughout the course of the pandemic. The final section offers the conclusion.

Understanding Strategic Narrative

Strategic narratives are tools that are used by political actors to construct (reconstruct) their political realities, extend influence, manage expectations, change discursive environments in which they operate and advance their cause to domestic and international audiences.[8] Examining the "strategy and intent of the communicating actor" and the aspects of "convergence or divergence" will illuminate how and where audience draw their understanding of international politics.[9] It is necessary to focus on the interlinked process of strategic narratives at all stages—formation, projection, and reception[10]—and its various constitutive elements of character/actors; setting/environment; conflict/action; to resolution/solution.[11] These elements form the raw materials that state actors use to craft a narrative to drive discourse.[12]

In international relations, strategic narrative emerges as an intellectual project which aims to examine the relationship of communication, persuasion and influence in global politics.[13] Rather than subscribing to 'soft power' in explaining how states influence or persuade others, shifting the focus on strategic narratives and its "interactive, dialogic, and relational properties" provides more explanatory power to assess the political dynamics within and between states.[14] States use narratives *strategically* not only to persuade their target audience but also to contest and even contradict others. Compelling narratives can be sources of power as they illustrate "the formation, projection and diffusion of ideas in the international system."[15] Such formation and projection of strategic narratives along with its reception and interpretation evoke a sense-making, order-making and path-making process where engagement, persuasion, and contestation of ideas and information are located, experienced, and examined.[16]

By analyzing narratives, scholars and policymakers could arrive at a more compelling explanation on power and influence as it demonstrates how "political actors strategically shape and are shaped by narratives." Strategic narratives could better explain how soft power tools and capabilities such as culture, values, and policies wield influence as they are linked by a causal logic in a communicative fashion.[17] There are three categories or levels of strategic

narratives—international or systemic, identity or national, and policy or issue-based. At the international level the focus is on the systemic properties, structural dynamics and the major players involved. While at the second level of identity or national narratives, the values, goals, principles, and standards of political actors take centerstage. Lastly, issue or policy-based-narratives underline the objectives and the motivation of policies promoted by state actors and how they are implemented.[18]

As an analytical tool, strategic narrative can illuminate the recent structural shifts in the international system caused by the on-going great power contest. Narratives serve as a window to explicate the relational aspects of the ensuing US-China trade-turned-tech war by shedding light on issues related to the perception and recognition on the rise of China and the decline of the US hegemony. The current reordering in the international system emanating from the US-China competition highlights a rivalry of strategic narratives. The former being the vanguard of the international rules-based order and the latter expressing its dissatisfaction with the status quo which it seeks to challenge or innovate to suit its interests.[19]

Several scholars have noted that the hegemony of the liberal order which was developed under the US leadership in the post-Second World War that inspired the fundamental basis for international law, free trade, human rights within the multilateral system is already over. The fading traction of liberal norms and values has given rise to some forms of illiberalism.[20] In ascertaining this transition into the 'new world order', three key dimensions comes to mind—power, values, and institutional dynamics.[21] Power is shifting horizontally and vertically, where transnational dynamics challenge conventional notions of sovereignty, and states are no-longer the central entity in international politics given the rise of non-state actors. The universality of liberal values underpinned by democracy and human rights has diminished as calls for their relativity and even abandonment becomes increasingly palpable.[22] While the rules-based multilateral system, comprised mainly of the US-led Bretton Wood institutions is also under extreme pressure to reform itself as western-dominated institutions to reflect the rise of other emerging powers.

Applied in the context of this paper, China's strategic narrative which it aims to propagate in the midst of the pandemic lies within its deep contestation on the preponderance of the US-led order. The COVID-19 pandemic highlights the systemic changes which are underway in the international system. It has become a critical flashpoint for both superpowers to draw compelling narratives and consequently negotiate their power status and level of influence based on their management of the outbreak. China has been capitalizing on the pandemic to prove the strength and endurance of the Chinese authoritarian model vis-à-vis the US international rules-based order. Its narrative has centered on its ability to quickly recover, resume its economy, and return to normalcy to depict a level of legitimacy as the rising superpower. By appearing unscathed from the pandemic, China attempts to cement its claims of legitimacy of great power status.[23] It positions itself in stark contrast to the underperformance of the US to control the outbreak—a symptom of its declining status. China's claims of superiority over the

US is further exacerbated by President Trump's threats of withdrawal from the World Health Assembly. The absence of US leadership provides a vacuum which China has been willing to fill in. At the World Health Assembly last May, China pledged $2 billion for coronavirus response—an amount which is twice more than what the US has provided the global health agency.[24] But how does China's strategic narratives get diffused to instigate discourse and reach its target audience? The discussion in the proceeding section establishes the linkage between strategic narrative and information warfare in the current era of hyperconnectivity where the latter acts as the critical driving force to stimulate discourse on the former at the regional and international level.

