

# China's Gambit for Total Information Dominance: A US-Australia Response

PATRICK M. CRONIN

ASIA-PACIFIC SECURITY CHAIR, HUDSON INSTITUTE



© 2021 Hudson Institute, Inc. All rights reserved.

## **ABOUT HUDSON INSTITUTE**

Hudson Institute is a research organization promoting American leadership and global engagement for a secure, free, and prosperous future.

Founded in 1961 by strategist Herman Kahn, Hudson Institute challenges conventional thinking and helps manage strategic transitions to the future through interdisciplinary studies in defense, international relations, economics, health care, technology, culture, and law.

Hudson seeks to guide public policy makers and global leaders in government and business through a vigorous program of publications, conferences, policy briefings and recommendations.

Visit [www.hudson.org](http://www.hudson.org) for more information.

**Hudson Institute**  
1201 Pennsylvania Avenue, N.W.  
Fourth Floor  
Washington, D.C. 20004

+1.202.974.2400  
[info@hudson.org](mailto:info@hudson.org)  
[www.hudson.org](http://www.hudson.org)

Cover: A woman uses her mobile phone to take a picture during a visit to the Chinese Military Museum in Beijing on September 8, 2017. (Wang Zhao/AFP via Getty Images)

# China's Gambit for Total Information Dominance: A US-Australia Response

PATRICK M. CRONIN

ASIA-PACIFIC SECURITY CHAIR, HUDSON INSTITUTE



# ABOUT THE AUTHOR



**Dr. Patrick M. Cronin** holds the Chair for Asia-Pacific Security at the Hudson Institute. Before joining Hudson in January 2019, he was the Senior Director of the Asia-Pacific Security Program at the Center for a New American Security (CNAS). Previously, he headed the Institute for National Strategic Studies (INSS) at the National Defense University, where he also oversaw the Center for the Study of Chinese Military Affairs. Before leading INSS, Dr. Cronin served as the Director of Studies at the London-based International Institute for Strategic Studies (IISS); Senior Vice President and Director of Research at the Center for Strategic and International Studies (CSIS); the third-highest ranking official at the US Agency for International Development (USAID); the Director of Research at the US Institute of Peace; and an intelligence officer in the US Navy Reserve.

Dr. Cronin is the author of many publications on the United States and Asian security. His recent major works include *Fear and Insecurity: Addressing North Korean Threat Perceptions* (Hudson Institute, 2021); *Pathways to Peace: Achieving the Stable Transformation of the Korean Peninsula* (co-author; Hudson Institute, 2020); *Total Competition: China's Challenge in the South China Sea* (co-author; CNAS, 2020); *The Cornerstone and the Linchpin: Securing America's Alliances in Northeast Asia* (Hudson Institute, 2019); *Contested Spaces: A Renewed Approach to Southeast Asia* (co-author; CNAS, 2019); *Negotiating with North Korea: How Will This End?* (co-author; CNAS, 2019); *A Precarious Accord: Navigating the Post-Summit Landscape* (co-author; CNAS, 2018); *Networking Asian Security: An Integrated Approach to Order in the Pacific* (co-author, CNAS, 2017); *Beyond the San Hai: Implications of China's Emerging Blue-water Navy* (co-author; CNAS, 2017); *Averting Disengagement: A Geoeconomic Strategy for the Trump Administration in Southeast Asia* (co-author; CNAS, 2017); *Breakthrough on the Peninsula: Third Offset Strategies and the Future Defense of Korea* (editor and co-author; CNAS, 2016); *Counterbalance: Red Teaming the Rebalance in the Asia-Pacific* (co-author; CNAS, 2016); *Power and Order in the South China Sea: A Strategic Framework for U.S. Policy* (CNAS, 2016); *Sustaining the Rebalance in Southeast Asia: Challenges and Opportunities Facing the Next Administration: Papers for the Next President* (CNAS, 2016); *Dynamic Balance: An Alliance Requirements Roadmap for the Asia-Pacific Region* (co-author; CNAS, 2016); *Solving Long Division: The Geopolitical Implications of Korean Unification* (co-author; CNAS, 2015); *Preserving the Rules: Countering Coercion in Maritime Asia* (co-author; CNAS, 2015); *If Deterrence Fails: Rethinking Conflict on the Korean Peninsula* (CNAS, 2014); and *Tailored Coercion: Competition and Risk in Maritime Asia* (co-author; CNAS, 2014).

# TABLE OF CONTENTS

Chapter 1: Introduction	7
Chapter 2: Diplomatic and Political Information	10
Persuasion	11
Covert Influence Operations	12
Discourse Power	14
Chapter 3: Economic and Technological Information	21
The Data Economy Era	21
From Made in China 2025 to Vision 2035	25
A Digital Superpower	29
Chapter 4: Security and Military Information	31
China's Total Security Paradigm	31
Exploiting the Gray Zone	34
System vs. System Warfare	35
Chapter 5: Pillars of a Democratic Grand Strategy	37
Countering Coercion with Collective Strength	38
Enhancing High-Tech Competitiveness	39
Shaping International Standards and Institutions	40
Waging Democratic Information Operations	41
A Confederated Innovation Base	42
Chapter 6: Policy Recommendations: An Alliance Information Action Agenda	43
Political and Diplomatic Responses	44
Economic and Technological Responses	45
Security and Military Responses	48
Endnotes	51







## CHAPTER 1: INTRODUCTION

**“THE FUTURE LIES [WITH THOSE] WHO CAN OWN THE FUTURE AS IT RELATES TO TECHNOLOGY... [AND] INDUSTRIES OF THE FUTURE—ARTIFICIAL INTELLIGENCE, QUANTUM COMPUTING, BIOTECH.... CHINA IS OUT INVESTING US BY A LONGSHOT, BECAUSE THEIR PLAN IS TO OWN THAT FUTURE... WE’RE IN THE MIDST OF A FOURTH INDUSTRIAL REVOLUTION OF ENORMOUS CONSEQUENCE.”**

**—PRESIDENT JOE BIDEN, WHITE HOUSE PRESS CONFERENCE, MARCH 25, 2021<sup>1</sup>**

China’s reemergence as a major power is driving economic opportunities while simultaneously raising global security

concerns. China is too important and its economy too large for it to be contained. However, blunting its more malign behavior should be a national security priority for the United States and key allies such as Australia. In particular, Beijing’s desire to achieve total information dominance in this area, catching up and overtaking the United States, should concern democratic Five Eyes intelligence-sharing allies and all others who wish to preserve their strategic autonomy. In the context of this study, total information dominance is defined as the ability of an actor to collect data and employ information and digital technology

---

Photo: Chairman of the Chinese Communist Party Xi Jinping, top center, waves to the crowd after his speech above the portrait of the late Chairman Mao Zedong above Tiananmen Gate at a ceremony marking the 100th anniversary of the Communist Party on July 1, 2021 at Tiananmen Square in Beijing, China. (Kevin Frayer/Getty Images)

for political, economic, and military objectives with greater success than their rivals. Allowing China to gain information dominance could have far-reaching effects and pose new political, economic, and military risks. This report outlines the scope of China's total information competition and proposes a starting point for an effective US-Australian response.

China's national rejuvenation hinges on the power of information. Permeating every aspect of China's total security strategy, information enables Beijing to harness all policy instruments short of war so as, ideally, to prevail without having to fight, but should fighting become necessary, to win. As it is essential for domestic political stability, the Chinese Communist Party (CCP) believes its survival depends on its having information,<sup>2</sup> making its possession as not only an external priority. Driving foreign intelligence, diplomacy, and influence operations, information contributes to the creation of regional and global order—as well as international standards and institutions and thereby enables China to protect its interests and expand its clout. Since information undergirds economic strength, today's economic competition hinges on advanced information and communications technology (ICT), artificial intelligence (AI), and quantum computing. Information-centric systems can also aid in securing a favorable military balance, since commercial technologies provide the basis for most military innovations. Amid an ongoing fourth industrial revolution, information plays an increasingly decisive role in prepping the battlefield, fielding superior military power, and, if necessary, winning a conflict in an informatized environment. But China's dream centers less on winning war than owning the future.

Despite the importance of information power in the twenty-first century, this concept's scope is large and difficult to grasp in its entirety. Moreover, studies in information power tend to concentrate on discrete issues rather than overall strategic implications, with analyses often balkanized into separate topics related to public diplomacy (influence operations), the Internet (cybersecurity), and military command and control (command,

control, communications, computers, intelligence, surveillance, and reconnaissance or C4ISR). This report, which builds on earlier research, assesses China's comprehensive approach to information power and this approach's implications for the US-Australia alliance.<sup>3</sup> Therefore, this report's purposes are threefold:

1. Enlarge alliance awareness of China's whole-of-society information challenge;
2. Highlight critical responses to this challenge from Canberra and Washington; and
3. Deepen alliance thinking regarding strategy and policy.

Because of the breadth of the impact on the alliance caused by China's information power, this report underscores selected challenges and responses and is not encyclopedic. However, Australia and the United States would benefit from broad consideration of China's growing information challenge and how the two allies can improve their ability to compete, be resilient, and defend against information-related threats.

At the outset, China's goals and its capabilities do not necessarily match. Aspiring to total information dominance is not the same as achieving it. Beijing faces nearly insurmountable obstacles in seeking to accomplish all of its technological and policy ambitions. Many of China's aspirations center on catching up with the United States, which, along with its allies, is not idle in this regard. Also, China's focus on information reflects the CCP leadership's extensive vulnerabilities, both real and perceived. Even if China achieves some of its goals of information dominance, that dominance does not necessarily translate into clear-cut victory. The information domain is vast and always contested, and there will always be a countervailing argument or lingering doubt about the actual "balance of information power."

Notwithstanding these caveats, the threat from China's pursuit of information dominance is palpable and mounting. As China



swiftly emerges as an information superpower, consider the types of behavior that have been or are still underway:

- Use of cyber espionage and other means of intellectual property theft to close the technological gap with more advanced nations;
- Employment of a Military-Civil Fusion industrial policy designed to ensure that China's national champion companies surpass foreign rivals in wealth and technological innovation;
- Buffeting Australia and other countries with caustic, "wolf warrior" diplomacy to reinforce coercive economic pressure designed to bring about their acquiescence to Beijing's policies;
- Mobilization of United Front Work Department organizations to silence unwanted criticism and policies from democratic societies;
- Hoovering big data and creation of the algorithmic means to influence opinions, interfere with decision-making, and build foreknowledge;
- Conducting global influence operations with Chinese narratives that depict China's inexorable rise and America's inevitable decline intended to divide democratic alliances and sap the political will to respond to China's assertiveness; and
- In advance of a crisis, gaining access to information systems in ways that could embolden China's policymakers and possibly pre-determine the outcome.

In short, even though China is "not hell-bent on world domination,"<sup>4</sup> its behavior of capturing greater information power at the expense of the United States and its allies is worrisome, as the PRC leverages information power to maximize its influence and control over an increasingly contested Indo-Pacific region. The stakes are

high, and past responses have been insufficient to keep pace with China's information technology and power juggernaut.

Examining the integrated components of China's use of information power can aid in analyzing the challenge, and so this study dissects China's use of information power into three broad categories: 1) diplomatic and political information; 2) economic and technological information; and 3) security and military. While connections across categories lead to some duplication, the binning of China's actions into one or more of these groups highlights Beijing's various interests and will help identify effective alliance responses. In addition, the recommendations provided in the final section of the report provide a specific agenda for the US-Australia alliance response.

Chapter 2 analyzes three related facets of China's approach to diplomatic and political information—persuasion, decentralized and covert influence operations, and discourse power. Chapter 3, which focuses on economic and technological elements of China's bid for information dominance, concentrates on Beijing's industrial party-state policies such as *Made in China 2025*, *Military-Civil Fusion*, and *Vision 2035*. Chapter 4 considers China's quest for security and military information through the prism of its total security paradigm, exploitation of gray zone competition below the threshold of traditional conflict, and system-versus-system warfare. Chapter 5 places an alliance response within the broader context of a democratic grand strategy comprised of collective strength, high-technology competitiveness, international leadership, offensive information operations, and collaborative innovation. Chapter 6 offers an alliance information agenda with thirteen actionable recommendations. As daunting as China's gambit for information dominance is, there are numerous ways to overcome it.



## CHAPTER 2: DIPLOMATIC AND POLITICAL INFORMATION

All states employ information for political objectives. What distinguishes China from other countries is the scale and scope of its information enterprise. Overt persuasion campaigns and decentralized and covert influence operations are thoroughly researched, carefully choreographed, and uninhibited by concerns over individual or sovereign rights. Beijing goes beyond the use of information and instead seeks to achieve primacy in discourse power by weaponizing narrative in ways analogous to asymmetric military strategies.

This chapter focuses on the diplomatic and political dimensions of China's use of information and divides the subject into three areas: use of persuasion, information operations, and the power of discourse. Also illustrated is Chinese weaponization of narrative integrated with economic

and other instruments of power to turn brand power to geopolitical advantage, of which China's varying responses to COVID-19 and Xi Jinping's signature One Belt One Road initiative are cases in point. Power is the ability to influence the behavior of others, and the Chinese have long been adept in the art of persuasion.

---

Photo: Deputy heads of the Publicity Department of the CCP Central Committee Xu Lin, Hu Heping, and Wang Xiaohui, deputy head of the CCP Central Committee's Organization Department Fu Xingguo, head of the Party History Research Center of the CPC Central Committee Qu Qingshan and assistant director of the Political Work Department of the Central Military Commission Li Jun attend a press conference on the 100th anniversary of the CCP on March 23, 2021 in Beijing, China. (VCG via Getty Images)

## Persuasion

Antecedents of contemporary Chinese influence campaigns can be found in China's rich history. Well before the invention of the printing press, the Chinese are credited with inventing paper, ink, and the "sacred art" of printing.<sup>5</sup> China's ancient civilization was among the first to understand the importance of language, including the use of rhetoric and narrative for persuasion and "soft power." Guiguzi, a Taoist mystic also known as the Master of the Ghost Valley, is the presumed author of China's foundational treatise on the subject.<sup>6</sup> His followers were also known as "wandering persuaders" because of their abilities to articulate a narrative in favor of a particular plan and to annihilate alternative arguments.<sup>7</sup>

Confucius reflected on the nature and order of things and the "rectification of names," that is, calling things by their proper names and using words correctly. "If names are not rectified, speech will not accord with reality; when speech does not accord with reality, things will not be successfully accomplished."<sup>8</sup> However, an obsession with the fixed and the hierarchical rectification of names can introduce a high degree of militancy into the art of persuasion. For instance, if "Confucianism opposed rule by force rather than by persuasion," the Legalist school of thought "advocated strong centralized government which should exercise absolute power by the threat of harsh punishments."<sup>9</sup>

The Chinese government uses Confucius Institutes to spread its influence. Launched globally by the Chinese government's Ministry of Education in 2004 as a means of exercising cultural soft power, Confucius Institutes were part of what former Politburo Standing Committee member Li Changchun described as "an important part of China's overseas propaganda set-up."<sup>10</sup> By 2018, Confucius Institute Headquarters, or "Hanban," was coordinating nearly 550 institutes in more than 150 countries. Frequently established at foreign universities in English-speaking countries, often without adequate oversight, Confucius Institutes are linked to efforts at censorship and lobbying.<sup>11</sup> The

Institutes are a vital part of China's larger "soft power" efforts on which the party-state spends an estimated \$10 billion a year.<sup>12</sup> Concerns about CCP influence explain why more than half of the Institutes operating on US campuses have closed (with forty-seven remaining open as of May 2021, down from 103 in 2017).<sup>13</sup> Australia hosted fourteen Confucius Institutes before arresting their spread in 2018 due to concerns.<sup>14</sup> However, even sensible security actions taken to regulate the Institutes have unintentionally undermined Chinese language education opportunities.<sup>15</sup> But while a new US administration reviews reporting and other restrictions enacted by its predecessor, a fair question to ask is whether learning Chinese language and culture from programs backed by the Chinese government is the best option.<sup>16</sup> Striving to keep pace with criticism, China has sought to rebrand the Confucius Institutes, changing the name of the Headquarters or Hanban to the Ministry of Education Center for Language Education and Cooperation.<sup>17</sup> Promoting the ideas of Confucius, whether through controversial support for centers at universities worldwide or by producing local-language editions of the *Analects* for Belt-and-Road partner countries, Confucius remains an information tool for Beijing and not simply a historical figure.<sup>18</sup>

Transcending Confucius Institutes, China's interest in persuasion extends through myriad channels into fantasies of global "thought management,"<sup>19</sup> and the pursuit of total persuasion goes to the very heart of power in Beijing. Xi Jinping relies upon party loyalists like Qi Yu,<sup>20</sup> who, as party secretary at the Ministry of Foreign Affairs, ensures that diplomats "firmly counterattack against words and deeds in the international arena that assault the leadership of China's Communist Party and our country's socialist system."<sup>21</sup>

The techniques of persuasion can be subtle or sharp, and, in today's China, both official and quasi-official rhetoric often comes in the form of razor-sharp debating points. 'Wolf warrior' diplomacy, named after a Chinese action film, "abandons diplomatic niceties for rhetorically aggressive and threatening

browbeating”<sup>22</sup> and parallels the strict orthodoxy of the Legalists’ enforcement of whatever is deemed proper to advance centralized power. In the latter half of the Warring States Period, Legalists were “political realists who sought to attain a ‘rich state and a powerful army’ and to ensure domestic stability in an age marked by intense inter- and intra-state competition.”<sup>23</sup> Legalism supported norms intended to prevent subversion of the ruler’s power. Beijing’s recent resort to a tougher type of persuasion creates space for officials to “control escalation of disputed issues” while receiving plaudits from Xi and Chinese nationalists.<sup>24</sup> Xi’s leadership encourages a “civilian army” to engage in combative messaging; as Peter Martin, the author of a 2021 book on wolf warrior diplomacy, argues, “The easiest way for diplomats to work towards Xi’s wishes is to assert Chinese interests forcefully on the world stage.”<sup>25</sup> Recognizing the backlash to wolf warrior diplomacy, Xi has belatedly called for projecting a more “lovable” image of China; however, assertiveness and influence are likely to remain a significant part of Xi’s approach to the world.<sup>26</sup>

China’s information power emanates chiefly from a desire to convince through use of words—or at least by means short of force. But in the hands of government officials and state-owned or state-influenced media, Beijing’s messaging has a singular and overwhelming quality. Talking points quickly become campaigns perpetuated by disciplined party-state organs. The PRC echo chamber is amplified by China’s *wumao*, its ‘50 cent’ army of Internet commentators who attack critics of the party-state.<sup>27</sup> But, since dominating the infosphere is often more about distraction than sustained argument, Beijing also “astroturfs” with millions of posts from fake social media accounts.<sup>28</sup> The Great Firewall of China imposes heavy censorship, but it also enables the state to fabricate covert influence operations, even if those operations are often decentralized.