Information Warfare: Pushing the Strategic Narrative Discourse

The rise of social media and the internet more broadly have become important avenues for states to propel their strategic narrative in today's highly connected digital society. The new multimedia environment has become an integral platform for states to construct strategic narratives that favor their foreign policy goals and to counter those that are opposed to their interests.[25] The upward trend in the adoption of Information and Communications Technology (ICT) has shifted the process on how states produce their own strategic narratives. More so, the instantaneous nature of Internet accelerated the dissemination as well as the contradiction of narratives between rival states, setting the stage for the emergence of threats related to information warfare.[26]

Information warfare and its related term influence operations is defined as the "deliberate use of information by one party on an adversary to confuse, mislead, and ultimately to influence the choices and decisions that the adversary makes".[27] It is a series of strategic narratives espoused by states which are spread online geared towards winning local and global opinion.[28] And in the evolving threat landscape, elements of information warfare have become increasingly integrated in launching cyber operations.[29] Throughout this paper, the term information warfare will be used more loosely to refer to the methodology or the approach used by the state to drive its strategic narrative and expand its influence.

The information environment is considered the battleground for information warfare. Competition in this environment occurs within the physical, informational, and cognitive/emotional domain in three distinct forms: propaganda operations, leak operations, and chaos-producing operations.[30] These three categorizations are not mutually exclusive and could reinforce each other to achieve the overall objectives of the strategic narrative. Social media plays a central role through social networking, propaganda as well as (fake) news and (dis)information sharing.[31] Information warfare is executed by building on existing narratives which are amplified through the network of bots to force the algorithm of the social media platform to make the elements that comprised the larger strategic narrative a trending topic.[32] Coercion and persuasion are often used as the decisive factors or key indicators to measure the impact and reach of information warfare.[33]

Initially, information warfare was conceived as a technology-oriented tactic deployed to gain information dominance, however, overtime, information transformed to become both the weapon as well as the target—making influence a critical aspect in the conduct of conflict.[34] In this setting, manipulation of information and its intended result of deception have become the centerpiece of the information warfare equation.[35] It is worth noting that human psyche plays a fundamental role to achieve the desired effects of information warfare. The interdependence that humans have built around the Internet can be leveraged to exploit their cognitive and affective biases, making them susceptible to misinformation and deception.[36] This makes information warfare a distinct type of warfare as it requires the exploitation of ICT systems and the vulnerabilities associated to political, economic and social discord particularly in free and democratic societies. Without the permissibility of political or socio-economic crisis, the deliberate use of information warfare lends itself ineffective to achieve psychological manipulation against adversaries.

China's Evolving Information Warfare

This section briefly surveys the transformation of China's approach to its information warfare from its early conception up until its newfound status as a rising power.

China has initially developed information warfare as an asymmetric weapon used by the People's Liberation Army (PLA) for longer-range power projection in response to its technological inferiority with the US in the aftermath of the Cold War.[37] Information warfare has been regarded as the neuro-system of the PLA which encompasses Command and Control, Communications, Computing, Intelligence, Surveillance, and Reconnaissance (C4ISR) even up to electronic and network warfare.[38] Strategic thinkers in the PLA have regarded information warfare as a fundamental aspect of the Revolution in Military Affairs. Rather than attempting to match the US strength in conventional military forces, the use of information warfare affords the PLA with a milieu of tactics which are deceptive, surprising, and decisive by design.[39] Its fundamental goal is information dominance—the ability to defend one's own network, while exploiting the vulnerabilities of the adversary.[40]

A clear distinction must be drawn when using information warfare in the context of US and China. While majority of US military experts view it as a way of fighting, Chinese experts on the other hand consider it as the fight itself.[41] General Wang Pufeng stated that "information war refers to a kind of war and a kind of war pattern, while information warfare refers to a kind of operation and operational pattern."[42] This primary distinction becomes obvious in the scope of application and limitation of these concepts in the strategic and operational context. Unlike the US military which only applies information warfare during conflict or crisis, the Chinese military considers it as an on-going pursuit.[43] The impact of such a distinction renders it as an "unconventional weapon and not a battlefield force multiplier," putting China at a strategic advantage to win information campaign without any need for military action.[44] This is rooted from the Chinese thinking of omnipresent struggle, a Maoist-Marxist-Leninist paradigm which

depicts China's enduring clash with the West which makes no clear distinction on wartime or peacetime.[45]

Chinese experts see conflict from violent and non-violent perspectives. The former occurs in the battlefield and is characterized as limited in scale, while the latter known as deterrence war takes up the majority of the space and time.[46] PLA analysts contend that the enemy is most vulnerable during the early phases of war, and thus, necessitates the effective launch of pre-emptive strikes. The notion of deterrence war which occupies the majority of space and time calls for the implementation of a preemptive strategy prior to the actual breakout of conflict.[47] The aegis of information warfare in the PLA's strategic doctrine as a pre-emptive strategy and asymmetric capability affirm its limited material capabilities to challenge the US dominance in the military domain in the aftermath of the Gulf War. It was a period that showcased the US technological superiority, standing in stark contrast to China's weak warfighting capabilities at that time. Although, there was momentum within the PLA to further develop its information warfare, China did not possess the adequate resources for research and development and the technological infrastructure to fully experiment and develop such capabilities.[48]

But nearly three decades later, China is now in the precipice of achieving great power status. It has emerged to become the second-largest economy in the world, inching closer to match the US in the world stage by all measure. Through its China model, the CCP has begun to highlight its unique path to development supported by its track-record of lifting millions of its population out of poverty. Relatedly, China's increasing competitiveness in the area of Artificial Intelligence, 5G, and other emerging technologies has made it a formidable rival against the US technological supremacy. These developments now afford China the capability to reinvigorate its information warfare capabilities.