## Covert Influence Operations

Chinese officials apparently prefer to conceal their efforts to influence others. Employing covert influence operations, they dupe, nudge, and bribe individuals and institutions into

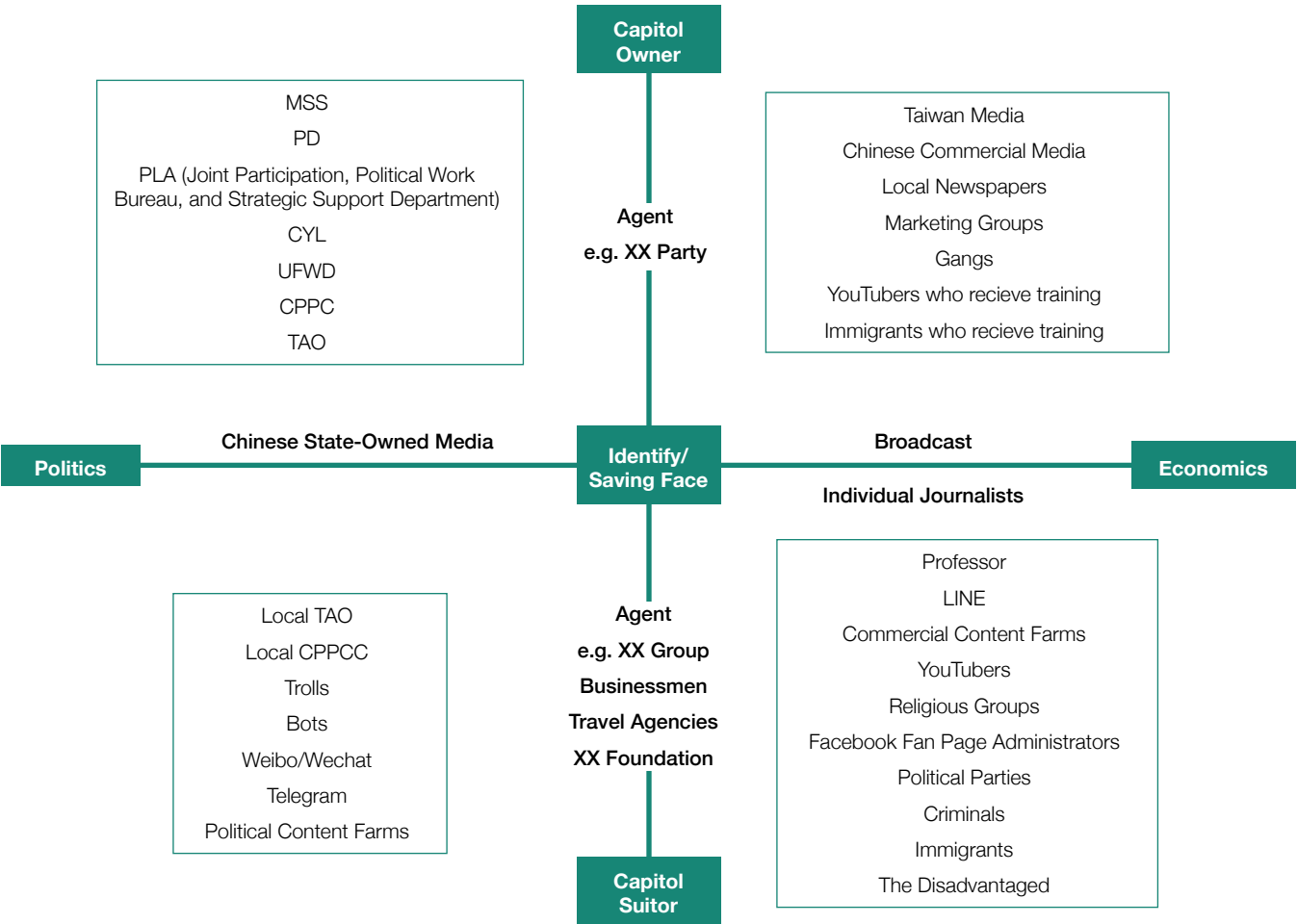
amplifying CCP messages. In studying Beijing’s disinformation campaign against Taiwan during its 2020 election, the Taipei-based researchers at Doublethink Lab identified the official initiators of messages intended to have psychological impact and the diffuse set of actors disseminating disinformation in a decentralized manner to various targeted audiences. This analytical framework illustrates how party-state agencies and those with economic interests in spreading China’s propaganda (owners) tap into a diverse network of groups and individuals with variably shared political or economic interests (suitors). China’s state organs churn out party propaganda (e.g., that China and Chinese culture are great and democracy is dysfunctional), which might then be picked up and echoed by a combination of local grassroots sympathizers, prominent content influencers, and more collaborative information-sharing means. This information operation network allows Beijing to go from cheerleading to sowing disruption and spinning conspiracies.<sup>29</sup>

## Decentralization

One means employed to cloak attempts to persuade others is through decentralized exploitation of multiple communication channels. Research from Doublethink Lab shows how China conceals the origins of its weaponized messages while relying on myriad sources’ legitimacy and audiences to deliver that message. In other words, to obscure the real messenger, China puts great store in employment of decentralized messaging, which thus represents a type of semi-covert information operation.

In some cases, the information operation is fully covert. For various reasons, China keeps its covert influence operations under wraps. Many are targeted attacks designed to silence dissidents or acquire technology or information, or are sustained arguments to achieve political objectives and influence foreign policy.<sup>30</sup> The advantage of quiet or clandestine influence operations is psychological in nature; one is more easily self-frightened when unaware that what has happened was, in fact,

Figure 1. Framework of actors behind Chinese influence operations



Source: *Deafening Whispers: China's Information Operation and Taiwan's 2020 Election* (Taipei: Doublethink Lab, May 2021), <https://medium.com/doublethinklab/deafening-whispers-f9b1d773f6cd>

a deliberate attempt by a foreign power to ‘kill a chicken to frighten the monkey,’ to drive a wedge between allies, or to sap a society’s political will. Even if a Chinese message delivered surreptitiously does not differ from overt communication, the advantage of employing covert influence operations is that their audience is typically less aware of the nefarious ends to which such messages are being aimed. Thus, obscuring the purpose

and source of such messaging tends to magnify its influence’s impact. Covert influence operations are thus analogous to an aggressive, undiagnosed cancer: by the time they are detected, the damage has been done. The concern is not China’s right to exercise “soft power,” but what former Prime Minister Malcolm Turnbull termed “covert, coercive or corrupt behaviour” designed for foreign interference.<sup>31</sup>



The coercive toolkit China has assembled is filled with levers of influence. Giving money to political leaders or influential people, providing misleading information about events or institutions, applying economic pressure, stealing IP, and resorting to harassment and forced extraditions are among its various means of applying leverage.<sup>32</sup> As one progressive US think tank has observed, these constitute examples of China's influence operations, potent means that have been designed to "demonstrate China's emphasis on building ... dominance through vehicles that help it project its legitimacy and power abroad."<sup>33</sup>

The scale of China's activities has inevitably invited scrutiny. For instance, between 2013 and 2015, Chinese-affiliated firms and donors gave more than 5.5 million Australian dollars to candidates from the two major political parties.<sup>34</sup> To help rein in Chinese interference and influence operations, Australia passed the National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018 (also known as EFI) and the Foreign Influence Transparency Scheme Act of 2018 (FITS Act).<sup>35</sup> Because democracies thrive on freedom, foreign relationships should be transparent. However, just because China's intent is to exercise influence does not mean its actions are against the law or, even if they are, that charges will stand up in court. Di Sanh "Sunny" Duong, a former member of the conservative Liberal Party and head of the Oceania Federation of Chinese Organizations from Vietnam, Cambodia, and Laos, has been the first Australian to be charged under new laws designed to counter foreign interference. However, the officials sifting through and translating copious evidence, including 2.23 gigabytes of electronic material, may find it difficult to explain or try individuals charged with preparing to engage in foreign interference or espionage.<sup>36</sup>

## The United Front Work Department

While many connections and activities may be innocent, or at least not illegal, China's United Front Work Department (UFWD) actively seeks to orchestrate covert influence operations, and

the organization's labyrinthine nature affords its officials plausible deniability. As Alex Joske explains, *tongzhan gongzuo* "is the process of building a 'united front' coalition around the CCP in order to serve the Party's objectives ... both domestically and abroad,"<sup>37</sup> and Anne-Marie Brady describes the crucial role the United Front played in helping the communists to emerge victorious from China's civil war and bring the CCP to power.<sup>38</sup>

Founded in 1942, the United Front Work Department has received heightened attention from CCP General Secretary Xi, China's paramount leader, who dubbed it a "magic weapon" during a 2014 speech marking the 65th anniversary of the Chinese People's Political Consultative Conference (CPPCC).<sup>39</sup> Through financial support to individuals and politicians, distortion of information, flagrant harassment of dissenters (especially among the Chinese diaspora), and other means, UFWD influence operations have spilled over into foreign interference in the political, journalistic, and academic institutions of Australia and other democracies.<sup>40</sup>

Xi's interest in deploying the United Front Work Department is reflected in his organizational reforms. New bureaus responsible for Xinjiang and "new media professionals and managerial staff in foreign enterprises" were created in 2016 and 2017, respectively.<sup>41</sup> In March 2018, the UFWD was responsible for work on religious groups, ethnic minorities, and the Chinese diaspora. The State Administration of Religious Affairs, the State Ethnic Affairs Commission, and the Overseas Chinese Affairs Office were all subordinated to UFWD.<sup>42</sup> Xi has enhanced the power and government-wide coordination responsibilities of the UFWD. Because the UFWD's remit extends globally, there is no distinction between domestic and foreign policy regarding controlling information on behalf of the CCP.

## Discourse Power

The battle over discourse power shows how uniquely unfettered Beijing remains in its struggle to attain persuasion and influence. Under Xi in particular, China mixes soft power with sharper



“discourse power” (*huayuquan*), which is defined as the “power to speak and be heard,” to “guide and lead debate,” to “set parameters of acceptable discourse,” and to “exercise influence.”<sup>43</sup> Xi’s narrative for a rising China forms part of a larger ideological battlefield on which Beijing wields influence in a titanic struggle with the United States and other democracies.<sup>44</sup>

Xi rose to power fearful of strong subversive currents within China. A secretive CCP memo circulated in 2013 warned about the seven perils posed by Western democracies.<sup>45</sup> These seven dire threats posed by Western ideology to the CCP’s survival are the following: Western constitutional democracy; universal values; civil society; neoliberalism; a free press (“the West’s idea of journalism”); historical nihilism; and questioning China’s reform.<sup>46</sup> Document No. 9 was an early indicator of the direction Xi intended to take China.<sup>47</sup>

This CCP centenary year is littered with examples of ascendant triumphalism. Throughout 2021, Beijing has been trumpeting, inter alia, beating the pandemic, “red tourism,” exploring Mars, and reliving the Long March. But underlying insecurity and fear regarding color revolutions, corruption, the Internet, and the party’s legitimacy have been hallmarks of Xi’s consolidation of power. Prior to issuing a steady stream of confident assertions of China’s triumphant reemergence, Beijing focused anew on the weaponization of narratives and foreign subversion.

Some China watchers have clung to the hope that Xi’s political oppression might lead to liberalization and reform.<sup>48</sup> Instead, Beijing has doubled down on its initial hardline tilt toward internal repression, strict party discipline, and defense of Mao’s legacy through a rectification campaign, accompanied by aggressive anti-Western diplomatic and informational activities.

### Weaponizing Narratives: “The revolutionary ideal is higher than heaven”

China expands today’s ideological battlefields by weaponizing narratives, especially those employed domestically to urge

extreme patriotism bordering on the spiritual. Although these present no direct threat to neighbors or the world’s democracies, indirectly they serve to create a cult of personality in Xi Jinping. Such narratives consistently fail to hold the CCP accountable or contest policy with alternative views, embellish the notion that authoritarian governance is superior to democratic models of government, and stoke a level of jingoism that could be manipulated to support external confrontation.

CCTV’s devotion of airtime to Xi’s inspection tour covering the Long March is an excellent example of discourse power. As part of the steady drumbeat of CCP achievements, one episode centers on the crucial 1934 battle in which the Red Army lost nearly two-thirds of its soldiers crossing the Xiangjiang River. The banks, state Xi, are stained with “the blood of tens of thousands of Red Army soldiers.” Xi’s reprise of the CCP armed forces’ evasion of the Kuomintang army was intended as a historical analogy whose purpose is to rally today’s Chinese and to impart the understanding that “the revolutionary ideal is higher than heaven, and once the fire of ideals and beliefs is ignited, it will produce great spiritual power.” As Xi tells his Chinese audience, “On the new Long March to achieve the second centenary goal, we must hold the belief of the certainty of our victory, bravely overcome all kinds of major risks and challenges from home and abroad, and march forward bravely towards the goal of realizing the great rejuvenation of the Chinese nation.”<sup>49</sup> Although this historical episode resembles the patriotic national rhetoric of many other countries, in this case, Beijing is using it to reinforce its foreign messaging to the effect that China’s rise is unstoppable and the PLA is prepared to fight if necessary.

The thrust of state media’s meta-message is China’s messianic mission. “Higher than heaven” is a lofty ambition indeed. Invoking spiritual power and tapping this “revolutionary ideal” empowers and justifies Xi’s goal of putting China at the center of a connected network of high-speed rail, highways, Internet cables, and satellite transmissions—all through an unsurpassed generosity to build a “community of common destiny for

mankind.”<sup>50</sup> Increasingly, China’s vision for the common future of humanity seems to fit under Xi’s legacy brand, One Belt One Road (OBOR).

## The OBOR Brand

Understanding Xi’s One Belt One Road helps to place it in the context of China’s contemporary domestic politics, historical identity, and international public relations efforts.<sup>51</sup> At home, OBOR represents an attempt to resurrect the ancient tributary system that placed China at the center of world power. It also enables the regime to unify China’s disparate economic and foreign policy activities under one harmonious slogan that resonates with the public. Abroad, the Chinese government refers to One Belt One Road with the relatively more benign-sounding name “Belt and Road Initiative,” language intended to emphasize China’s peaceful re-emergence and highlight its role as a dispenser of public goods to less developed countries.<sup>52</sup>

However, the multi-dimensional One Belt One Road remains opportunistic and politically driven while continuing to evolve. It has also become a potent tool of grand strategy, advancing China’s sovereignty and domestic stability, economic interests, and industrial-military power.<sup>53</sup> In effect, OBOR has acted as the silk interweaving all of these global Chinese threads together into a whole. Xi’s creation of OBOR not only subsumed many preexisting projects but assembled a diverse assortment of projects under a new name. In 2013, Xi announced a land-based “Silk Road economic belt” linking China with Central Asian countries.<sup>54</sup>

Quickly adding to the notion of OBOR as restoring a lost past, Xi announced a sea-based 21st Century Maritime Silk Road in the context of China’s famous eunuch admiral Zheng He, whose seven expeditions around the Indo-Pacific region have been sanitized into “touching stories,” with all elements of tribute-seeking coercion removed.<sup>55</sup> Zheng He is the subject of less censored histories likening the early Ming dynasty “ten-masted

Chinese ‘treasure ships’ (*bao chuan*)” to “floating castles”<sup>56</sup> and noting that a chief purpose of the voyages was “to impose Chinese authority.”<sup>57</sup> Since then, Beijing has added, among other things, a “Polar Silk Road” to the Arctic,<sup>58</sup> a “digital Silk Road” of 5G telecommunications systems,<sup>59</sup> and a “spatial information corridor” featuring a state-of-the-art Beidou satellite navigation network.<sup>60</sup> Amid the pandemic and a push to curb climate change, China has also added a “health Silk Road” and a “green Silk Road.”<sup>61</sup>

Although the cost of the global need for infrastructure greatly surpasses China’s OBOR investments, Beijing’s commitment of some \$1 trillion to build many silk roads and infrastructure projects is a significant selling point.<sup>62</sup> A trillion dollars correctly leveraged can buy a significant amount of influence, and so the debate continues over exploitation by China’s state-owned banks of borrowing nations to gain trade and geopolitical advantage, a practice one commentator has dubbed “colonization by other means.”<sup>63</sup> While talk of “debt traps” may be over-simplified, infrastructure financing can create a serious debt squeeze for the governments of developing countries. As Papua New Guinea is discovering, owing more than half a billion dollars to China for loans to build telecommunications projects and a data center poses long-term constraints on decision-making.<sup>64</sup> One study that examined 100 OBOR contracts found that China’s contracts contained unusual confidentiality clauses and suspect clauses apparently designed to influence debtors’ domestic and foreign policies. “Overall,” the study concluded, “the contracts use creative design to manage credit risks and overcome enforcement hurdles, presenting China as a muscular and commercially savvy lender to the developing world.”<sup>65</sup>

Understandably, authoritarian leaders prefer China’s brand of state-to-state foreign assistance, which is free from human rights and environmental constraints, while also fearing loss of sovereignty through acceptance of China’s largesse.<sup>66</sup> In short, as discussed in the conclusion of this report,

China's approach carries real risks but also provides ample opportunities for the United States, Australia, and other democracies to offer a better model based on collaborations in high-standard trade and development. Money is not the only consideration, however; one of the high hurdles to offering compelling alternative assistance with infrastructure development is Beijing's skill in marketing OBOR and use of information power to secure deals, cut out opposition, and reinforce the China brand. Recently, Beijing has even come close to openly admitting its long-term plans and agenda; one common refrain of CCP officials is "the East is rising while the West is declining."<sup>67</sup>

### Pandemic Diplomacy

The COVID-19 coronavirus believed to have begun in China in late 2019 has spawned a protracted period of pandemic diplomacy. China's forced bravura, projecting the image of an ever-confident nation, stands in stark contrast to its oscillating defensive and offensive responses in handling the coronavirus.<sup>68</sup> Concerning the COVID-19 response, there is ample criticism to go around, and it took the United States more than a year to move from pandemic denier to global public health provider. But from the beginning, China sought to control the COVID-19 narrative within and outside China.

Concealment and deception at the outset quickly transitioned into an effective if a draconian set of intrusive and mandatory lockdowns and monitoring. Xi imposed an early information blockade about human-to-human transmission of the coronavirus, and both the origin and China's early handling of the coronavirus remain clouded with obfuscation. The government described the tragic death of Dr. Li Wenliang, the heroic whistleblower who tried to alert the world to the deadly virus, as "a minor stumble."<sup>69</sup> China countered attacks on theories that the virus had leaked from the Wuhan Institute of Virology—for which there is some serious circumstantial evidence—with disinformation that the coronavirus might have originated at Fort Detrick in Maryland, for which there is no

supporting evidence.<sup>70</sup> While still playing down the coronavirus in January 2020, China hoarded personal protective equipment (PPE). As Beijing began successfully containing the virus within China, officials sought to change the international conversation from COVID-19's origins to China's provision of public goods, thus pivoting from a defensive crouch to an offensive posture through use of "mask diplomacy."<sup>71</sup>

This use of mask diplomacy foreshadowed a geopolitical contest over vaccine diplomacy. As COVID-19 began to ravage the United States and other countries, America's high death rates and pandemic denialism provided easy targets for Chinese propaganda.<sup>72</sup> Beijing bristled when Australia backed a World Health Organization (WHO) investigation into the virus's origins,<sup>73</sup> and Australia soon found itself under escalating Chinese economic coercion.<sup>74</sup> The WHO thus became embroiled in pandemic politics. US policy support for vaccine development accelerated efforts to immunize people for the coronavirus, and, while the United States was still busy seeking to vaccinate Americans, China made an early point of prioritizing international distribution of vaccine for political gain.<sup>75</sup> An essay in the official *People's Daily* assailed India's and America's approach to COVID-19 vaccine production and distribution, arguing that the United States sought vaccine supremacy and only belatedly woke up to vaccine diplomacy: "America and some of its allies' vaccine supremacy lies in the fact that they deploy their authority willy-nilly and abuse their dominant position on what at first appears a seemingly understandable basis—namely, that their citizens (many of whom are reluctant to wear masks or loath to engage in social distancing) should have privileges to get the shot first."<sup>76</sup>

China's extensive effort in media coverage of its coronavirus response underscores its attempt to gain discourse power. In a report commissioned by the International Federation of Journalists, former National Public Radio Beijing bureau chief Louisa Lim and two co-authors canvassed journalists in fifty-four countries and found that China had researched foreign

media.<sup>77</sup> As the pandemic spread, the May 2021 report noted, China activated its global media infrastructure,

which includes training programs and sponsored trips for global journalists, content sharing agreements feeding state-sponsored messages into the global news ecosystems, memoranda of understanding with global journalism unions, and increasing ownership of publishing platforms. As the pandemic started to spread, Beijing used its media infrastructure globally to seed positive narratives about China in national media, as well as mobilizing more novel tactics such as disinformation.<sup>78</sup>

The report added:

During 2020, China's global disinformation campaign came to the fore. Tweets from its Foreign Ministry spokesman Zhao Lijian showcased conspiracy websites, including one that claimed Covid-19 was brought to China by US soldiers attending the Army Games in Wuhan, the city in which the first outbreak was discovered. That narrative was then amplified across social media by an army of Chinese ambassadors and other foreign ministry spokesmen, who became known as practicing 'Wolf Warrior' diplomacy. Twitter and Facebook are still banned in China.<sup>79</sup>

The pandemic has been a potent foil for Chinese diplomacy. To be sure, the report's authors see this global response more as an indicator of China's developing power than as a short-term effort to quash international scrutiny. China seeks to tell its story and build influence despite—and not just because of—the United States.<sup>80</sup> Nonetheless, it is hard to ignore the record, which ranges from Document No. 9 to wolf warrior diplomacy to vitriolic anti-American commentaries published in the Chinese press. For instance, a commentary published in *Xinhua* in December 2020

warned its domestic audience in Manichean terms that Chinese who “worship America” and “kneel to America” are turncoats who “forget their ancestors and aid the evil-doers.”<sup>81</sup>

## The Contest for Narrative

China's success in leveraging information for diplomatic and political power has catalyzed a major-power contest for control of the narrative. From persuasion to covert influence operations to discourse power, China is perfecting the weaponization of narrative. Information power plays a significant role in China's transmutation of weakness into strength. China's vaccine diplomacy response to the coronavirus and evolving OBOR effort are two cases in which China has used what most nations would consider humanitarian or development assistance as an asymmetric weapon. China deploys discourse power to gain political and diplomatic power in its global contest with the United States over influence and rulemaking. Thus, what began as a defensive effort to find asymmetric means of blunting the strengths and exploiting the liabilities of foreign powers has become an asset.

As China reemerged as a major power, it simultaneously transformed into an information superpower. Nadège Rolland has likened China's counteroffensive in the war of ideas to China's “anti-access and area denial” military strategy.<sup>82</sup> “In other words,” writes Rolland, “it is an active strategic counterattack on exterior lines to prevent or constrict the deployment of an opponent's forces into a given theater of operations and to limit their freedom to maneuver once they are present.”<sup>83</sup> China accomplished this in a digital era of unprecedented connectivity, amplifying the power of influence by expanding the government's ability to gain access to data and information, wield soft power, use sharp power to interfere with and block the use of unwanted words and deeds, achieve increased discourse power, and, in military contingencies, fight and win informatized wars.

If the United States and Australia are to reassert control over the narrative, they must overhaul and augment their existing public diplomacy channels. China's ability to reshape criticism

of its early handling of the COVID-19 crisis into powerful public narratives seemed to highlight Beijing's discourse power and the atrophying of America's historic advantages in public diplomacy. As one media analyst summed up the situation:

**The United States may have pioneered the tools of covert and overt influence during the Cold War, but the government's official channels have withered. The swaggering C.I.A. influence operations of the early Cold War, in which the agency secretly funded influential journals like *Encounter*, gave way to American outlets like Voice of America and Radio Liberty, which sought to extend American influence by broadcasting uncensored local news into authoritarian countries. After the Cold War, those turned into softer tools of American power.<sup>84</sup>**

Countering a narrative requires the ability to halt malicious interference from the outside. In the past few years, both Washington and Canberra have invested in efforts intended to counter Chinese interference. In addition to new laws designed to shine a spotlight on foreign influence, both governments have invested in public diplomacy. Both can do more to augment discourse power, however. As part of the Biden administration's elevation of diplomacy, it should build on the fledgling Global Engagement Center. In addition, public diplomacy should be prioritized throughout the interagency, including provisioning it with talent and funding commensurate to the challenge, and closely coordinated with leading allies such as Australia. Strategic oversight for this mission and related to China's information campaign should fall under the newly created US position of coordinator for the Indo-Pacific. Only that will guarantee that messaging and information are treated as strategic assets and vulnerabilities and not dismissed as mere aspects of public relations.

As the United States, Australia, and other democracies build discourse power to combat disinformation, they must remain true to their democratic values. Offensive political information

operations pose severe risks. They may stray too far into domestic politics or too far from reality. When private groups and individuals generate information operations, the government may have little control over their activities.

Contests over narrative are typically waged as much by non-state as by state actors and, in some cases, more by non-state than state actors. As an example, take the case of the strange 'Whistleblower Movement' led by businessman Guo Wengui. In the past few years, Mr. Guo (aka Miles Guo or Miles Kwok) built a vast media outlet network to spread online disinformation. Thousands of social media accounts associated with the network—which is comprised of many corporate and media entities having obscure structures—have conducted harassment campaigns, some of which have been linked to violent incidents.<sup>85</sup> In June 2020, the movement issued a statement announcing that its mission was to create a "New Federal State of China," to "take down the CCP," a "terrorist organization," and to "prevent the CCP from implementing its plan of complete enslavement of the Chinese people and dragging the rest of the world down the same path."<sup>86</sup> It did not take the network long to stray into other political affairs, however, and it did so as of last year.

Money and politics can make for unusual alliances in our 'post-truth' era.<sup>87</sup> Through its unlikely partnership with former White House strategist Steve Bannon, Mr. Guo's network has been linked to peddling false conspiracy theories about the January 6th insurrection and vaccine safety. A report by *Graphika* found "the network acts as a prolific producer and amplifier of mis- and disinformation, including claims of voter fraud in the US, false information about Covid-19, and QAnon narratives."<sup>88</sup> In addition, "despite Guo's self-proclaimed status as a Chinese dissident, his network has repeatedly attacked well-known anti-CCP activists."<sup>89</sup> In short, the same instruments appear to have been diverted to interfere with American politics—making it precisely the kind of tool for political interference that such offensive political information operations should be designed to thwart.

Despite the dangers of rogue operations, the United States and Australia must incorporate some capacity for offensive information operations in their policy toolkits. Provided quality control and accountability are maintained, muscular information operations can successfully sanitize foreign disinformation. In addition, they may prevent the Chinese people from taking their country's propaganda too seriously. It's one thing for Xi to stoke

nationalist sentiment during the CCP centenary, but it would be another matter entirely if the PLA were to begin believing the time is right to test its ability to fight and win local wars. Stated differently, a new generation of Chinese may begin to think that the ultimate sacrifice is needed for writing, as Xi described it, "a new magnificent chapter and forging a red monument that will never fade."<sup>90</sup>





## CHAPTER 3: ECONOMIC AND TECHNOLOGICAL INFORMATION

The raising of China's voice in the world is inseparable from its economic development. After four decades of unprecedented growth, Beijing is in an enviable position to influence others and rewrite rules of order. If China can surpass all others in mastering emerging technologies over the next three or four decades, then it will indeed hold the reins of power in the twenty-first century. Information-centered technologies such as fifth- and sixth-generational telecommunications, artificial intelligence (AI), and quantum computing may determine not just who drives the global economy but also who possesses the most formidable military. This chapter describes how China hopes to use information dominance to win economic and technological competitions.

### The Data Economy Era

In our advanced digital age, data illuminates the pathway to economic supremacy. China has used and continues to use data to drive its sustained economic rise and to identify advantages over other economies. China is also weaponizing and monetizing data and information while also investing in AI and future generations of digital technologies. Data are

---

Photo: A container is loaded onto a cargo ship during the opening ceremony of the Qingdao Port in China's Shandong province on January 19, 2021. The new port will link several Belt-and-Road countries through shipping routes extending across Northeast Asia. (Zhang Jingang/VCG via Getty Images)

the building blocks of information power. China is poised to become a leader in science and technology (S&T) and solidify its position as the leading power in information processing and cyberspace.

Its long-term plans reveal China's economic ambitions, but difficult questions to which Beijing offers contradictory answers are impeding its way forward. At its core, the dilemma facing China is that the political freedom required to achieve the economic power it craves collides with the party-state's need to control data and information. China's efforts to block cryptocurrencies like Bitcoin and create a cyber yuan cryptocurrency highlight this dilemma.<sup>91</sup> Beijing fears what it does not control and yet wants others to trust what China controls.

Some aspects of the data-driven economics are straightforward and open: Beijing is pouring money into digital infrastructure, drafting new laws concerning data use, and building new data centers around the country to position China as a leader in transforming the world economy over the next few decades. But other aspects of Xi Jinping's handling of big tech companies seem counterproductive. As described next, the stories of Alibaba and Apple illustrate the power of the party-state and its determination to control data and information despite the power of big-tech firms inside and outside of China.

### Harnessing Tech Giants Domestic and Foreign

Jack Ma's story personifies China's economic clout and its ongoing crackdown on big tech giants. Ma, the unrivaled entrepreneur who founded Alibaba, spawned an empire made up of Alipay, money market funds, the Taobao online marketplace, and much more. In 2014, Alibaba generated the Ant Group, expanding Ma's power and prompting Xi to use state-owned enterprises and regulations to limit the clout of high-tech CEOs.<sup>92</sup> However justifiable, Xi's power grab, masquerading as an antitrust drive, reversed decades of economic liberalism. Augmenting CCP power and its control over big data are driving Beijing's crackdown more than a

desire to protect the Chinese consumer. When Deng Xiaoping opened China to the world in the late 1970s, his tolerance of private enterprise made China increasingly reliant on the private sector for growth, jobs, and tax revenue.<sup>93</sup> Deng famously stated, "Black cat or white cat, if it can catch mice, it's a good cat." Jiang Zemin's "Three Represents" took another step toward economic liberalism by incorporating China's capitalist class into the CCP power structure.<sup>94</sup> But after Xi came to rule, his efforts to consolidate power led to increased numbers of anti-corruption campaigns and increased financial regulation. While Ma's showmanship made him a sensation on the global stage, it also produced "*gonggago gaizhu*," a situation in which "a subject's achievements make the king feel uneasy."<sup>95</sup> There is only one emperor in the Middle Kingdom, and that is Xi. After decades of relatively unfettered operations, China's tech giants now operate under duress to subordinate themselves to a CCP fearful of losing its monopoly on power.

In fact, preserving the party-state's monopoly of political power has more to do with the record fines levied against and the sidelining of celebrity entrepreneurs than with breaking up China's monopolies to create economic competition. The PRC and its big-tech national champions are at an inflection point: Beijing wants to capture and sift through the treasure trove of data that tech giants have gathered, as these data are essential for China to achieve its economic development and perpetuate the CCP's power. The taming of Jack Ma signified that a turning point had been reached, i.e., that at which China's political leaders require the digital capacity of industry to achieve the next stage of their global competition. Data provide an all-purpose key for unlocking innovation, market access, and economic growth.<sup>96</sup>

China does not just direct and control Chinese enterprises: It also dictates how US and other nations' tech giants are allowed to operate within China. Apple provides one case study. By allowing China to perpetuate its narrative on Apple's platform, the US firm self-censored and essentially ceded control over

data to China. Therefore, purpose-built data centers run by a state-owned firm now store the personal data of Apple's Chinese customers, allowing the state to acquire that big data. However, Chinese law gives companies like Apple little choice but to comply.<sup>97</sup>

Although the current strict terms of doing business in China are not entirely new, they have been ratcheted up to force companies like Apple to compromise Western standards related to privacy, civil liberties, and intellectual property rights through the years to gain market access. In the words of Amnesty International's Asia director, Nicholas Bequelin, "Apple has become a cog in the censorship machine that presents a government-controlled version of the internet."<sup>98</sup> Moreover, this situation is by no means unique to Apple but points instead to a divide between Washington policymakers of both parties and big business. Once a company like Apple becomes acutely dependent on China (which assembles nearly every iPhone, iPad, and Mac), disentanglement becomes difficult at best. So, although Apple's iCloud service encrypts sensitive data, the compromises Beijing has forced Apple to make will enable China to gain access to that data—either by demanding them or simply taking the encryption keys, which have remained in China.<sup>99</sup> In either case, the party-state will not be denied the data it wants.

From the perspective of Beijing officials, access to increased amounts of data can boost China's economic, technological, and military competitiveness while ensuring increased political control at home, externally around China's periphery, and globally. Likewise, the fear that China's acquisition of unlimited data can doom the United States, allies like Australia, and the postwar international system, is predicated on an equally specious notion that big data equates to immense power. In short, big data does not automatically translate into superior power as a regional or global hegemon because data are inherently biased rather than being objective facts. This limitation of data gives experts pause with respect to the rapid introduction of AI and machine learning into policymaking. As

Diane Coyle has cautioned, "Before we entrust more decisions to data-based machine-learning and AI systems, we must be clear about the limitations of the data."<sup>100</sup>

## Artificial Intelligence and Information Processing

Even though processing more information faster offers no guarantee of obtaining a correct answer, US and Australian officials should be clear-eyed about China's desire to collect big data. Data are "profoundly dumb," at least when it comes to the significant task of deriving explanations. However, technology may be on the cusp of adding value to data by creating a "Causal Revolution."<sup>101</sup> According to Judea Pearl, smart AI hinges on learning machines that can make the leap from data collectors and processors to "makers of explanation."<sup>102</sup> China seems to be chasing this AI dream, perhaps hoping that machines will gain "the ability to reflect on their mistakes, to pinpoint weaknesses in their software, to function as moral entities, and to converse naturally with humans about their own choices and intentions."<sup>103</sup> Under careful control, smart AI can be a force for good; in the wrong hands and absent checks and balances, the possibilities are more alarming.<sup>104</sup> Put simply, "causality has been mathematized."<sup>105</sup> While that future may be decades off, AI is accelerating not just our data-driven economy but also our data-driven national security. Of course, democracies seeking defense against emerging threats can employ the same technology China uses to exploit new information-processing speeds. AI and machine learning will help with "connecting the dots" at speed, as the Director-General of the Australian Security Intelligence Organization, Mike Burgess, describes it.<sup>106</sup>

Whereas the prospect of a massive, information-processing leap through AI is frightening enough when employed by democratic governments, in the hands of a major-power rival, it threatens fantastic new means of influence and control. As Vladimir Putin said of AI, "Whoever becomes the leader in this sphere will become the ruler of the world."<sup>107</sup> Can governments afford to gamble that Putin is wrong?