Under the leadership of Xi Jinping the role of information warfare has become integral as the CCP views the challenges posed by cybersecurity and the flow of information against the regime's continuing existence and survival.[49] Xi views the internet as an ideological battlefield which strengthened his resolve to devote more resources to conduct "online public opinion work". During a Party conference in 2016 on public opinion work, Xi emphasized the urgency for China to construct an external discourse system that enhances its power status on the world stage.[50] For instance, the active promotion of China's model was viewed as an attempt by the CCP to challenge the hegemony of universal values.[51] In the present information age, the PLA has rapidly integrated psychological warfare, cyber warfare, and electronic warfare to influence the opponent's psychological behavior which could permeate all aspects from politics, economics, religion, culture, society to science and technology.[52] Winning without fighting has been the centerpiece of the PLA's ongoing work on discourse power, which requires the integration of the three types of warfare—public opinion, legal, and psychological—to complement and/or reinforce existing political and diplomatic struggle or in the advent of future wars.[53]

Strategic Narrative with Chinese Characteristics

China's renewed political, economic, and military strength in the world stage has enabled it to refashion its Information Warfare capabilities and drive its strategic narrative as a rising power centered around the promotion of the post-liberal order on multiple fronts at varying degrees. This section unpacks China's strategic narrative playbook with Chinese characteristics. Throughout the COVID-19 pandemic, China is exploiting the information environment across the physical, information, and cognitive domains. To systematically assess China's overall approach on its information warfare to spark international, domestic and policy discourse, the paper proposes three analytical tools: asset, tactics, and narrative.

Assets include the social media platforms that are used by China to conduct information warfare and promote its strategic narrative. As briefly mentioned, China's ability to exploit well-established American social media apps and the meteoritic rise of its own social media natives like TikTok affords it with more resources to undermine liberal values in open and democratic societies and promote its own agenda.

Tactics underscore the trends, patterns and techniques used to operationalize China's information warfare. Similar to cyber or network operations, the covert nature of information warfare complicates the process of attribution. Despite the active policies adopted by Facebook, Twitter, and Google to ban coordinated and inauthentic behaviors, well-resourced threat actor like China continue to adapt and experiment to minimize detection and achieve a level of legitimacy.

Lastly, *Narratives* probe the salient topics and themes that are injected through the information warfare tactics at the international, domestic, and issue-based level. Focusing on the elements of the strategic narrative underscores China's covert operations to leverage on the vulnerabilities that are present in the physical, informational and cognitive aspects of the online information environment.

Assets

China's current information warfare has become a sophisticated asymmetric capability with acquired potency and stealth due to its untethered potential to dominate the Fourth Industrial Revolution. China has developed its homegrown tech champions like Baidu, TenCent, Huawei, and Alibaba which in recent years has continued to gain traction as possible rivals to the US tech giants like Apple, Google, Facebook, Amazon, and Microsoft. However, the tipping point for China's information warfare came in 2019 following the breakthrough of TikTok, a social media app owned by Chinese company ByteDance.

A growing body of research has examined how Chinese-linked hackers and troll farms use Facebook, Twitter, YouTube, WhatsApp and Telegram as part of its information warfare to achieve its pursuit of National Rejuvenation towards Hong Kong, Taiwan, and in the territorial disputes in the South China Sea.[54] But the game-changer was China's successful penetration

of the US dominated social media landscape through its crown jewel—TikTok, a short video-sharing social media app that has gained global followers, especially in the US.

While majority of Western social media apps are still banned in China, TikTok has expanded beyond Chinese borders and captured a global market of 700 million users as of July, 2020.[55] As the first major international social media platform with Chinese roots, TikTok is becoming a powerful political actor capable of covertly controlling information flows across geographies and culture.[56] Due to its growing influence, the Trump administration viewed TikTok as a threat to the US national security due to its linkage with ByteDance.[57] The US alleges that TikTok can be used by China for espionage purposes given its access to millions of personal user data. President Trump has issued various executive orders demanding the divestment of the app's operation from its parent company and to find a suitable US partner if it aims to continue its operations.[58]

Amidst the perceived overreaction on the Trump administration's efforts to ban the app, a closer look at TikTok's operations reveals that such moves are warranted. The core algorithm that runs TikTok is mandated under the Chinese law to propagate the CCP's propaganda.[59] Having such extensive reach provides the CCP with a heavy hand to shape TikTok's global content moderation. ByteDance CEO Zhang Yiming has confirmed that the company's product and business lines are designed to promote CCP's agenda, including manipulating TikTok's core algorithm to reflect the party line and promote socialist core values.[60]

Tactics

Fundamental to understanding the execution of Chinese-linked information warfare are the tactics or techniques it has deployed to maximize various social media platforms. Over the course of the pandemic Facebook, Twitter, and YouTube were the major social media assets that were instrumental in China's information warfare to push for its favorable strategic narrative among foreign audiences. Meanwhile, TikTok has also started to gain traction. China was able to leverage on Facebook, Twitter, and YouTube for its information warfare to amplify its strategic narrative, while it facilitates censorship on TikTok to silence narratives that do not align with the CCP's broader agenda. China has used all of the identified social media apps to fan social unrest particularly in the US and other parts in the Indo-Pacific region to divert scrutiny away from the CCP's lack of transparency during the early onset of the pandemic.

Much of the information warfare tactics and techniques conducted by Chinese-linked trolls have morphed, and now rely not only on bots but also on personal accounts that exude a veneer of legitimacy. Clearly, inauthentic coordinated networks are still driven by networks of automatic bots, but the rise of pro-China patriotic trolls on social media platforms have also made it challenging to make a direct attribution of various information warfare campaigns.[61] There is a growing cross-posting strategy from Facebook to Twitter that uses repurposed accounts. While China's campaign operators are purchasing the bulk of user accounts in Facebook and Twitter that were based in Bangladesh, Russia, Indonesia, and France,[62] but it

was also observed that there is a growing propensity to use Facebook pages rather than individual user accounts which is a new type of asset experimentation. Although Facebook fan pages could result into more traction, it will most likely be mixed with individual accounts to maintain a degree of diversity.[63]

Aside from Facebook and Twitter, YouTube has also become a critical tool in ramping up China's information warfare. A pro-Chinese political spam network called *Spamouflage dragon* was spreading English-language videos that were critical of the Trump administration's tit-for-tat policies against China.[64] The network was initially spotted in 2019 focusing on the Hong Kong protests and by early 2020 it has started to post videos which are critical of the US government's inadequate response to the coronavirus pandemic.[65]

China's information warfare extends beyond the digital realm and, includes all the other available tools—political, economic, and diplomatic—at its disposal to inculcate the major themes and key elements of its strategic narrative.[66] In light of the global backlash following its mismanagement of the virus, the Chinese Academy of Sciences has crafted a coordinated and coherent messaging strategy among Chinese diplomats and state-owned media which offers a wide range of responses. This include aggressive media monitoring and rapid response; promoting the use of diverse sources; supporting Chinese social media like Weibo, WeChat, and Douyin; targeting specific audiences through enhanced means of communication; and cultivating foreign talents.[67] Although there is a general consensus that Western social media platforms are central elements of Chinese information warfare, CCP's potential control of TikTok's global content policies equips the Chinese government an unrestricted apparatus to boost and complement its strategic narrative.

Narrative

China's information warfare has evolved throughout the course of the pandemic. Although the strategic narrative has initially focused in containing the global backlash it has received, it has immediately shifted gears by painting itself as a responsible stakeholder through its cooperation with the World Health Organization (WHO). China eagerly established the credibility of its approach in the early stages of the pandemic by highlighting its sacrifices during the initial lockdown as the model for the world to emulate to contain the outbreak.[68] Chinese diplomatic and state-owned media's online accounts boosted this narrative about China's upbeat performance against COVID-19 and compared it to the lackluster response made by the US and Europe, and even highlighted its ongoing cooperation with regional groupings such as ASEAN, Arab League, and the African Union.[69] China's top diplomats Lijian Zhao and Hua Chunying also exploited the mounting criticisms levied by the US against the WHO. For instance, while the US President Donald Trump's threatened to defund and even pull out from the WHO, Hua Chunying asserted China's commitment and its level of transparency with the WHO.[70] The specific tweet from the Chinese Ministry of Foreign Affairs was also amplified by state-run media CGTN and Xinhua. Additionally, Chinese-linked accounts also constructed a narrative

that accused the US behavior as 'selfish, foolish, and destructive', compared to China's good behavior in supporting international cooperation through WHO.[71]

China has also used the COVID-19 pandemic to reaffirm its One China principle and downplay Taiwan's impressive performance to contain the virus. A coordinated anti-Taiwan trolling emerged following Dr. Tedros Adhamon, the WHO Director-General, accused Taiwan of racial attacks. There were 65 accounts pretending to be Taiwanese netizens who offered apologies to Tedros with the hashtag #saysrytoTedros.[72] A network analysis of the accounts revealed a cluster of commonly followed accounts which were classified as inauthentic. Taiwan's Investigation Bureau Cybersecurity Head Chang Yu-jen confirmed that Chinese trolls were behind the fake posts aimed to put Taiwan as the culprit behind the coordinated racist abuse against Dr. Tedros.[73] The Twitter accounts that were fomenting the racism spat with the WHO chief were also discovered to be part of a larger campaign that has begun in early 2020.[74] Most of these accounts mimicked or trolled Western media outlets to mislead readers and harass real accounts by responding with abusive replies or asserting that the troll account was authentic.[75]