Uncertainty as to the seriousness of the advantage in foreknowledge that big data and AI dominance can provide a nation is driving high-tech competition in general and the contest for leadership in AI in particular. In mid-2017, when China announced a dramatic increase in state funding to make China an AI innovation hub by 2030, it still significantly lagged the United States in AI financing and number of AI companies.<sup>108</sup> In setting a target of 11 trillion renminbi for the 2030 value of China's AI industry, Xi prioritized mastery of AI at the forefront of China's Made in China 2025 industrial strategy.<sup>109</sup> Despite growing concern about an AI "arms race," Chinese officials see AI as crucial to military modernization and competition with the United States.<sup>110</sup>

China's ambitions are not to be dismissed. Indeed, the final report of the bipartisan National Security Commission on Artificial Intelligence (NSCAI) warns, "For the first time since World War II, America's technological predominance—the backbone of its economic and military power—is under threat. China possesses the might, talent, and ambition to surpass the United States as the world's leader in AI in the next decade if current trends do not change."<sup>111</sup>

One detailed analysis of applied AI suggests that the implications are "not evolutionary, but revolutionary."<sup>112</sup> According to an assessment of applied AI in business intelligence, for instance, the impact will be transformational:

It means the way intelligence and law enforcement conceptualize 'intelligence' must radically change to include a new intelligence cycle in which an 'analyst' serves to educate the initial development of an artificial ecosystem and the validation and communication of the artificially derived outputs. It means the types of people serving central roles in the intelligence business must be examined through their roles in the recreation and interactions with artificial ecosystems.<sup>113</sup>

Its possible impact on the future of deterrence and war could be profound. Along with the ability to sow disinformation on a massive scale, conduct cyber attacks, and create smart weapons to wage autonomous warfare, AI could call into question the ability of the United States to project power forward in the Indo-Pacific to defend its vital interests and those of allies such as Australia. The impact on military systems and operations could be equally profound, giving rise to "algorithmic" or "intelligentized" war, pitting algorithm against algorithm.<sup>114</sup> As the NSCAI report concludes, "Advantage will be determined by the amount and the quality of a military's data, the algorithms it develops, the AI-enabled networks it connects, the AI-enabled weapons it fields, and the AI-enabled operating concepts it embraces to create new ways of war."<sup>115</sup>

### Data-Intensive, Multi-Use Systems

The interlocking of data and technology portends new risks, as the multiple uses of unmanned aerial vehicles (UAVs) suggests. Whereas in peacetime large UAVs and quadcopters can collect data and gain access, at the onset of hostilities, these same platforms can be transformed into smart weapons capable of autonomous warfare. Because the same systems that benefit society could also pose national security risks, who manufactures these data-collecting systems matters greatly. Although a recent Pentagon review found "no malicious code or intent" in drone software made by the Shenzhen-based company DJI, tensions between commerce and security are likely to persist with respect to Chinese UAVs.<sup>116</sup>

Potential future risks to security posed by technology made by China could prompt Congress to restrict Chinese drone use in defense and law enforcement. Because in this advanced digital age every platform is capable of collecting data, drone origins matters. In May 2019, the US Department of Homeland Security issued an industry alert regarding "Chinese Manufactured Unmanned Aircraft Systems" that expressed "strong concerns about any technology product that takes American data into the territory of an authoritarian state that

permits its intelligence services to have unfettered access to that data or otherwise abuses that access.”<sup>117</sup> In December 2020, the US Department of Commerce blocked American firms from exporting technology to DJI because of the use of that firm’s quadcopters in enforcing the suppression of human rights in Xinjiang and elsewhere.<sup>118</sup> US policy responses reflect Chinese security operations’ use of Military-Civil Fusion to interweave information and technology. The US ban included everything from construction companies helping China militarize disputed areas of the South China Sea to Chinese universities exploiting joint research agreements that might assist PLA modernization. In December, Japan announced that its Coast Guard would no longer use Chinese drones because doing so could allow China to steal sensitive data related to the Senkaku Islands.<sup>119</sup> Japanese construction companies joined the government ban on Chinese-made drones as part of Japan’s broader effort to prevent theft of sensitive information via drones used to inspect cables, bridges, and other infrastructure projects.<sup>120</sup>

Although DJI claims it takes information security seriously, Chinese firms must obey CCP party-state laws. In 2017, Beijing adopted the National Intelligence Law, in which Article Seven states, “Any organization or citizen shall support, assist, and cooperate with state intelligence work according to law.” Article Fourteen says that organizations and citizens must also protect the secrecy of “any state intelligence work secrets of which they are aware.”<sup>121</sup>

## From Made in China 2025 to Vision 2035

Xi Jinping is putting China at the forefront of high-technology innovation. Aided by intellectual property (IP) theft, forced technology transfers, decades of education training abroad, and other forms of gathering and exchanging scientific and technical know-how, China’s industrial policy goes beyond protectionist measures like subsidies. Thus, Xi’s massive interventions reverse a decades-long experiment in market liberalization.<sup>122</sup>

## The Theft of Intellectual Property

Before China could dominate markets and technological innovation, it first had to excel at accumulating IP, which it did through theft and acquisition of intellectual property by any means necessary. These methods have primed the pump of Chinese technological innovation and R&D and may empower Beijing past the United States and other advanced economies in the near future.

By 2013, the Obama administration had become alarmed over the degree to which China was stealing trade secrets and dealing in counterfeit goods and pirated software.<sup>123</sup> As a bipartisan commission on the theft of American IP noted, China is “the world’s principal IP infringer,” with IP robbery costing the US economy as much as \$600 billion a year.<sup>124</sup> Because China was gaining access to so much information—open, proprietary, and classified—via the Internet, finding ways to clamp down on China’s economic espionage became a national security priority. Unfortunately, a US-China cyber commitment made in September 2015 was short-lived. According to a 2018 report from the US National Counterintelligence and Security Center, China continues to exploit cyberspace for IP theft, albeit with a more targeted focus on “cleared defense contractors or IT and communications firms.”<sup>125</sup>

China’s comprehensive approach goes well beyond cyberspace. Instead, “China’s cyberspace operations are part of a complex, multipronged technology development strategy that uses licit and illicit methods to achieve its goals.”<sup>126</sup> As the Office of the Director for National Intelligence (ODNI) analysis illustrates, China’s IP theft tools include those depicted in Figure 2 on the next page<sup>127</sup>.

The US intelligence community often speaks of “all-source” information. Under Xi, China is accumulating big data and IP to establish both cutting-edge technology and analysis, boosting China’s economic development and bolstering its military modernization.

Figure 2. Methods of intellectual property theft used by China



Source: The National Counterintelligence and Security Center, Foreign Economic Espionage in Cyberspace (Washington, D.C.: ODNI, 2018), <https://www.dni.gov/index.php/ncsc-newsroom/item/1889-2018-foreign-economic-espionage-in-cyberspace/>.

China's interest in hoovering data is not limited to tapping technological innovation but applies equally to human capital. The massive hack of 22.1 million files from the Office of Personnel Management (OPM) first disclosed in 2015 stands as one of the largest heists of data on the US federal workforce.<sup>128</sup> A 2017 attempt to use the same rare malware tool used in the OPM hack led to the arrest of a Chinese national, suggesting that democracies can learn from their mistakes.<sup>129</sup> But using the Internet, facial recognition technology, and surveillance technology, the Ministry of State Security and the PLA enable Beijing to steal everything from digital exhaust to tracking critical military platforms as they transit chokepoints or arrive and depart air bases and naval ports. Only recently has the US government taken remedial

steps to protect digital data from mobile phones of its soldiers and other national security personnel.<sup>130</sup> But China has many ways of acquiring information from overseas, often through the guise of cooperation.

## Educating, Training, and Equipping the PLA

A formative challenge for the United States, Australia, and other democracies is preserving an open scientific and research environment without facilitating the transfer of vital technology and know-how to Beijing. The most glaring examples center on how China's defense-affiliated universities and research centers appear to exploit collaborative relationships with leading institutions in democracies. Of special concern are the so-called "Seven Sons of National Defense": the Beijing Institute of Technology, Beijing University of Aeronautics and Astronautics, Harbin Engineering University, Harbin Institute of Technology, Nanjing University of Aeronautics and Astronautics, Nanjing University of Science and Technology, and Northwestern Polytechnical University.

Evidence of this problem is pervasive and growing. Chinese military-affiliated institutions have successfully exploited exchanges with foreign universities. Consider a few of the findings of four significant recent studies:

- According to a 2018 study by the Australian Strategic Policy Institute (ASPI), during the decade between 2007 and 2017, the Chinese military sent more than 2,500 scientists to train and work in foreign universities.<sup>131</sup> According to Alex Joske, "Dozens of PLA scientists have obscured their military affiliations to travel to Five Eyes countries and the European Union, including at least 17 to Australia, where they work in areas such as hypersonic missiles and navigation technology."<sup>132</sup>
- ASPI's tracker shows that China's Military-Civil Fusion is linked to Beijing's grand strategy for building nearly 100 world-class institutions by 2050. Engaging in exchanges with high-risk institutions—such as the Seven Sons of



National Defense—highlights a challenge for which civilian universities in Australia and elsewhere have been ill-equipped to address.<sup>133</sup>

- In 2018-2019, thirteen US technology companies operated joint training programs with PLA-affiliated institutions; according to the Georgetown University Center for Security and Emerging Technology study, these joint programs included projects focused on machine learning, big data, and integrated circuit design. Further, several major US tech firms established close working relationships with defense-affiliated universities in China.<sup>134</sup>
- Other Five Eyes countries, such as the United Kingdom, have also been inadvertently helping the PLA modernize its military hardware through research exchanges with defense-affiliated institutions. According to UK think tank Civitas, the ASPI tracker deemed a “very high risk” the dozen Chinese universities working with British universities on research projects related to hypersonic missiles, radar jamming systems, and other advanced technologies that could be employed on the battlefield.<sup>135</sup>

## MIC 2025

Xi’s ambitions to make China a leader in emerging technologies were self-evident in the ten-year industrial policy known as Made in China 2025 (MIC 2025). That 2015 plan set targets of 70 percent self-sufficiency in high technology industries as part of the march toward global market domination. MIC 2025 sought to boost China’s economic competitiveness with breakthroughs in ten sectors: information technology; high-end computerized machines and robots; aerospace; high-tech ships; advanced railway transportation; new energy and energy-saving vehicles; energy equipment; agricultural machinery; new materials; and biopharma and advanced medical devices.<sup>136</sup>

By the mid-2020s, China could transition from a “manufacturing giant into a world manufacturing power.” In that case, by 2035, China would achieve parity with global industry and, by 2049, would lead worldwide manufacturing and innovation.<sup>137</sup>

Made in China 2025 clearly signaled Xi’s seriousness about winning a high-tech competition, and his subsequent steps heightened US concerns. Xi announced that China would reign supreme in AI innovation by 2030.<sup>138</sup> The Chinese government championed companies like Huawei to dominate global fifth-generation (5G) telecommunications.<sup>139</sup> Beijing also declared as a goal Chinese self-sufficiency in semiconductors chips—a core technology at the heart of many other advanced technologies—particularly advanced chips 14 nanometers and under.<sup>140</sup>

## Military-Civil Fusion

China’s bid for total information dominance leads to its use of a distinctive whole-of-society approach aimed at building a dazzling wealth of data and information designed to advance technological breakthroughs. When Military-Civil Fusion is taken into consideration, this development has far more than economic and technological ramifications: China expects to rival the United States military and also the armed forces of US allies. Commercial strategy is inseparable from the military system. There is nothing novel about a strong economic foundation providing a basis for military strength, and experts caution that China’s military-civil fusion must be seen as aspirational rather than reflecting reality or the end of bureaucratic turf wars in China.<sup>141</sup> Nonetheless, China has taken this concept to new lengths, focusing on advanced technologies in the current digital age. Perhaps reflecting both the need for China to catch up and the aspiration to seize an opportunity, Xi has made military-civil fusion part of China’s national strategy, with IT and cyber in the bullseye of Beijing’s ambitions.

Xi Jinping has put all of these elements together in various speeches, including his 2016 address to the Work Conference for Cybersecurity and Informatization. At least four points stand out:

First, military-civil fusion boils down to seeing the connection between “market and battlefield.” As reported in *Xinhua* in 2018, Xi stated that China must “grasp the historical

opportunities of information technology reform and new military revolution” and “deeply understand the inherent relationship between productivity and combat effectiveness, market and battlefield.”<sup>142</sup>

Second, not only do “cybersecurity and informatization” now constitute the “frontier field” for military-civil fusion, but no national security is possible today without them. Xi sees cybersecurity as “the core technology [and] the heavy weapon of the country.”<sup>143</sup>

Third, for the United States, cybersecurity is both a crucial vulnerability to be avoided and the soft underbelly. Xi echoes Sun Tzu and classical strategists when he importunes:

Only if one knows oneself and one’s opponent, will one not be beaten in a hundred battles. Not being aware of risks is the biggest risk. Cybersecurity has a very strong concealed nature, one technological loophole or one security risk may be hidden undiscovered for a few years, with the result that ‘we do not know who has entered, we do not know whether they are friends or foes, and we do not know what they have done,’ they can ‘lie low’ for a very long time, and suddenly spring into action when something is up.

To safeguard cybersecurity, we must first and foremost know where the risks are, what kind of risks there are, and at which moment risks occur, in other words, ‘a good listener hears the noiseless, a good watcher sees the shapeless.’<sup>144</sup>

Fourth, the battle for technology is simultaneously a struggle for superior discourse power. “At present,” Xi stated in 2016, “the cybersecurity game between large countries is not only a technological game, it is also a game of ideas and a game of discursive power.”<sup>145</sup>

Perhaps this reminder—that the technological struggle is also a war of ideas and words—is a reminder of the gap between China’s ambitions and China’s ability to accomplish its far-reaching goals. An international contest over rules of the road and standards for global technologies is ongoing. The outcome of that contest may well determine China’s ability to fully match and then surpass the United States technologically. Nonetheless, military-civil fusion aspirations face stiff headwinds from bureaucratic politics and other structural impediments within China. As one analyst has cautioned, just “because Chinese state-capitalism blurs the lines between state and private [does not mean] those lines are ... frictionless.”<sup>146</sup>

## Vision 2035

Vision 2035, which forms part of China’s ambitious 14th Five Year Plan (2021-2025), sees China’s achievement of a modern economy as integral to a larger regional economy predicated on new infrastructure, multilateral trade agreements, the development of Chinese megacities, and technological breakthroughs and high-tech supply chains.<sup>147</sup> OBOR, membership in the Regional Comprehensive Economic Partnership (RCEP) and other trade accords, and industrial policies like Made in China 2025 and military-civil fusion may create tomorrow’s most interconnected and robust regional economy.<sup>148</sup> By 2035, China hopes to double its per capita GDP.

Under this vision, China would expand R&D capabilities and transition into a “digital, cloud-based, and artificial intelligence (AI) economy.” This vision further expects 600 million Chinese to reside in five emerging super-city clusters—the Beijing-Tianjin-Hebei region (Jing-Jin-Ji), the Yangtze River Delta, the Mid-Yangtze River area, the Greater Bay Area (GBA), and the more recently announced Chongqing-Chengdu city cluster.<sup>149</sup>

Increasingly, global competition over high technology depends upon setting standards, and China is rapidly becoming a formidable power in setting global technical standards.<sup>150</sup> Standards 2035 is China’s plan to set international standards

in critical areas such as telecommunications and the Internet of Things and may provide it a springboard for dominating the technological competition.<sup>151</sup>

China's most recent five-year plan targets various tasks, including frontline technology sectors.<sup>152</sup> Chinese analysts have identified several prominent themes in this first of the three five-year plans on the way to 2035. One theme is a “dual circulation” economy that balances China's past emphasis on foreign exports with expanding domestic consumption and demand. Another theme is investment in strategic sectors and boosting innovation, including additional investment in modern infrastructure to “instigate the growth of high-tech manufacturing sectors such as 5G, digital centers, high-speed rail and clean energy.”<sup>153</sup> Also emphasized are competitiveness and secure supply chains “that are free of ‘weak links.’” Softer elements focus on green development and carbon neutrality, covering everything from climate change to building a Green Belt and Road.<sup>154</sup>

### From 5G to Quantum

The rise of Huawei and its domination of 5G hardware grew out of a combination of forward-looking industrial policy and predatory foreign policy. Hoping to lead the next industrial revolution, China enabled the development of national champions such as Huawei. Whereas US wireless carriers spend billions of dollars to access radio frequencies and property for cellular towers, China gives its carriers both spectrum and real estate.<sup>155</sup> China also boosts the export of Huawei and other Chinese technology firms as part of its Digital Silk Road, thereby aligning its domestic industrial policy with its foreign policy in an effort to out-compete US and European firms.<sup>156</sup>

China hopes that its increasing gains in AI will further boost its ability to dominate 5G telecommunications. Xi's goal is China becoming “the world's premier artificial intelligence center” by 2030, because that feat will “establish the key fundamentals for an economic great power.”<sup>157</sup> Although leadership in AI technology matters to the leaders of all major powers, the

securitization of quantum computing and cryptography poses a more severe long-term threat.<sup>158</sup> China's recent gains in quantum key distribution could render Beijing communications impervious to eavesdropping while simultaneously leaving US encryption vulnerable to the kind of codebreaking that was vital to winning World War II.<sup>159</sup> China's latest five-year plan invests heavily in quantum computing as, according to a quartet of analysts, “the power of quantum computing, quantum communications and other quantum enabled technologies will change the world, reshaping geopolitics, international cooperation and strategic competition.”<sup>160</sup> Consequently, as President Biden has indicated, whoever wins the competition in quantum technology will own the future.<sup>161</sup>

One of the most notable additions included in the 14th Five-Year plan is the new priority placed on quantum computing. Over the past five years, China has invested heavily in this sector. Qin Yong, director of the Department of High and New Technology at the Ministry of Science and Technology, has stated China's desire to leverage first-mover advantages in quantum technologies.<sup>162</sup> Beijing recognizes the potential of quantum computing to dominate the information processing space and thereby gain control over other sectors, such as advanced manufacturing, the digital economy, logistics, national security, and intelligence.