Throughout the pandemic, China has been relentless in undermining the US' reputation and credibility amidst their ongoing strategic rivalry. There were 62 identified accounts on Facebook and 200-300 Twitter users who posted, shared and retweeted similar narratives which started as early as February 2020.[76] The inauthentic, cross-platform campaigns were believed to be conducted by Chinese-affiliated actors, which targeted Western and US-based audiences to drive divisive or negative narratives against the US, primarily the Trump administration's COVID-19 response, and the spiraling tension in the US-China relations. A further investigation on Facebook and YouTube revealed on-going inauthentic activities with similar themes that centered around the Trump administration's mishandling of the outbreak, threats to ban TikTok in the US,[77] increasing tension from the Black Lives Matter protests, and the heightened anticipation of the US presidential elections.[78] Google's Threat Analysis Group has removed a total of more than 2,000 channels that exhibited coordinated influence operations that were tracked back to China.[79] According to William Evina, Director of the National Counterintelligence and Security Center, China expanded its influence efforts ahead of the US elections by emphasizing the Trump administration failures in managing the pandemic.[80] The Chinese narrative mirrored the commentaries of Western-liberal media against President Trump's mismanagement of the coronavirus in the US. However, the information warfare component is based on the coordinated and inauthentic tactics that were used to amplify the content. Key issues central to the narratives accused President Trump's denial about the severity of the virus and manipulation on the real statistics on the spread of the virus that led to hundreds of thousands of deaths.[81] Indeed, the impact of Trump's disastrous performance in managing the outbreak was also a frequent theme discussed or promoted online.[82]

Some campaigns were also attempting to ignite conspiracy theories on the origin of the virus. An article that circulated on Twitter purports the Fort Detrick theory, which asserts that the coronavirus originated from the Fort Detrick Lab in Maryland, and resembles the same China-state apparatus conspiracy talking points.[83] TikTok was under fire for circulating baseless assertions regarding the public health crisis. For instance, some users were claiming that Microsoft CEO Bill Gates and his non-profit organization at the Pirbright Institute based in the UK were connected to the coronavirus outbreak.[84]

Chinese-linked trolls were also actively stoking racial divisions after the viral news surrounding the death of George Floyd by amplifying the eruption of Black Lives Matter protests in the US. Content showing a black protester resisting a white counter-protester were shared excessively over in Facebook and Twitter to exacerbate racial divide.[85] In contrast, TikTok was engaged in censoring content that are related to the George Floyd protests that used the hashtag #acab, which stands for "all cops are bastards".[86] Following a public outcry on its censorship, TikTok immediately restored the hashtags related to the protests. But a few months later, TikTok continued to ban anti-racism and anti-police brutality protests after a surge on social media activity spiked. Following the police shooting of Jacob Blake, the hashtag #acab was once again censored.[87]

China's Strategic Narrative in the New Normal

Despite China's rapid emergence to great power status marked by its rapid accumulation of conventional military capabilities across all domains, the role of asymmetric capabilities remains a centerpiece in the CCP's regime survival and triumph. Three decades after China's early conception of information warfare as an asymmetric capability, the PLA continues to see its indispensable value against the technologically capable US. As it rapidly becomes a well-resourced state actor, China has been relentless in refining the force-multiplier effect of such capability to be more sophisticated and highly suited in today's hyperconnected world.

In this article, the analysis of China's information warfare throughout the pandemic unveils its unique approach in promoting its strategic narrative that echoes its global ambition as a new superpower. The fallout from its lack of transparency at the onset of the pandemic served as the impetus for China to employ its information warfare at such unprecedented level, unleashing a whole-of-CCP approach, which was orchestrated by its large networks of automated bots, paid campaign operators, the Chinese diplomatic community, and state-owned media all working in unison. The CCP aimed to shift the ire of blame by promoting instead its narrative of triumph against the coronavirus. It was able to capitalize on such a vulnerable spot to project its China model worth emulating in the ongoing public health crisis by juxtaposing it to the US' lackluster performance.

The whole-of-CCP approach will be fundamental to China's emerging strategic narrative in the new normal designed to achieve two-fold: first, to mitigate the impact of worsening

international perception given the uncertainty in the post-COVID-19 era especially as China prepares for a protracted war with the US in the coming decades. Second, to consistently capitalize on the eruption of unexpected crises in the international landscape to advance and highlight the superiority of its Chinese model. The CCP will continue to advance elements of the post-liberal order to depict the decline of a Western-centric order which is incapable of withstanding the disruptive effects of black swan events in international politics. And fundamental to the future of China's information warfare is the stratified approach to propagating its strategic discourse across international, domestic and policy-oriented narratives. Chinese experts will continue to experiment on their tactics and themes including the integration of cyber or network operations and information warfare with emerging technologies to achieve more sophisticated outcomes.

The current trends assessed in this article surrounding China's information warfare points to its future trajectory as it becomes even more vital and stealthy in nature. The breakthrough of TikTok into the mainstream and global social media arena that is largely dominated by Facebook and Twitter provides the CCP with a new platform to elevate its information warfare to a different level. China's revised export control law which covers the Algorithms and AI embedded on TikTok demonstrates the centrality of the app and other emerging Chinese-tech towards winning the global public opinion and reaching its ambition for national rejuvenation in the years to come. Having such unprecedented control over TikTok, China can now directly export its strategic narrative with lesser constraints across the world. It will aim to normalize censorship against narratives that are inimical to the CCP's authoritarian ideals which sets a dangerous precedent in threatening the core notion of 'free speech' in open and democratic societies. As more countries raise concerns on Facebook, Twitter and YouTube's community guidelines, TikTok could be a viable alternative. TikTok's content moderation policies that are synonymous to censorship might be appealing among developing countries that lean towards censoring content and/or anemic to the universal application of free speech.