Currently, China is still trying to catch up with advanced economies, but its plans center on leaping to the top of the pack in the coming years.

### A Digital Superpower

If the diplomatic and political dimension of information power can be reduced to words, the economic and technological dimension of information power can be reduced to China's emergence as the world's leading cyber superpower.

Achieving economic power in a digital age requires China to become a cyber power, and so China's investments and policies

seek to make virtual reality actual reality for information and communication technology. We already exist within a “bipolar tech world,” as Microsoft executives Brad Smith and Carol Ann Browne have observed: “China’s emergence as a technology superpower, in some respects, signals that we now live in an increasingly bipolar technology world. China and the United States are the world’s two largest consumers of information technology. They have also become the two largest suppliers of this technology to the rest of the world.”<sup>163</sup> Most governments, businesses, and societies are wary of decoupling, fracturing the Internet and disrupting supply chains, and being caught in a bipolar technological competition that they cannot hope to win or control; but selective and managed decoupling is part of the high-tech competition for digital and technological sovereignty, as suggested by the competition in 5G and AI.<sup>164</sup> And that competition is not slowing down.

Democracies face a “moment of reckoning,” in the words of GCHQ Director Jeremy Fleming. Either democracies like the UK, Australia, and the United States compete with China in

5G, AI, and quantum computing, or they must live with the consequences of losing control over the web of surveillance and data-gathering technology that can be arrayed against them. “If we don’t control the technology, if we don’t understand the security required to implement those effectively, then we’ll end up with an environment or technology ecosystem where the data is not only used to navigate but it could be used to track us.”<sup>165</sup> In the wake of hacks from Russia-linked Solar Winds Orion Platform, breaches, and the China-backed attacks on the Microsoft Exchange Server, Fleming argues, “Cyber security is an increasingly strategic issue that needs a whole-nation approach. The rules are changing in ways not always controlled by government.” But governments that can seize advantages in today’s complex and interconnected digital world stand to wield greater power and security than otherwise.

China’s data-driven economic rise is giving Beijing unprecedented technological and cyber power. In a world of multi-use technology and connected information streams, that has profound implications for defense and national security.



## CHAPTER 4: SECURITY AND MILITARY INFORMATION

Information power is vital not just to China's achieving its political and economic ambitions but also its security objectives. To win without fighting—and avoid losing if violence became necessary—it is essential to dominate the information domain. Information thus creates the enabling environment for action, and information dominance maximizes the chances of successful action. Analysis that begins with the enumeration of an order of battle cannot avoid missing crucial non-military aspects of power. While China's vulnerabilities are many, Xi Jinping is to be credited with having created a comprehensive strategic framework. Within a view of security that encompasses the domestic and foreign arenas, China's armed forces and national security apparatuses are collecting big data, harnessing advanced digital-age technologies, and thinking systemically about potential conflict with the United States and its allies. Chinese leaders may well believe that they are

on the correct path toward attaining military primacy, especially in the Asia-Pacific. Still, China does not seek military conflict and would greatly prefer creeping assertions of sovereignty through gray-zone activities. For China, the military dimension of information power begins with a “total security” mindset and leads to systemic mastery over command and control.

### China's Total Security Paradigm

China is sensing a historical moment when it can get away with pushing its narrative, and global respect for its rules

---

Photo: A man looking at his phone is silhouetted against an image of the Chinese national flag on the side of a building in Beijing, during the 19th Communist Party Congress on October 23, 2017. (Greg Baker/AFP via Getty Images)



and ideas about order cannot be ignored. Not only is it quashing what it has termed a ‘century of humiliation,’ but it is also being inoculated from the predations of outside powers so that that historical chapter can never be repeated. Equipped with a robust authoritarian model of governance, China can now safeguard its system, prevent domestic subversion, and call the shots overseas. In a seminal speech at the beginning of Xi’s first term as CCP General Secretary, he called for “building a socialism that is superior to capitalism, and laying the foundation for a future where we will win the initiative and have *the dominant position*.”<sup>166</sup> [Emphasis added] In regaining the Middle Kingdom mindset that accompanies its newfound major-power position, the CCP under Xi has adopted what has been called a “total security paradigm.”<sup>167</sup>

### Information as the Foundation of Total Security

Xi’s total security paradigm emerged in 2013. One concrete pillar of that paradigm is the Central National Security Commission, which was established to improve decision-making across the government. “Currently we are challenged by pressure from two sources,” wrote Xi. “Internationally we must safeguard state sovereignty, national security and our development interests, and domestically we need to maintain political and social stability.”<sup>168</sup> Threats to peripheral sovereignty and internal stability required an integrated approach, with traditional defense and political and social stability working to mutually reinforce one another.

Marshalling the full authority of an autocratic government, Xi pulled rank on members of the CCP Central Committee in making his case for a long-term and all-encompassing strategy: “You come from different departments and units, and you need to see things from a greater perspective. For major decisions, first we should judge whether a proposed reform measure meets the needs of the country, and whether it is conducive to the long-term development of the cause of the Party and state.”<sup>169</sup>

Xi appreciates both the opportunity that information power provides and the threat it poses to his leadership, the CCP’s survival, and the China dream. Uncontrolled information is a massive source of risk for the Party. To obtain and maintain centralized control, Xi has seized on the need to centralize information and the Internet:

With fast growth in the users of micro-blogs, WeChat and other social network services and instant communication tools, which spread information quickly and can mobilize large numbers of users, how to *strengthen oversight...and how to ensure the orderly dissemination of online information, while at the same time safeguarding national security and social stability have become pressing problems for us...*[Our aim is] to integrate the functions of the related departments and *form joint forces in the management of the Internet covering both technology and contents, and ranging from daily security to combating crimes, to ensure correct and safe Internet usage.*<sup>170</sup> [Emphasis added]

In the name of “upholding and developing socialism with Chinese characteristics,” so-called ‘Xi thought’ has embraced an expansive and assertive paradigm that Party theory has enshrined as the “total national security outlook.”<sup>171</sup> Xi’s total security concept requires regulating all areas of human activity within China and the forceful expression of CCP views outside China. In sharp contrast to China’s official foreign ministry and state media narrative, Xi promoted a zero-sum Cold War framework when the Obama administration announced its pivot to Asia and sought strategic stability in US-China relations. Mao Zedong saw cultural subversion as a significant threat, notably when US policy promoted communist rollback in the 1950s. Xi governs a far more powerful state, and that power amplifies its active use of discourse power for “‘securing’ cultural expression, information, and media against forces deemed politically harmful to the CCP and its leadership.”<sup>172</sup>



Information power enables Beijing to pitch OBOR as a win-win proposition despite the predatory economic practices and lack of transparency it employs. It informs Made in China 2025 high-technology industrial policy. In addition, information power is the basis of PLA military strategy—from its Three Warfares to system-destruction warfare. Information helps Beijing blur the distinction between domestic and foreign policy, between civilian and military power, and between fact and fiction. For instance, because virtually everything threatens China's "image sovereignty" (*xingxiang zhuquan*), the CCP has mobilized an Internet army of commentators to fight on "the main battlefield for public opinion."<sup>173</sup> So, in early May 2021, when the Group of Seven countries meeting in London issued a lengthy communique including references to human rights and cross-Strait stability, a self-described "wolf warrior artist" generated a computer-generated graphic depicting the G-7 leaders as foreign invaders during the 1900 Boxer Rebellion.<sup>174</sup>

### Culture and Sovereignty Are Indivisible

Because protecting Chinese culture is inseparable from its other sovereign interests, Beijing tends to see foreign public displays of diplomacy as attempts to undermine Chinese culture and society with a possible color revolution. In addition, it perceives its benign use of Confucius Institutes as an unalloyed public good, providing language and cultural education with no strings attached. For instance, one critique of State Department support for Chinese nongovernmental organizations to help instruct on the rule of law or corporate social responsibility was dismissed as "selling dog meat as mutton," in the words of Professor Li Haidong of the China Foreign Affairs University.<sup>175</sup> Opined the *Global Times*:

as an institution that enhances people's understanding of the Chinese language and culture, Confucius Institutes have for many years upheld the purpose of abiding by the laws and regulations of host countries and have never participated in any activities related to the host countries' politics,

religious affiliations, or racial discourse. Since the first Confucius Institute was founded in 2004, these institutes have had many achievements in improving China-US cultural exchanges.<sup>176</sup>

Although Chinese professors and state media are given a principal role in dispensing invective, the People's Liberation Army and Chinese national security officials are not restricted to passive listening or to reputation-protection efforts. Instead, they use data collection, their technological prowess, and all instruments of power available to them to advance intelligence and foreknowledge. Included is the comprehensive collection of information—not just to suppress Uighurs in Xinjiang or crack down on Hong Kong autonomy—but also to monitor, track, and prepare to thwart foreign forces. Moreover, open democracies and careless bureaucracies have unwittingly facilitated much of this information-collection activity.

Espionage is nothing new, and China is not alone in leveraging relationships, physical location, and open access to information sources. But, based on the total security concept of military-civil fusion, the PRC is serious about collecting datasets and information and integrating these into domestic and foreign security policy. The techno-nationalist approach seeks to achieve economic preeminence through such emerging information-centric technologies as 5G, artificial intelligence, robotics, 3D manufacturing, and quantum computing, all technologies having military as well as civilian value.

Where the digital age transformed signal intelligence collection, computers have transformed Chinese intelligence.<sup>177</sup> China had achieved a global reach even before building outposts worldwide or its satellite network.<sup>178</sup> China's exploitation of computers is visible in "Titan Rain," the name given to a series of cyber-theft intrusions in US defense, space, and corporate networks and in UK and other networks that started nearly two decades ago.<sup>179</sup> Since then, such intrusions have grown in number and complexity but have generally remained in the gray

zone between war and peace, calibrating coercion to fall short of triggering outright conflict.

## Exploiting the Gray Zone

Seizing opportunities incrementally and below the threshold that might trigger a military response, the focus of China's military activities is heavily on operating in the gray zone separating peace and war. Employing coercion intermingled with inducements, China seeks to neutralize anti-China coalitions before they emerge. If necessary, however, Beijing is also preparing to use force to render stillborn any international coalition of forces that would obstruct Beijing's goals. Information infuses all Chinese actions, including gray-zone coercion in maritime Asia. In addition, China seeks to isolate smaller opponents, ranging from Taiwan to the Philippines to key US allies like Japan and Australia.

## China Occupies the Gray Zone with Information

While gray-zone activities allow China to harness all instruments of power to wage an asymmetric campaign, information is at the center of its holistic political warfare campaign. As its military might mounts—thanks to more than two decades of increases in defense spending—China has begun to move beyond its now well-advertised anti-access and area denial (A2/AD) posture.<sup>180</sup> A2/AD capabilities rely on the Asian mainland for defense in depth (many bases and means of production) and favorable force-exchange ratios (firing missiles is easier and cheaper than building naval combatants). With the building of artificial island reefs in the Spratly Islands, China can maintain hundreds of ships—naval, coast guard, and maritime militia—over sustained time periods. These ships can then survey, harass, and intimidate neighbors all along the perimeter of China's expansive 9-dash line claim to the vast majority of the South China Sea. Thanks to its ability to resupply ships from Fiery Cross Reef, Mischief Reef, and other Spratly bases, China now regularly deploys a significant maritime presence around Vanguard Bank to stymie Vietnam's ability to explore for oil and gas within its Exclusive Economic Zone (EEZ);

pressure Malaysia to accede to China's de facto control of its EEZ around Luconia Shoals; and coerce the Philippines and control the waters around the Second Thomas Shoal and Scarborough Shoal.<sup>181</sup>

Detailed examination of what China has built on its artificial island reefs reveals more than docks and runways and a sophisticated array of information-centric technology. Michael Dahm, a former US assistant naval attaché in Beijing, details the mix of fiber-optic cables, satellite communications, high-frequency communications, inter-island communications, radar, electronic intelligence, and other infrastructure that have been assembled on critical outposts like Fiery Cross Reef in the Spratly Islands.<sup>182</sup>

## The Great Leap from a Gray to a Black-and-White Zone of Conflict

China's military expansion may propel China to consider actions beyond the gray zone. As China has accumulated new power-projection capabilities, it has overcome its previous opposition to overseas bases. For instance, Djibouti is now one of its overtly military installations overseas. But Beijing is said to be scouting not just for a potential 'string of pearls' in the Indian Ocean but for bases and access points along the west coast of Africa and the Gulf of Thailand and throughout the South Pacific.<sup>183</sup> Meanwhile, China is also deploying aircraft carriers and naval combatants with unmatched alacrity.

China's emerging blue-water navy, backed by comprehensive national and maritime power, is "tipping the balance in the Pacific."<sup>184</sup> In thirty-five years, the People's Liberation Army Navy (PLAN) has been transformed from a coastal defense force into a serious peer competitor of the US Navy and of the naval forces of US allies in the Western Pacific. Without an effective counterweight, China may, over the next ten to fifteen years, come to dominate militarily most of the maritime Indo-Pacific. While Beijing already enjoys global maritime reach, the sharpest impact of its ascending naval power affects potential

contingencies involving Taiwan, the Senkaku Islands in the East China Sea, and disputes in the South China Sea. Moreover, the PLAN and its auxiliary forces intend to maintain this trend over the next decade, prompting some to term the 2020s the “decade of concern,” and mounting PLA capabilities could, in fact, embolden Chinese leaders to become more aggressive.

Before retiring as US commander of the Indo-Pacific Command, Admiral Philip Davidson warned that China’s rapid defense buildup was “accumulating risk” and an “unfavorable balance.” He was worried China might decide to attack Taiwan in the next several years.<sup>185</sup>

Deterrence could break down, and China could go on the offensive against Taiwan or other countries in the next five years. Admiral Davidson illustrated China’s dramatic force posture gains in the Asia-Pacific over the past two decades.<sup>186</sup>

But while naval competition is vital, another type of competition is worth also bearing in mind— political, or irregular, warfare, which is making a resurgence. Major and regional powers bent on revising the post-World War II global order, in whole or in part, are seeking to achieve their aims without triggering a major conflict. Through shadow and covert warfare and various other means designed to achieve success with little or no use of kinetic force, revisionist powers are eroding rules, coercing states, and weaponizing information. If China does use force on its periphery, it will do so because it thinks its preparations have produced a balance of power that would allow a successful and swift, sharp gray-zone dust-up.

## System vs. System Warfare

Although China wants to exert its influence without triggering open conflict, it is simultaneously preparing to win a major-power conflict, if necessary. In this preparation, the focus of China’s military strategy is system-destruction warfare, with a heavy emphasis on information-based intelligence, weapons, and targets.

As one RAND analyst writes, China approaches modern war as a contest between opposing systems.<sup>187</sup> Waging a modern conflict therefore requires the destruction of an adversary’s system, and thus modern war is not about annihilating enemy forces on the battlefield but is,

**rather, ... won by the belligerent that can disrupt, paralyze, or destroy the operational capability of the enemy’s operational system. This can be achieved through kinetic and nonkinetic strikes against key points and nodes while simultaneously employing a more robust, capable, and adaptable operational system of its own. These realizations have been reached after watching two decades of US post-Cold War operations and the revolutionary role of information systems in that context. Systems thinking has an enormous impact on how the PLA is currently organizing, equipping, and training itself for future war-fighting contingencies.**<sup>188</sup>

Considerations related to countering China’s systems’ approach to warfare requires detailed military analysis and so transcends the scope of this report. Of importance here, however, is that information is at the center of China’s total competition strategy— whether this consists of influence-seeking or modern warfare. Fortunately, nuclear weapons remain a sobering deterrent to embarking on World War III. Although major powers have of late contemplated conflict more openly, the aim of much of this rhetoric is to jockey for psychological advantage, reassurance, and deterrence. The objective of both China and the United States appears much more focused on gaining influence without instigating open conflict, and it is this competition short of war that consumes so much data and information technology.

How can the United States and allies like Australia win the total competition with China, given that winning means avoiding major war while denying China or any single power exclusive control over the Western Pacific and maritime Asia? A winning

approach requires the adoption of a similar total competition strategy, albeit one suited to democracies. It also requires the favorable slate of activities required to bolster the prevailing rules, institutions, and partnerships to preserve a sustainable

Indo-Pacific order for all. One such response would start with a grand strategy of democratic solidarity and then focus on specific actions that could be taken to strengthen the competition's political, economic, and military dimensions.