The future of the Internet appears to be bleak. As countries like China and the US push their respective strategic narratives, a China- or US-approved Internet might eventually be established in the years ahead. If this transpires, China's vision for a post-liberal society will materialize and contradicts the very same ideals upon which the Internet was founded on—openness, transparency, and collaboration. Thus, the key to combatting the increasing prevalence of information warfare as it becomes part of the new normal lies in these same virtues. Encouraging transparency across all social media platforms whether on their community guidelines and policies, content moderation and algorithms is imperative. Social media and tech companies must regularly disclose any information warfare campaigns prevailing in their networks and systems to raise public awareness and resilience among social media users against potential manipulation or deception. Lastly, combatting information warfare

must be a collaborative venture, enjoining government agencies, tech companies, academia, and civil society organizations to create an information warfare-proof Internet based on accountability frameworks through periodic assessments that could safeguard user-data privacy and protection.

NOTES

1. Mark Bryan Manantan is the Lloyd and Lilian Vasey Fellow at the Pacific Forum, and concurrently a non-resident fellow at the Center for Southeast Asian Studies, National Chengchi University in Taiwan. You can reach him at brymanmedia@gmail.com.
2. Max Smeets and Stefan Soesanto, "Cyber Deterrence Is Dead. Long Live Cyber Deterrence!" Council on Foreign Relations, last modified February 18, 2020, https://biblioteca.fba.up.pt/form_utilizadores/Purdue_OWL_Chicago.pdf.
3. Alexander Spangher, Gireeja Ranade, Besmira Nushi, Adam Fourney, Eric Horvitz, "Analysis of Strategy and Spread of Russia-sponsored Content in the US in 2017," *Social and Information Networks*, last modified October 23, 2018, https://arxiv.org/abs/1810.10033; Scott Shane, "The Fake Americans Russia Created to Influence the Election," *New York Times*, last modified September 7, 2017, http://cs.brown.edu/people/jsavage/VotingProject/2017_09_07_NYT_TheFakeAmericansRussiaCreatedToInfluenceTheElection.pdf; Tom McCarthy, "Facebook, Google and Twitter grilled over Russian meddling—as it happened," *The Guardian*, last modified October 31, 2017, https://www.theguardian.com/technology/live/2017/oct/31/facebook-google-twitter-congress-russian-election-meddling-live.
4. Foo Yan Chee, "Google, Facebook, Twitter have to do more fight fake news: EU," *Reuters*, last modified last April 23, 2019, https://www.reuters.com/article/us-eu-tech-fakenews-idUSKCN1RZ0WU.
5. Laura Silver, Kat Delvin, and Christine Huang, "Unfavorable Views of China Reach Historic Highs in Many Countries," Pew Research, last modified October 6, 2020. https://www.pewresearch.org/global/2020/10/06/unfavorable-views-of-china-reach-historic-highs-in-many-countries/.
6. Robert Mueller III, "Report on the Investigation into Russian interference in the 2016 President Election," *US Department of Justice*, March 2019, https://www.justice.gov/storage/report.pdf; "Government response to the Intelligence and Security Committee of Parliament report 'Russia'," *Intelligence and Security Commitment*, July 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/902342/HMG_Russia_Response_web_accessible.pdf.
7. Jessica Brand and Torrey Taussig, "The Kremlin's disinformation playbook goes to Beijing," B*rookings*, last modified May 19, 2020, https://www.brookings.edu/blog/order-from-chaos/2020/05/19/the-kremlins-disinformation-playbook-goes-to-beijing/.
8. Alister Miskimmon, Ben O'Loughlin, and Laura Roselle. S*trategic Narratives: Communication Power and the New World Order.* (New York: Routledge, 2017), 2; Alice Ba, "China's "Belt and Road" in Southeast Asia: Constructing the Strategic Narrative in Singapore," A*sian Perspective* 43 (2019): 253. https://doi.org/10.1353/apr.2019.0010.
9. Natalia Chaban, Alister Miskimmon, and Ben O'Loughlin, "The EU's Peace and Security Narrative: Views from EU Strategic Partners in Asia," *Journal of Common Market Studies* 55 (2017): 1274. doi:10.1111/jcms.12569.;
10. Chaban et al., "The EU's Peace and Security Narrative," 1274.
11. Laura Roselle, Alister Miskimmon, and Ben O'Loughlin, "Strategic narrative: A means to understand soft power," *Media, War and Conflict*, 7 (2014): 12, doi:10.1177/1750635213516696.
12. Miskimmon et. al, S*trategic Narratives: Communication Power and the New World Order,* 12.
13. Roselle, et. al, Strategic narrative: A means to understand soft power," 77.
14. Alice Ba, "China's "Belt and Road" in Southeast Asia: Constructing the Strategic Narrative in Singapore," 252.
15. Roselle, et al., Strategic narrative: A means to understand soft power," 74.
16. Ibid., 75.
17. Ibid., 74.
18. Ibid., 76.
19. Caitlin Byrne, "Securing the 'Rules-Based Order' in the Indo-Pacific," *Institute for Regional Security*, 16 (2020), https://www.jstor.org/stable/10.2307/26924333.
20. Fareed Zakaria, "The Rise of Illiberal Democracy" *Foreign Affairs* 76 (1997).
21. Andre Barrinha and Thomas Renard, "Power and diplomacy in the post-liberal cyberspace," 4.
22. Ibid., 6.
23. Andrew Jacobs, Michael Shear, and Edward Wong, "US-China Feud Over Coronavirus Erupts at World Health Assembly," *New York Times*, last modified May 18, 2020, https://www.nytimes.com/2020/05/18/health/coronavirus-who-china-trump.html.
24. Ibid.