## CHAPTER 5: PILLARS OF A DEMOCRATIC GRAND STRATEGY

The alliance response to China's information challenge should take the form of a grand strategy of "democratic solidarity."<sup>189</sup> Democracies thrive on transparency, truthful and accurate information, and accountability; autocratic governments prefer opacity and dissemination of knowledge that serves central political control and diminishes the importance of popular accountability. Accordingly, the US-Australia alliance needs to forge a larger coalition among like-minded countries. While the aim should be to avoid an entrenched, zero-sum Cold War, democracies should borrow from successful policies employed throughout the post-World War II period. President Truman understood the significant stakes that communism's taking root in Greece and Turkey would entail—namely, "whether the postwar world would be shaped by liberal principles of self-determination and freedom of choice—or would

instead be molded by coercion, predation, and authoritarian aggression."<sup>190</sup> As Hal Brands and Charles Edel write, "The overarching strategic question of this century is whether the United States and other democracies can preserve a system predicated on the dominance of liberal governments and liberal ideas, or whether the world will slip back toward a state in which

---

Photo: British Prime Minister Boris Johnson, US President Joe Biden, Canadian Prime Minister Justin Trudeau, Italian Prime Minister Mario Draghi, President of the European Commission Ursula von der Leyen, President of the European Council Charles Michel, Japanese Prime Minister Yoshihide Suga, German Chancellor Angela Merkel and French President Emmanuel Macron sit around the table during the G7 meeting on June 11, 2021 in Carbis Bay, Cornwall. (Leon Neal - WPA Pool/Getty Images)



illiberal regimes and coercive practices are ascendant.”<sup>191</sup> The information contest lies in the bullseye of this question about the future fate of democracies.

Prime Minister Scott Morrison and President Joe Biden have already expressed their implicit support for a grand strategy of democratic unity. Addressing India’s Raisina Dialogue in mid-April, Prime Minister Morrison warned of “a great polarization” developing “between authoritarian regimes and ... liberal democracies.”<sup>192</sup> Prime Minister Morrison stated that democratic sovereign nations are “threatened and coerced by foreign interference,” including sophisticated cyberattacks.<sup>193</sup> Problems ranging from “economic coercion” to an assault on “rules and norms” require collective action from like-minded countries.<sup>194</sup>

Echoing his Australian counterpart, President Biden confidently declared before a joint session of Congress: “Autocrats will not win the future. We will.”<sup>195</sup> But the president also acknowledged that Xi Jinping’s China is “deadly earnest about becoming the most significant, consequential nation in the world. He and others ... think that democracy can’t compete in the 21st century with autocracies because it takes too long to get consensus.”<sup>196</sup> This view is mistaken, Biden argued: “We will meet the center challenge of the age by proving that democracy is durable and strong.”<sup>197</sup> Democracy remains the most desirable form of government, despite its shortfalls. However, the diffusion of information over the Internet and through digital technologies requires that democracies evolve to deal with the rise of disinformation and ‘fake news.’

Dealing with China’s information power requires a level of democratic solidarity that avoids embracing autocratic rulers, seeks to rally like-minded countries, and protects democratic values at home.<sup>198</sup> Allies, contend Brands and Edel, should “focus primarily on building denser, overlapping networks of cooperation around key issues, and exploiting—where possible—nascent moves in this direction.”<sup>199</sup> For instance,

advancing networked security was plainly on display in May during the ARC 21 amphibious exercise comprised of platforms and units from Australia, the United States, Japan, and France.<sup>200</sup> Such networks maximize collective strength and minimize risk to individual nations.<sup>201</sup> Because “democratic solidarity is more a matter of function than form,” the US and Australia should replicate the style of the first leaders’ meeting among the four Quadrilateral Security Dialogue, or Quad, nations—the United States, Australia, Japan, and India. The Quad virtual summit addressed real-world challenges such as climate change, high-technology rules of the road, and, most concretely, a plan to help vaccinate more than one billion people in Southeast Asia and the Asia-Pacific.<sup>202</sup>

While Brands and Edel offer eight pillars for a grand strategy of strategic solidarity, coping with China’s total information competition requires five lines of effort. Three pillars can be adapted from Brands and Edel: 1) countering coercion, 2) advancing technological competitiveness and cooperation, and 3) shaping international standards and institutions. Two additional lines of effort are needed: 4) waging democratic influence operations and 5) forging an integrated or confederated innovation industrial base.

## Countering Coercion with Collective Strength

Over the past decade, countering China’s coercion has concentrated on imposing costs on gray-zone maritime activities, especially in the South China Sea. Blunting the effects of coercion in this manner can assume either an offensive form consisting of cost imposition or a defensive form, i.e., adoption of a defensive posture through strengthened defenses and resilience. For Australia, the focus of the most glaring instances of recent Chinese coercion has been economic statecraft. Beginning with halting purchases of Australian barley, beef, and wine in May 2020 escalated its embargo on Australian goods over the next twelve months. Secretary of State Anthony Blinken, meeting with Foreign Minister Marise Payne, emphasized “that

the United States will not leave Australia alone ... on the pitch, in the face of economic coercion by China. That's what allies do. We have each other's backs so we can face threats and challenges from a position of collective strength."<sup>203</sup>

Notably, however, Beijing's focus is not economic policy but rather the ideas and words of the democratic powers standing in its way. Thus, it leverages its economic importance to penalize state and non-state actors that call out Chinese acts of political oppression or otherwise stray from Beijing's approved narrative.

Demonstrating collective strength is essential to countering coercion. Although joint action can take the form of a declaratory policy such as supporting freedom of speech, backing words with tangible actions is far better—strengthening supply chains or reducing over-reliance on Chinese export markets, for instance. Because the best defense is a strong economy, it is incumbent on the United States to work closely with Australia and other allies and partners to retain the open innovation quality of market economies while addressing key areas of competition in emerging technologies.

## Enhancing High-Tech Competitiveness

China is determined to gain technological supremacy in 5G telecommunications, AI, robotics, fintech, quantum computing, biotechnology, and other sectors identified in Made in China 2025 and subsequent CCP industrial plans. Given that China's state capitalism relies on state subsidies, IP theft, massive information collection, and integrated policies difficult for democracies to mirror, the United States and Australia should seek to level the playing field.

To do so, Washington, Canberra, and other democracies can work jointly to protect both civil liberties and intellectual property. By combining research and development in selected technologies, democracies can prevent China from buying superiority in critical areas like AI. By working collectively to set high international standards on export controls and

transparency, the United States and Australia can prevent China from imposing a rule set and set of business practices favorable to Beijing that would not hold up under close scrutiny. Joining with a group of like-minded democracies, perhaps the G-7 plus a few other advanced democracies, would build the kind of collective strength needed to stand up to coercion and technological competition.

Unlike the United States with its big-tech firms, however, small- and medium-sized enterprises comprise 97 percent of Australia's industry, and the cultures of these enterprises include a willingness to work with anyone. For example, the labor force in Australia's fledgling space industry by and large displays a lack of concern related to security, but the clearance requirements adopted by the industry do somewhat compensate for this lack. However, Chinese intelligence and military operations target the relatively open environments of academic, research, and commercial enterprises in democracies, and so, despite differences in US and Australian economies, both provide a range of targets for Beijing to attempt to exploit.

The solution to China's behavior in this area is neither complacency nor total decoupling, and the choice between interdependence and decoupling is a false one. China is part of the global and Indo-Pacific economy, and neither the United States nor Australia can afford the disruption to the entire global economy that total decoupling with China's economy would entail. However, disentanglement can be performed to varying degrees of severity—termed targeted, managed, and selective decoupling—and is well underway and almost certain to continue, especially in the most competitive area, that of emerging and disruptive technologies. Furthermore, the ICT sector in particular requires increased levels of vigilance, extra resilience, and implementation of targeted regulations. The Biden administration's 100-day review of supply chain security coincided with a decision to largely reaffirm—but seek to make more enforceable—the list of Chinese companies that are off limits to US investors consisting of 59 companies and including

Huawei and other tech firms, particularly those affiliated with the PLA.<sup>204</sup>

However, the United States and Australia understand that erecting constraints on China can be counterproductive or, at a minimum, produce both expected retribution and unintended consequences. Few were surprised by China's condemnation of Prime Minister Turnbull's August 2017 decision to ban Huawei (specifically, "vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law").<sup>205</sup> Regarding less intended consequences, the Trump administration's May 2019 executive order preventing Huawei from using Google's Android operating system prompted Huawei to accelerate development of its own operating system, HarmonyOS. Although how this will play out is uncertain at this point, it seems likely that sanctioning Huawei could have the unintended consequence of spurring Chinese competition, thereby undercutting Google and other US firms in global markets and putting an increasing number of devices globally beyond the reach of US scrutiny and protection.<sup>206</sup>

The United States should not only seek to preserve its unique status as a global innovation hub but should also, along with Australia and other democracies, ensure a better-educated workforce with deep expertise in STEM education and R&D. Catalytic initiatives—such as the bipartisan Senate proposal to spend as much as \$100 billion to fund a new Directorate for Technology within the National Science Foundation and \$5 billion to establish a Democratic Technology Partnership mechanism within the State Department—could help jumpstart a more holistic and competitive approach.<sup>207</sup> Congress is also pushing to boost US competitiveness in high-end semiconductor manufacturing.<sup>208</sup> The challenge is for Washington and Canberra to identify priority areas of overlapping interest in which to sustain a durable and highly competitive response. However, sharing the rules and organizations through which these technologies would be regulated remains another critical area for cooperation among like-minded states.

## Shaping International Standards and Institutions

The United States and Australia should contest authoritarian influence in international institutions and global norms and standards, especially regarding the data and technology of the digital era. Cyber rules of the road, i.e., standards governing global communications, finance, and emerging technology such as AI, need to reflect liberal democratic values—or, at a minimum, not undercut them. A club of democratic nations could steer development of multilateral norms, and it remains vital for the United States to engage rather than leave multilateral institutions, ranging from the World Health Organization to the Paris Agreement on climate.

A significant challenge is, on the one hand, engaging in competition without inducing a self-fulfilling prophecy of major-power confrontation and conflict, and, on the other, balancing economic ties and security. Ample lessons and recommendations on which to draw are readily available, however. For example, the Commission on the Theft of American Intellectual Property emphasizes the need to ensure mutual benefit and reduce vulnerability. In March 2021, the IP Commission underscored the importance of at least four activities: 1) elevating responsibility and authority for IP protection and messaging to keep it a high-priority issue—even setting as a national goal the delegitimization of Chinese indigenous innovation efforts that are dependent on IP theft; 2) imposing costs for committing such violations as denying infringed products access to markets and thereby changing the cost-benefit calculus of IP theft; 3) increasing the speed and force with which IP theft is identified and remedied; and 4) better informing US businesses regarding IP theft threats abroad.<sup>209</sup>

These recommendations supplement several actions taken in recent years by the United States to stem IP theft, including the Holding Foreign Companies Accountable Act; the Protecting American Intellectual Property Act of 2020; Security and Exchange Commission regulations concerning IP; FY21

provisions of the National Defense Authorization Act intended to deter China's economic espionage; reform of the International Trade Commission; NDAA FY20 Section 1281 to update lists of entities with a history of IP theft; the Foreign Investment Risk Review Modernization Act of 2018; and the 2016 Defense Trade Secrets Act, among others. These measures should be part of an ongoing alliance consultation to determine priorities for closing gaps without stifling innovation.<sup>210</sup>

## Waging Democratic Information Operations

In countering coercion, advancing technological competitiveness and resilience, and forging agreed-upon rules and institutions, the first step is to spotlight what China says and does. Misinformation and disinformation require transparency and facts, and this truth-telling needs to be disseminated via effective campaigns. Hence, the need to wage democratic information operations is pressing.

As necessary as countering coercion, enhancing high-tech competitiveness, and shaping rules and institutions are for democratic solidarity, they fail to address the seriousness of China's influence operations and the need to counter these effectively. Recognizing that the aim of China's powerful toolkit of influence operations is to project its legitimacy and power abroad, how can the United States and Australia counter or pursue influence in democratic ways? Education, transparency, and better use of cyberspace constitute three important elements of an effective response.

*The first step is to build human and institutional capacity within the government and across society to understand CCP tactics.* Beijing's influence operations seek to promote its own party-state legitimacy and "tilt the playing field in its favor" by leveraging relations with people and institutions in government, academia, the private sector, and the media. As noted by Duncan Lewis, the former Director-General of the Australian Security Intelligence Organization, China prefers "pulling the strings from offshore."<sup>211</sup>

*A second step is giving institutions the ability to shine a spotlight on unwanted foreign influence.* For instance, the CCP strangles open discussion of human rights or autonomy in Xinjiang, Tibet, Hong Kong, or Taiwan. Among the entities China relies on to exert pressure or counter free speech is the Chinese Students and Scholars Associations (CSSA) worldwide, which mobilizes students to support Beijing's foreign policy. For instance, the LinkedIn Page for the CSSA at George Washington University claims that it "is a student organization dedicated to the goal of promoting social, intellectual and cultural activities for Chinese students and scholars at GWU" and "facilitating the exchange of information between China and Chinese students studying abroad."<sup>212</sup> However, the high degree of government control of the CSSA is both unusual and lacking in transparency, especially regarding activities in an open academic setting.<sup>213</sup> Officials who illuminate the problem are quickly assailed. For instance, FBI Director Christopher Wray testified that there is a "level of naivete on the part of the academic sector," mainly because of China's "use of nontraditional collectors ... whether it's professors, scientists, students."<sup>214</sup> This testimony prompted some student leaders at Georgetown University to write a letter to the university president complaining that the FBI Director was engaged in "a witch-hunt fueled by Dreyfus-style xenophobia and McCarthyist craze"<sup>215</sup> and so provide an example of Wray's testimony. Moreover, the academic-government divide appears to have expanded, leaving less room in the center for a frank discussion about the challenges posed by foreign actors like CSSA that seek to exploit Western democratic institutions.

*A third measure involves cyber training to guard against coordination of influence operations via cyberspace.* Tech platforms performing better policing for disinformation, trolling, and fake accounts would aid in accomplishing this. Facebook now flags what it determines to be disinformation, for instance. However, a Chinese foreign ministry spokesman, a government official, who tweets a grotesque, fabricated image of an Australian soldier killing a young Afghan child poses a quandary for Twitter.<sup>216</sup>

Finally, vital to understand is that China's influence ecosystem makes it difficult to separate foreign from domestic policy, influence from engagement, and political warfare from war itself. For lack of a better term, this is dubbed the gray zone between peace and war—and the information component is a vital dimension running through all facets of this zone. Competing with China in the gray zone requires a disciplined focus on *shaping long-term allied objectives* and denying China the opportunity of exercising malign influence over important economic and social institutions.<sup>217</sup>

## A Confederated Innovation Base

Innovation is one key element of strong, positive collective action. The United States and Australia need to work with other democracies to demonstrate the inherent advantage of a system of innovation that is based on a free and open governance model. Other countries should not have to buy into an authoritarian rule set to achieve economic growth. China deploys all the resources available to a state capitalist model towards its top-down goals, but that democratic spending alone can out-compete China does not follow. Although the combined budgets of democracies may exceed China's, there is no way that a democracy can harness its entire potential without treading on its political independence. However, targeted initiatives can help catalyze innovation. The proposed \$100 billion Directorate for Technology within the US National Science Foundation would be well positioned to be a force multiplier for innovation.<sup>218</sup>

Still, Washington and Canberra need a coordinated game plan that fully utilizes market forces to remain innovation leaders, while also relying on diplomatic means to pressure China into complying with high global standards and rules. As one astute observer argues, "Out-competing and out-innovating China requires that America remain the world's most attractive innovative hub, enticing the best talent, drawing in the most

venture capital, and generating the largest revenues to support US leadership of technology's newest frontiers. It means continuing to 'move fast and break things.'"<sup>219</sup>

We live in an era of information economies. From Australian and American universities to China's wolf warrior diplomacy, to Huawei and 5G telecommunications, and to competition for mastery of AI, there is no shortage of issues for which economic power hinges on information. To perpetuate economic growth and achieve ascendant economic power, the CCP uses information as both a carrot and a stick. Once another economy has come to rely on doing business with China, the pain of disentangling that relationship makes targeted decoupling an arduous and costly prospect. At the center of economic competition is a major-power contest over the foundational technologies of the 21st century, "the new crown jewels of geostrategic power."<sup>220</sup>

A few years ago, open innovation was seen as an advantage—a magnet attracting the best and brightest minds and producing discoveries that could lift all boats. However, major-power competition is compelling greater degrees of protectionism and national self-reliance. At the same time, democracies have had to erect new constraints to safeguard their open innovation economies from being exploited by authoritarian states like China. The Trump administration spoke of the "National Security Industrial Base," and various laws, sanctions, and tariffs were imposed, primarily to constrain what was seen as China's predatory economic behavior. A confederated alliance innovation base could thus constitute an essential building block in a long-term, positive agenda for tomorrow.

The final section of this report suggests specific measures that the United States and Australia should adopt to defend their political, economic, and security interests from the predations of China's total information challenge.





## CHAPTER 6: POLICY RECOMMENDATIONS: AN ALLIANCE INFORMATION ACTION AGENDA

China wields information power to control discourse, gain economic and technological leadership, and ensure that its military is unsurpassed; hence, a unified response to this challenge by the United States and Australia is needed. Building on shared security interests and democratic values, US-Australian alliance managers should begin by forging a unified view of an emerging, advanced digital era in which comprehensive information power determines power and order. Thus, this concluding section offers specific recommendations for the United States and Australia to blunt China's bid for information dominance and successfully compete across the political, economic, and military dimensions of power.