NOTES

25. Kalathmika Natarajan, "Digital Public Diplomacy and a Strategic Narrative for India," *Strategic Analysis* 38 (2014), https://www.tandfonline.com/doi/abs/10.1080/09700161.2014.863478.
26. Martin Libicki, "The Convergence of Information Warfare" *Strategic Studies Quarterly* 11 (2017),

https://www.jstor.org/stable/pdf/26271590.pdf?refreqid=excelsior%3Af342323547ec27f92fcd6c3eb5839946.

27. Herbert Lin and Jaclyn Kerr, "On Cyber-Enabled Information Warfare and Information Operations", SSRN, (2019), 4, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015680&download=yes.
28. Yeygeniy Golovchenko, Mareike Hartmann, and Rebecca Adler-Nissen, "State media and civil society in the information warfare over Ukraine: citizen curators of digital disinformation," *International Affairs* 94 (2018), https://academic.oup.com/ia/article/94/5/975/5092080.
29. Martin Libicki, "The Convergence of Information Warfare."
30. Herbert Lin and Jaclyn Kerr, "On Cyber-Enabled Information Warfare and Information Operations."
31. Jarred Prier, "Commanding the Trend: Social Media as Information Warfare," Strategic Studies Quarterly 11 (2017), https://www.jstor.org/stable/26271634?seq=1#metadata_info_tab_contents.
32. Jarred Prier, "Commanding the Trend: Social Media as Information Warfare."
33. Ibid.
34. William Hutchinson, "Information Warfare and Deception," *Informing Science*, 2006, http://inform.nu/Articles/Vol9/v9p213-223Hutchinson64.pdf?q=deception.
35. William Hutchinson, "Information Warfare and Deception."
36. Miguel Alberto Gomez, "Cyber-Enabled Information Warfare and Influence Operations. A revolution in Technique?" *Information Warfare in the Age of Cyber Conflict*, ed., Christopher Whyte et al., (New York: Routledge, 2020), 133.
37. James Mulvenon, "The PLA and Information Warfare," in *The People's Liberation Army in the Information Age*, ed. James C. Mulvenon and Richard Yang, (Santa Monica, CA: RAND Corporation, 1999), 176.
38. Chris Wu, "An Overview of the Research and Development of Information Warfare in China," in *Cyberwar, Netwar and the Revolution in Military Affairs,* ed. Edward Halpin, et.al., (London: Palgrave MacMillan, 2006). https://link.springer.com/chapter/10.1057%2F9780230625839_11.
39. Vincent Wei-Cheng Wang, "Asymmetric War? Implications for China's Information Warfare Strategies," Ithaca College (2002), https://digitalcommons.ithaca.edu/cgi/viewcontent.cgi?article=1015&context=politics_faculty_pubs.
40. James Mulvenon. "The PLA and Information Warfare," 180.
41. Barrington Barrett, Jr., "Information Warfare: China's Response to U.S. Technological Advantages," *International Journal of Intelligence and CounterIntelligence* 18 (2006), 684.
42. Barrington Barrett Jr., "Information Warfare: China's Response to U.S. Technological Advantages," 684.
43. Ibid., 685.
44. James Mulvenon. "The PLA and Information Warfare," in The People's Liberation Army in the Information Age, 183.
45. Mark Bryan Manantan, "The People's Republic of China's Cyber coercion: Taiwan, Hong Kong, and the South China Sea," Issues and Studies 56 (2020), https://doi.org/10.1142/S1013251120400135.
46. Barrington Barrett, Jr., "Information Warfare: China's Response to U.S. Technological Advantages," 685.
47. James Mulvenon. "The PLA and Information Warfare," in *The People's Liberation Army in the Information Age*, 183-184.
48. Chris Wu, "An Overview of the Research and Development of Information Warfare in China."
49. Elsa Kania, "The Ideological battlefield: China's approach to political warfare and propaganda in an age of cyber conflict"," in *Information Warfare in the Age of Cyber Conflict*, ed. Christopher Whyte et al., (New York: Routledge, 2020).
50. Elsa Kania, "Ideological Battlefield".
51. Ibid.
52. Ibid.
53. Ibid.
54. Mark Bryan Manantan, "The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea."
55. Fergus Ryan, Audrey Fritz, and Daria Impiombato, "TikTok and WeChat," *Australian Strategic Policy Institute*, last modified September 8, 2020, https://www.aspi.org.au/report/tiktok-wechat, 3.