### Recommendation #1: Establish an Information Dominance Steering Group as part of the Australia-US Ministerial Consultations (AUSMIN).

Tapping officials from appropriate departments and agencies of each government, the Biden and Morrison administrations should establish a strategic steering group dedicated to information dominance and its multi-faceted dimensions. This group's purpose would be to inventory the breadth of emerging

---

Photo: Australian Foreign Minister and Minister for Women, Marise Payne, holds a joint press availability with US Secretary Antony Blinken at the US State Department in Washington, DC on May 13, 2021.

(Leah Millis/Pool/AFP via Getty Images)

challenges and ongoing policies and to identify ideas salient to joint action. By reviewing a problem's diplomatic, economic, and military dimensions, the steering group could then catalyze, shape, and guide a coordinated set of activities and could also aid each ally in steering its course while collaborating with others both regionally and globally.

## Political and Diplomatic Responses

Information can inflict damage, but it remains, first and foremost, a tool of political warfare.

As the schoolyard saying goes, “Sticks and stones may break my bones, but words will never break me.” Chinese information operations seek, however, to defy the physical reality of this juvenile maxim. Keeping overt force in reserve, Beijing deploys words to seize control of a narrative and, as necessary, render harm. Information operations are thus used to muzzle critics, deflect blame, penalize opponents, promote a favorable image, spread conspiracy theories, and attempt to dictate what can be said about China. Three lines of effort are central to countering this Sino-suasion: protecting free speech; ensuring transparency; and building alliance discourse power.

### Recommendation #2: Protect free speech by reporting on China's influence and interference with civil liberties outside China's border.

Each government should determine the best means of producing an objective and credible report detailing unwanted foreign influence and interference activities by China as well as others. For the United States, the Biden administration should consider tasking the State Department's Bureau of Human Rights, Democracy, and Labor with preparing a fact-based narrative of China's infringements on freedom of expression, a free press, Internet freedom, and other civil liberties that occur outside of China, particularly within the Indo-Pacific region including Australia and the United States.

The Department of State already compiles a comprehensive country-by-country description of human rights issues

worldwide.<sup>221</sup> However, these detailed descriptions focus on events within China, including Hong Kong, Macau, and Tibet. Still, they seldom relate issues in which the government of China or Chinese-affiliated groups or individuals interfere with civil liberties elsewhere, including among ethnic Chinese diaspora populations.<sup>222</sup> This report could fill that gap and highlight what is publicly known about China's influence and interference operations beyond its borders.

The US should coordinate its report with the Australian Department of Foreign Affairs and Trade (DFAT) so as to determine how Canberra could produce a similar report. Additional funding should be provided to DFAT, which might commission an objective, third-party assessment from a nongovernmental research institution. The findings of these reports could be presented at an international public forum led by an NGO examining freedom of expression and civil liberties within the region and featuring leading research organizations, media representatives, and academic institutions.

### Recommendation #3: Develop a common toolkit for democracies designed to blunt disinformation and malign information operations.

By mobilizing a small group of perhaps 10 democracies—a D-10 that includes the Quad partners—the United States and Australia could help devise a playbook for countering unwanted foreign interference and malign information operations—both overt and decentralized ones and covert ones.

Among other nations, Australia and the United States have passed legislation or enacted executive orders to help protect against unwanted foreign influence and interference. Registration and other disclosure requirements are at the heart of Australia's Foreign Transparency Scheme Act of 2018 and the US Foreign Agent Registration Act (FARA). But the range of government, private, and civil society requirements is diverse, and leading democracies should help craft the highest standards and highlight the best practices for countering these malign activities.

In preparation for a larger group of democracies, the United States and Australia should take the first step by conducting a joint audit of relevant laws, orders, policies, and best practices within their countries. The purpose of this audit would be to compare the two governments' laws and executive orders and make recommendations to each government with respect to refinements, additions, or modifications to the legal and regulatory scaffolding. The audit could then help inform a framework that other democratic countries could employ.

Importantly, each government should create an ombudsman-like advisory panel to ensure that views and critiques are broadly representative and that security measures are objective, balanced, and free from racism and xenophobia.

#### Recommendation #4: Build alliance discourse power by jointly reviewing lessons learned from the State Department's Global Engagement Center.

The Global Engagement Center, created in 2016, is an interagency entity for coordinating messaging intended for foreign audiences. Its core mission is described as follows:

To direct, lead, synchronize, integrate, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining or influencing the policies, security, or stability of the United States, its allies, and partner nations.<sup>223</sup>

After five years of evolving operations, a comprehensive review of the GEC's record of achievement is now due. The Biden administration should carefully examine the center's record and identify GEC strengths and best practices, as well as any significant gaps or concerns. A US performance review undertaken in close consultation with Australia's National Counter Foreign Interference Coordinator (NCFIC), a position created in 2018, and other Australian officials with

experience and expertise could suggest ways to improve countering Chinese disinformation.<sup>224</sup> Congress and the Parliament should be approached to augment existing capabilities, with the proviso that there is strict accountability and oversight.

### Economic and Technological Responses

China has achieved far more influence in the economic dimension of competition than it would otherwise because of its phenomenal growth in recent decades and, more recently, because of a lack of US engagement. However, the United States and its allies can offer other partners in the Indo-Pacific an alternative to the supposedly binary choice between America and China that apparently makes them uncomfortable. Countries should not be forced to decide between either forfeiting economic gains to remain secure or surrendering their security to become prosperous, and thus Indo-Pacific governments should be able to pursue both prosperity and security. By recognizing the information dimension of China's competition—including One Belt One Road's limitations—and building on the strengths of the US, Australia, and other democracies, President Biden, Prime Minister Morrison, and other allies can mount an effective, asymmetric response to One Belt One Road.<sup>225</sup>

#### Recommendation #5: Expand the human capacity of a trusted science and technology (S&T) network.

The United States and Australia should expand on allied and partner S&T personnel exchanges and training and educational opportunities. The allies should increase scientific interactions between one another and with other democratic and like-minded partners across government and industry. Additionally, governments can learn from industry best practices related to personnel exchanges, and critical areas such as cybersecurity, artificial intelligence, and quantum computing deserve special effort. Washington and Canberra can coordinate their efforts in building out the human capacity of a trusted science and technology network. Further, they and other like-minded



countries can pool resources to create training, educational, research, and development funding for specialized areas related to AI and quantum computing.<sup>226</sup> For many regional partners, nurturing an S&T relationship in stages, beginning with less sensitive areas, will be necessary. Lastly, working with non-English-speaking partners will require overcoming additional barriers to cooperation.

Although officials within Australia's Defence Science Technology (DSTG) and their American counterparts would remain more comfortable working with Five Eyes partners through Five Points, the benefits of expanding S&T cooperation with advanced economies like those of Japan and South Korea would justify the effort required to do so. In addition, making Japan a member of Five Eyes deserves serious consideration,<sup>227</sup> and the United States should again review streamlining of the International Traffic in Arms Regulations (ITAR), which ideally should reflect the twin ideals of maximizing security and minimizing strategic cooperation.

#### Recommendation #6: Expand English-language education for Indo-Pacific partners and ramp up Chinese-language training for US and Australian students.

Along with efforts to increase partner capacity in the Indo-Pacific, it is important to give partners from non-English-speaking countries the ability to communicate with Americans and Australians. Enhanced English-language programs would increase the pool of potential employees available to help their countries in areas essential for combating disinformation and working in an advanced digital economy. Expanding enrollment of students from regional countries other than China in US and Australian universities would also help offset possible reductions in the number of Chinese students enrolled.

At the same time, the United States and Australia should invest significantly in Chinese-language education opportunities

in their own countries. Chinese-language education could be delivered from abroad and virtually and could emphasize primary, secondary, and university education programs. In addition, increased funding in this field of study would reduce colleges' and universities' reliance on foreign-funded Confucius Institutes. One possibility here is an increase in scholarships for study in Taiwan.

In short, both countries should increase investment in ensuring an educated labor force steeped in both language and regional studies, on the one hand, and science and technology on the other. Also, alliance mechanisms for dialogue and policy coordination require refinement. A workforce prepared for the decades ahead and institutional organs purpose-built to meet the challenge of China's information power will be tremendously important in ensuring the resilience of democracies in the face of digital-age illiberalism.

#### Recommendation #7: Create a US-Australian supply chain task force to review bilateral cooperation in information and communications technology (ICT) supply chains.

The pandemic has highlighted supply chain vulnerabilities and technological competition with China. Using the study of bilateral cybersecurity cooperation and the Biden administration's major review of supply chain security as a springboard, Canberra and Washington should establish a joint task force for addressing ICT supply chain issues, beginning this process with a discussion of the findings of the Biden administration's supply chain review. However, as the weight of this report suggests, ICT supply chains are deserving of particular emphasis.

#### Recommendation #8: Australia and the United States should work together to establish high-standard multilateral digital trade rules and norms.

Officials from the United States Trade Representative (USTR), Australian DFAT, and the Japanese government should come together to forge a high-standard, multilateral digital trade and

economy agreement. This multilateral agreement could be based upon existing bilateral agreements, including the US-Australia FTA, the 2019 US-Japan Digital Trade Agreement, and the digital-trade and e-commerce portions of recent multilateral agreements, including the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) and the Digital Economy Partnership Agreement. The allies should also borrow relevant parts of DEPA, which involves New Zealand, Singapore, Chile, and Canada and includes provisions on new and advanced technologies, including AI. Working together, the US and Australia could promote standards for data privacy that are consistent with democratic values. Such an effort would provide the United States with a leading role among like-minded countries in helping to shape the rules, standards, and norms of this critical and growing sector. Moreover, it would be a concrete immediate way for Washington to engage in the region on trade while simultaneously considering broader initiatives, such as rejoining an updated and revised CPTPP. As David Dollar and Jonathan Stromseth have suggested, an open-data agreement could provide a digital backdoor for the United States to re-engage with the eleven signatories of the CPTPP, even if further adjustments related to labor and environmental issues were required.<sup>228</sup>

A regional digital trade and economy agreement could complement the Quad's work on technology standards and norms at a critical time and provide an alternative trade governance model to the one emerging from China. Moreover, a civil backlash is currently underway in China against the mass collection of biometric data, including social credit scores and facial recognition technology.<sup>229</sup> Democracies coming together in setting a common, high standard to protect against unwanted surveillance could highlight the value of democracy and place pressure on Chinese authorities to listen to a greater degree to public concern in China. Tianjin passed the first legislation banning collection of biometric data from Chinese citizens earlier this year, and Guangdong Province and Dalian followed suit this year.<sup>230</sup>

### Recommendation #9: Hold an annual infrastructure summit in conjunction with Quad and other partners, thereby emphasizing digital economies and information power, and create a regional infrastructure hub in Southeast Asia.

Such a high-level forum of like-minded countries would boast multiple benefits. First, it could demonstrate democratic support for regional infrastructure, particularly that related to advanced digital economies.

Second, the forum would help revitalize and enlarge the effort begun in 2018 to conduct a US-Australia-Japan infrastructure forum. This Quad-plus infrastructure summit could pool resources to provide countries in Southeast Asia and the Indo-Pacific with alternatives to China's OBOR. A regional hub might allow the Quad (or Quad and other partner) countries to strengthen partnerships and increase collaboration among governments and the private sector.<sup>231</sup>

Third, holding this summit would provide an opportunity to reinforce the ability of democracies like the United States and Australia to push for higher standards. Moreover, as Michael Green and Evan Medeiros argue, China could be invited, because the summit's main point would be for the United States "to create and then drive a global conversation about the infrastructure that focuses on financing and debt sustainability, project, design, labor and environment rights, and multinational cooperation."<sup>232</sup>

Fourthly, the forum could help to provide alternatives to dependency on Huawei and other Chinese national champions seeking to dominate 5G telecommunications, primarily through the financing of relatively low-cost hardware. The Quad and other partners could also expand the range of available choices, including support for open radio access networks (ORANs) and whatever future technological developments eventually comprise 6G telecommunication. US and allied policymakers, meanwhile, should prioritize as an area of strategic competition cloud



infrastructure and services, in which the United States already has superior products to offer. A regional summit could also open up new opportunities by allowing trusted partner companies to provide more significant financial and technical support and combine services like cloud computing with related infrastructure.<sup>233</sup> The United States, Australia, Japan, and other democracies have already begun to move in this direction but require focused projects such as cloud computing to bring it to fruition. Although Chinese tech giant Huawei remains mostly a hardware provider, its inroads into software and services should not be underestimated; it is, for instance, currently seeking to expand into the growing cloud-computing market. In addition, it offers developing countries three serious inducements: 1) promises of major cost savings and lowered operating expenses; 2) a combination package of hardware and services; and 3) financing, albeit typically with one of China's two largest policy banks.<sup>234</sup>

Finally, a Quad-plus summit could enable like-minded countries to prioritize partner countries as economic partners in order to deny China near-exclusive economic dominance. But the key to accomplishing this goal is for the US and its allies to combine in offering third countries good alternatives to those offered by China and so to effectively compete with China in these countries, whether in infrastructure, training, education, or S&T relationships. The geoeconomics agenda adopted by the US, Australia, and other democracies should thus be designed to help other countries avoid falling into excessive dependence on China's economy by offering these countries a viable alternative. Indeed, the US needs to begin by helping Australia in this regard. As Ian Bremmer eloquently states in arguing for an enlightened way to confront China with the bedrock principle of competition: "Washington's overarching aim is to competitively coexist in as many third-party countries with China as possible to make sure none fall completely into China's orbit."<sup>235</sup>

## Security and Military Responses

The global economy hinges on the movement of goods at sea through vital maritime chokepoints and on the movement of

Internet data through submarine cables. Consequently, any US and Australian response to One Belt One Road and to China's economic policies should include the firm commitment to maintain freedom of the seas, in pursuit of which information plays a vital role, whether related to situational awareness or agreed-upon rules of the road.

For Beijing, China's geographical position poses natural challenges. The comparatively smaller expense involved in shipping as opposed to transport overland acts as an impediment to China's reducing its dependence on moving goods and resources through the Malacca Strait. Therefore, China is investing in naval power, ports, telecommunications infrastructure, and areas astride critical chokepoints.<sup>236</sup> Although some Chinese infrastructure projects may be undesirable, unsustainable, or fail to win the hearts and minds of the other societies they also affect, the allies need to remain vigilant for new investments by China in the South Pacific, Southeast Asia, and the Indian Ocean that would increase its access to critical military and national security data and information.

## Recommendation #10: Forge an Indo-Pacific Code of Conduct with like-minded countries to underscore customary international law and strengthen the ability of ASEAN to negotiate with China.

Negotiations regarding a Code of Conduct between the Association of Southeast Asian Nations (ASEAN) and China have been ongoing for a quarter of a century. China, however, seeks to impose its rules on its smaller neighbors, and it could exploit divisions within ASEAN and leverage the power associated with being these neighbors' top trade partner to block alternative rules of the road. However, it continues to mix inducements with maritime coercion, and its actions thereby alter the regional balance of power and facts on the ground. While China threads information throughout these efforts—including Chinese narratives asserting the destabilization caused by US freedom of navigation operations and China's maritime activities as providing for the common good—Canberra and Washington

could take the lead in working with Japan and other like-minded countries to create and formally announce adoption of a set of binding principles concerning maritime conduct. The agreement could allow international maritime partners to sign on, thereby boosting ASEAN efforts to negotiate a fair deal with China. The basic outline for an alternative Code of Conduct is readily available and could be adapted from a CSIS working group's informal and unofficial language.<sup>237</sup>

#### Recommendation #11: Draw up an allied plan of action for understanding the impact of increased deployment and integration of unmanned aerial vehicles.

The rapid advent of unmanned aerial vehicles (UAVs), or drones, requires concerted analysis of the threats and opportunities these pose within the Indo-Pacific region. Reliance on Chinese-made drones has become an obvious risk for democracies; deployment of drones has heightened deterrence concerns in hotspots; and reliance on UAVs could facilitate information-sharing among regional partners and allow development of new operational concepts.

UAVs, or drones, can contribute to establishment of a common operating picture for actors in the Indo-Pacific region, and a review of this operating picture could help in the creation of a blueprint for moving forward. For instance, having such a standard operating picture has enabled the Philippines and Vietnam to remain apprised of PLA and maritime militia operations in the South China Sea to a limited extent. Deployment of drones around narrow chokepoints and near disputed territory is beneficial. Japan recently accepted delivery from Guam of two US MQ-4C Triton unarmed surveillance drones that are to be based at Misawa. Unsurprisingly, Chinese analysts then warned that the use of UAVs, which could be used for “military pressure and political coercion,” could increase the “risk of miscalculation” by “Chinese vigilance forces.”<sup>238</sup> While this narrative is unlikely to be believed outside of China, it has undoubtedly fueled nationalist resentment within China.

#### Recommendation #12: Draw up an alliance plan of action to build partners' defense capacity against state or nonstate actor propaganda and disinformation.