NOTES

56. Fergus Ryan, Audrey Fritz, and Daria Impiombato, "TikTok and WeChat," 3-4.
57. Justin Sherman, "Unpacking TikTok, Mobile Apps and National Security" *Lawfare*, last modified April 2, 2020, https://www.lawfareblog.com/unpacking-tiktok-mobile-apps-and-national-security-risks.
58. Nikki Carvajal and Caroline Kelly, "Trump issues order banning TikTok and WeChat from operating in 45 days if they are not sold by Chinese parent companies," *CNN*, last modified August 7, 2020, https://edition.cnn.com/2020/08/06/politics/trump-executive-order-tiktok/index.html
59. Fergus Ryan, Audrey Fritz, and Daria Impiombato, "TikTok and WeChat,"18.
60. Ibid., 18-19.
61. Jake Wallis, Tom Uren, Elise Thomas, Albert Zhang, Dr. Samantha Hoffman, Lin Li, Alex Pascoe, and Danielle Cave, "Retweeting through the great firewall," *Australian Strategic Policy Institute*, last modified June 11, 2020. https://www.aspi.org.au/report/retweeting-through-great-firewall, 19.
62. Jake Wallis, Tom Uren, Elise Thomas, Albert Zhang, Dr. Samantha Hoffman, Lin Li, Alex Pascoe, and Danielle Cave, "Retweeting through the great firewall," 22-23.
63. Ibid.
64. Ben Nimmo, Camille Francois, C. Shawn Eib and Lea Ronzaud, "Spamouflage Goes to America," *Graphika*, last modified August 2020, https://public-assets.graphika.com/reports/graphika_report_spamouflage_goes_to_america.pdf, 1-2.
65. Ben Nimmo, Camille Francois, C. Shawn Eib and Lea Ronzaud, "Spamouflage Goes to America," 3-11.
66. Mark Bryan Manantan, "The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea."
67. Wallis, et al, "Retweeting through the great firewall," 5.
68. "Covid-19 disinformation and social media manipulation trends," 3.
69. Ibid.
70. "Covid-19 disinformation and social media manipulation trends," *Australian Strategic Policy Institute*, last modified April 15, 2020, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-04/COVID-19%20Disinformation%20%26%20Social%20Media%20Manipulation%20Trends%208-15%20April.pdf?LK2mqz3gNQjFRxA21oroH998enBW__5W=, 2.
71. Elise Thomas, Albert Zhang, and Dr. Jake Wallis, "Viral Videos: Covid-19, China, and inauthentic influence on Facebook," *Australian Strategic Policy Institute*, last modified September 29, 2020, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-09/Viral%20videos.pdf?oRBhvSURmY5drwKr_EbnIZq6eu_87CKh= , 14.
72. "Covid-19 disinformation and social media manipulation trends," *Australian Strategic Policy Institute*, 2.
73. Samson Ellis, "Taiwan Accuses Chinese Trolls of Fomenting Racism Spat with WHO," *Bloomberg,* last modified April 10, 2020, https://www.bloomberg.com/news/articles/2020-04-10/taiwan-accuses-chinese-trolls-of-fomenting-racism-spat-with-who.
74. Elise Thomas and Albert Zhang, "COVID-19 Attacks Patriotic Troll Campaigns in Support of China's Geopolitical Interests," *Australian Strategic Policy Institute*, last modified June 11, 2020, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/202004/Patriotic%20Troll%20Campaigns%20Report_ASPI%20Cyber.pdf?3UM1P9V4gVpAacBYaf7zxRM9HM-la_twV=, 3
75. Elise Thomas and Albert Zhang, "COVID-19 Attacks Patriotic Troll Campaigns in Support of China's Geopolitical Interests," 2.63
76. Elise Thomas, Albert Zhang, and Dr. Jake Wallis, "Automating Influence on COVID-19," *Australian Strategic Policy Institute*, last modified August 24, 2020, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-08/Automating%20influence%20on%20Covid-19.pdf?DxaB4psM9BvTNrhNQNTpu_jWNWmqPGXg=.
77. Elise Thomas, Albert Zhang, and Dr. Jake Wallis, "Viral Videos: Covid-19, China, and inauthentic influence on Facebook," *Australian Strategic Policy Institute*, last modified September 29, 2020, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-09/Viral%20videos.pdf?oRBhvSURmY5drwKr_EbnIZq6eu_87CKh= .
78. Thomas, et al., "Automating Influence on COVID-19," 6-10.
79. Thomas, et al., "Viral Videos: Covid-19, China, and inauthentic influence on Facebook".
80. Office of the Director of National Intelligence, "Statement by NCSC Director William Evanina: Election Threat Update for the American Public," *Press Release*, August 7, 2020, https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public

NOTES

81. Thomas, et al., "Viral Videos: Covid-19, China, and inauthentic influence on Facebook," 12-14.
82. Ibid.
83. Thomas, et al., "Automating Influence on COVID-19," 6-7.
84. Dawn Chmielewski, "TikTok Used To Spread Misinformation About The Coronavirus," *Forbes*, last modified January 28, 2020, https://www.forbes.com/sites/dawnchmielewski/2020/01/28/tiktok-used-to-spread-misinformation-about-the-coronavirus/#5ed32ac916d6.
85. Thomas, et al., "Automating Influence on COVID-19," 3; Thomas, et al., "Viral Videos: Covid-19, China, and inauthentic influence on Facebook".
86. Fergus Ryan, Audrey Fritz, and Daria Impiombato, "TikTok and WeChat," 9.
87. Ibid.