Capacity building to defend against China's information operations and malign information power is a growing need. With oversight from the White House and Australia's Department of the Prime Minister and Cabinet, various elements of the two governments—including their defense, intelligence, and diplomatic arms—should implement efforts to enhance allied and partner capabilities to detect, deflect, and defend against disinformation, cyberattacks, and influence operations. The US Indo-Pacific Command and the Daniel K. Inouye Asia-Pacific Center for Security Studies, both located in Hawaii, could play vital roles in this effort, as also could US special operations forces. Toward this end, in recognition of the intensification of major-power information warfare—including the use of traditional media, social media, cyber operations, propaganda, and disinformation—the United States Special Operations Command has already announced the formation of an Indo-Pacific task force to ensure that competitors like China that flex information power do not get a “free pass” and to help allies and partners “recognize what is truth from fiction.”<sup>239</sup> SOCOM Commander General Richard Clarke stressed the continuing importance of “using our intel communities,” a statement also applicable to US-Australian relations.<sup>240</sup>

#### Recommendation #13: Create a defense-led but whole-of-government alliance red team to consider system-destruction warfare and scenarios centered on the possible breakdown of deterrence.

The defense departments of the United States and Australia should create a red team incorporating other government agencies and private sector actors whose purpose is to probe their own information-centric system weaknesses and the vulnerabilities of potential adversaries within this same area. Included could be cyber and space domains, undersea warfare, and chokepoint and SLOC security.

Tactically, conducting an ongoing red team exercise would highlight opportunities and risks. Operationally, deepening coordination of chokepoint control—where Australian, Japanese, and other allies’ submarines, which are ideal for the purpose, cover critical maritime chokepoints—is an increasingly important way to track the PLAN’s growing submarine forces as they attempt to leave shallow areas

near seas and reach the deeper waters outside the first island chain.<sup>241</sup>

Strategically, systematic due diligence could prevent the breakdown of deterrence and the advent of a strategic surprise, such as a transition from gray-zone activity to conventional force or even system-destruction warfare.

# ENDNOTES

- 1 Excerpted from President Joe Biden, “Remarks by President Biden in Press Conference” (East Room of the White House, March 25, 2021), <https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/03/25/remarks-by-president-biden-in-press-conference/>.
- 2 For instance, see Roger Garside, *China Coup: The Great Leap to Freedom* (Berkeley, CA: University of California Press, 2021). China is more focused on internal security than dealing with external threats—see the author interview available at the following URL, in which he notes, “There is no trust and no truth in China” (<https://www.ucpress.edu/blog/55984/watch-interview-with-roger-garside-author-of-china-coup/>).
- 3 In particular, see Patrick M. Cronin and Ryan Neuhard, *Total Competition: China’s Challenge in the South China Sea* (Washington, DC: Center for a New American Security, January 2020), <https://www.cnas.org/publications/reports/total-competition>.
- 4 The phrase is attributed to former Australian Foreign Minister Gareth Evans. See Ben Packham, “Politics Now: Beijing ‘Not Hell-Bent on Global Domination,’ Gareth Evans Says,” *The Australian*, May 5, 2021, <https://www.theaustralian.com.au/nation/politics/politicsnow-beijing-not-hellbent-on-global-domination-gareth-evans-says/news-story/90515e66419359d-92579d31089ab9f08>.
- 5 “Printing is called ‘a sacred art’ and also known as ‘the mother of civilization.’” Jialu Fan, Qi Han, Zhaochun Wang, and Nianzu Dai, “The Four Great Inventions,” in *A History of Chinese Science and Technology*, ed. Yongxiang Lu, vol. 2 (Shanghai: Shanghai Jiao Tong University Press and Berlin/Heidelberg: Springer, 2015), 195.
- 6 See Guiguzi, *China’s First Treatise on Rhetoric*, trans. Hui Wu, with commentaries by Hui Wu and C. Jan Swearingen (Carbondale, IL: Southern Illinois University Press, 2016).
- 7 See the discussion of Guiguzi, transliterated by Kuei Ku-tzu, in Dennis and Ching Ping Bloodworth, *The Chinese Machiavelli: 3,000 Years of Chinese Statecraft* (New York: Farrar, Straus and Giroux, 1976).
- 8 Confucius, *Analects: With Selections from Traditional Commentaries* 13.3, trans. Edward Slingerland (Indianapolis, IN: Hackett Publishing Company, Inc. 2003) 139-140.
- 9 Herrlee G. Creel, *Chinese Thought: From Confucius to Mao Tse-tung* (Chicago, IL: University of Chicago Press, 1953) 136.
- 10 Clive Hamilton and Mareike Ohlberg, *Hidden Hand: Exposing How the Chinese Communist Party is Reshaping the World* (London: Oneworld, 2020) 228.
- 11 “China’s Impact on the US Education System,” Staff Report, Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, United States Senate, February 28, 2019, <https://www.hsgac.senate.gov/imo/media/doc/PSI%20Report%20China’s%20Impact%20on%20the%20US%20Education%20System.pdf>.
- 12 An estimate made by David Shambaugh; see “China is Spending Billions to Make the World Love It,” *The Economist* March 23, 2017, <https://www.economist.com/china/2017/03/23/china-is-spending-billions-to-make-the-world-love-it>.
- 13 “How Many Confucius Institutes Are in the United States?” National Association of Scholars, May 18, 2021, [https://www.nas.org/blogs/article/how\\_many\\_confucius\\_institutes\\_are\\_in\\_the\\_united\\_states](https://www.nas.org/blogs/article/how_many_confucius_institutes_are_in_the_united_states).
- 14 Jeffrey Gil, “Can Confucius Institutes Survive on Australia’s University Campuses?” *The China Story*, November 19, 2020, <https://www.thechinastory.org/can-confucius-institutes-survive-on-australian-university-campuses/>.
- 15 Jamie P. Horsley, “It’s Time for a New Policy on Confucius Institutes,” *Lawfare*, April 1, 2021, <https://www.lawfareblog.com/its-time-new-policy-confucius-institutes>.
- 16 Gary Sands, “Are Confucius Institutes in the US Really Necessary?” *The Diplomat*, February 20, 2021, <https://thediplomat.com/2021/02/are-confucius-institutes-in-the-us-really-necessary/>.
- 17 Zhuang Pinghui, “China’s Confucius Institutes Rebrand After Overseas Propaganda Row,” *South China Morning Post*, July 4, 2020, <https://www.scmp.com/news/china/diplomacy/article/3091837/chinas-confucius-institutes-rebrand-after-overseas-propaganda>.
- 18 For instance, “China Releases Analects of Confucius Versions for Belt and Road Countries,” *Xinhua*, May 16, 2021, [http://www.xinhuanet.com/english/2021-05/16/c\\_139949240.htm](http://www.xinhuanet.com/english/2021-05/16/c_139949240.htm).
- 19 Hamilton and Ohlberg, *Hidden Hand*, 226.
- 20 Charlotte Gao, “What Does Qi Yu’s Surprising Appointment Mean for China’s Foreign Ministry?” *The Diplomat*, February 1, 2019, <https://thediplomat.com/2019/02/what-does-qi-yus-surprising-appointment-mean-for-chinas-foreign-ministry/>.
- 21 Chun Han Wong and Chao Dung, “China ‘Wolf Warrior’ Diplomats Are Ready to Fight,” *The Wall Street Journal*, May 19, 2019, [https://www.wsj.com/articles/chinas-wolf-warrior-diplomats-are-ready-to-fight-11589896722?mod=article\\_inline](https://www.wsj.com/articles/chinas-wolf-warrior-diplomats-are-ready-to-fight-11589896722?mod=article_inline).
- 22 Michael Auslin, “China’s New Realism in China,” *Foreign Policy*, July 7, 2020, <https://foreignpolicy.com/2020/07/07/trumps-new-realism-in-china/>.
- 23 Yuri Pines, “Legalism in Chinese Philosophy,” Stanford Encyclopedia of Philosophy, rev. November 16, 2018, <https://plato.stanford.edu/entries/chinese-legalism/>.
- 24 Yaoyao Dai and Luwei Rose Luqiu, “China’s ‘Wolf Warrior’ Diplomats Like to Talk Tough,” *The Washington Post*, May 12, 2021, <https://www.washingtonpost.com/politics/2021/05/12/chinas-wolf-warrior-diplomats-like-to-talk-tough/>.
- 25 Peter Martin, *China’s Civilian Army: The Making of Wolf Warrior Diplomacy* (New York: Oxford University Press, 2021) 10.

- 26 Adam Taylor, "Xi's Call for a 'Lovable' China May Not Tame the Wolf Warriors," *The Washington Post*, June 3, 2021, <https://www.washingtonpost.com/world/2021/06/03/china-wolf-warrior-reset/>.
- 27 "How to Spot a State-Funded Chinese Internet Troll," trans. David Wertime, *Foreign Policy*, 2015, <https://foreignpolicy.com/2015/06/17/how-to-spot-a-state-funded-chinese-internet-troll/>.
- 28 Gary King, Jennifer Pan, and Margaret E. Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument," *American Political Science Review* 111, no. 3 (2017): 484-501, [https://gking.harvard.edu/files/gking/files/how\\_the\\_chinese\\_government\\_fabricates\\_social\\_media\\_posts\\_for\\_strategic\\_distraction\\_not\\_engaged\\_argument.pdf](https://gking.harvard.edu/files/gking/files/how_the_chinese_government_fabricates_social_media_posts_for_strategic_distraction_not_engaged_argument.pdf).
- 29 *Deafening Whispers: China's Information Operation and Taiwan's 2020 Election* (Taipei: Doublethink Lab, May 2021), 6, <https://medium.com/doublethinklab/deafening-whispers-f9b1d773f6cd>.
- 30 With respect to these aims, there are parallels with the "information objectives" of China's intelligence activities. For instance, see Nicholas Eftimiades, *Chinese Intelligence Operations* (Reed Business Information, 1994), 24-26.
- 31 Prime Minister Malcolm Turnbull, "Speech Introducing the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017, December 7, 2017," <https://www.malcolmturbull.com.au/media/speech-introducing-the-national-security-legislation-amendment-espionage-an>.
- 32 Carolyn Kenney, Max Bergmann, and James Lemond, "Understanding and Combatting Russian and Chinese Influence Operations," Center for American Progress, February 28, 2019, <https://cdn.americanprogress.org/content/uploads/2019/02/26042755/RussiaChinaInfluence-brief-1.pdf>.
- 33 Kenney et al., "Understanding and Combatting."
- 34 Chris Uhlmann and Andrew Greene, "China-Australia Political Donations," ABC News, June 7, 2017, <https://www.abc.net.au/news/2016-08-21/china-australia-political-donations/7766654?nw=0>.
- 35 See "National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018, <https://www.legislation.gov.au/Details/C2018A00067>; and "Foreign Influence Transparency Scheme Act," <https://www.legislation.gov.au/Details/C2018A00063>.
- 36 "Melbourne Man Charged with Preparing Foreign Interference," Australian Federal Police, November 5, 2020; Yan Zhuang, "Australia Quiet on First Foreign-Meddling Arrest, But Target Is Clear," *The New York Times*, November 6 2020, <https://www.nytimes.com/2020/11/06/world/australia/australia-foreign-interference-law.html>; and Eliza Rugg, "Prosecution of First Personal Charged under Foreign Interference Laws Delayed," *9News*, April 6, 2021, <https://www.9news.com.au/national/prosecution-of-first-person-charged-under-foreign-interference-laws-delayed/ab4769bb-19b1-4fb7-8251-70d931958e33>.
- 37 Alex Joske, "Reorganizing the United Front Work Department: New Structures for a New Era of Diaspora and Religious Affairs Work," *China Brief* 19, issue 9 (May 9, 2019): 6-13, <https://jamestown.org/wp-content/uploads/2019/05/Read-the-05-09-2019-CB-Issue-in-PDF4.pdf?x13176>.
- 38 Anne-Marie Brady, "Resisting China's Magic Weapon," *The Interpreter*, September 27, 2017, <https://www.lowyinstitute.org/the-interpreter/resisting-china-s-magic-weapon>.
- 39 Marcel Angliviel de la Beaumelle, "The United Front Work Department: 'Magic Weapon' at Home and Abroad," *China Brief* 17, issue 9 (July 6, 2017), <https://jamestown.org/program/united-front-work-department-magic-weapon-home-abroad/>.
- 40 One pathbreaking documentary on China's influence operations in Australia first aired on ABC's Four Corners under the title "Power and Influence: The Hard Edge of China's Soft Power" on June 5, 2017. Although the program has been removed from the ABC website for "legal reasons" (<https://www.abc.net.au/4corners/power-and-influence-promo/8579844>), it can be viewed elsewhere (e.g., [https://www.youtube.com/watch?v=7T\\_Lu1S0sII](https://www.youtube.com/watch?v=7T_Lu1S0sII)).
- 41 Joske, "Reorganization the United Front Work Department."
- 42 Joske, "Reorganization the United Front Work Department."
- 43 David Murphy, "*Huayuquan*: Speak and Be Heard," chap. 4 in *Shared Destiny: China Story Yearbook 2014*, ed. Geremie R. Barmé, Linda Jaivin, and Jeremy Goldkorn (Canberra: ANU Press, 2015) 54.
- 44 See Elsa B. Kania, "The Ideological Battlefield: China's Approach to Political Warfare and Propaganda in an Age of Cyber of Conflict," in *Information Warfare in the Age of Cyber Conflict*, ed. Christopher Whyte, A. Trevor Thrall, and Brian M. Mazanec (London and New York: Routledge, 2021).
- 45 "Communiqué on the Current State of the Ideological Sphere: A Notice from the Central Committee of the Communist Party of China's General Office," April 22, 2013 republished as "Document 9: A ChinaFile Translation: How Much Is a Hardline Party Directive Shaping China's Current Political Climate?," ChinaFile, November 8, 2013, <https://www.chinafile.com/document-9-chinafile-translation>.
- 46 "Communiqué on the Current State of the Ideological Sphere."
- 47 Chris Buckley, "China Takes Aims at Western Ideas," *The New York Times*, August 19, 2013, [https://www.nytimes.com/2013/08/20/world/asia/chinas-new-leadership-takes-hardline-in-secret-memo.html?\\_r=0](https://www.nytimes.com/2013/08/20/world/asia/chinas-new-leadership-takes-hardline-in-secret-memo.html?_r=0).
- 48 For instance, Robert Lawrence Kuhn, a corporate strategist and adviser to the Chinese government, argued that Xi was protecting his left flank in advance of economic reforms: "Nobody can accuse him of being soft. He has totally buttoned up the entire left." Quoted in Simon Denyer, "China's Leader, Xi Jinping, Consolidates Power with Crackdowns on Corruption, Internet," *The Washington Post*, October 3, 2013, <https://www.washing->



tonpost.com/world/chinas-leader-xi-jinping-consolidates-power-with-crackdowns-on-corruption-internet/2013/10/01/fd-8ceeee-1eb7-11e3-9ad0-96244100e647\_story.html.

- 49 “Xi Jinping emphasized during his inspection in Guangxi to emancipate the mind and deepen the reforms, concentrating on hard work, building socialism with Chinese characteristics in a new era, and making Guangxi beautiful,” CCTV, April 27, 2021, [https://repositories.lib.utexas.edu/bitstream/handle/2152/73730/TNSR\\_Vol\\_2\\_Issue\\_1\\_Tobin.pdf?sequence=2&isAllowed=y](https://tv.cctv.com/2021/04/27/VIDEwhO6iXK6Ag3qt5WtFgLC210427.shtml?spm=C31267.PFskSaKh6QQC.S71105.3CCTV, April 27, 2021; translation by Bill Bishop, Sinocism.</a></li><li>50 Liza Tobin, “Xi’s Vision for Transforming Global Governance: A Strategic Challenge for Washington and Its Allies,” <i>Texas National Security Review</i> 2, issue 1 (November 2018): 155-66, <a href=).
- 51 For a longer discussion, see Patrick Cronin, “How to Asymmetrically Out-Compete Xi Jinping’s One Belt One Road Initiative,” *War on the Rocks*, March 2, 2021, <https://warontherocks.com/2021/03/how-to-asymmetrically-out-compete-xi-jinpings-one-belt-one-road-initiative/>.
- 52 See Eyck Freymann, *One Belt One Road: Chinese Power Meets the World* (Cambridge, MA: Harvard University Asia Center, 2021). Freymann notes that China uses OBOR domestically but markets OBOR abroad as the Belt and Road Initiative or BRI.
- 53 Thomas P. Cavanna, “Unlocking the Gates of Eurasia: China’s Belt and Road Initiative and Its Implications for US Grand Strategy,” *Texas National Security Review* 2, issue 3 (July 2019): 11-37, <https://tnsr.org/2019/07/unlocking-the-gates-of-eurasia-chinas-belt-and-road-initiative-and-its-implications-for-u-s-grand-strategy/>.
- 54 “President Xi Jinping Delivers Important Speech and Proposes to Build a Silk Road Economic Belt with Central Asian Countries,” Ministry of Foreign Affairs of the People’s Republic of China, September 7, 2013, [https://www.fmprc.gov.cn/mfa\\_eng/top-ics\\_665678/xjpfwzysiesgjthshzzfh\\_665686/t1076334.shtml](https://www.fmprc.gov.cn/mfa_eng/top-ics_665678/xjpfwzysiesgjthshzzfh_665686/t1076334.shtml).
- 55 State Councilor Yang Jiechi, “Jointly Built the 21st Century Maritime Silk Road By Deepening Mutual Trust and Enhancing Connectivity,” speech delivered at the Launching of the Year of China-ASEAN Maritime Cooperation, March 28, 2015, [https://www.fmprc.gov.cn/mfa\\_eng/zxxx\\_662805/t1249761.shtml](https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1249761.shtml).
- 56 Philip Ball, *The Water Kingdom: A Secret History of China* (Chicago: University of Chicago Press, 2016), 131.
- 57 Bruce Elleman, “The Cyclical Nature of Chinese Sea Power,” chap. 2 in *Strategy in Asia: The Past, Present, and Future of Regional Security*, ed. Thomas G. Mahnken & Dan Blumenthal (Stanford, CA: Stanford University Press, 2014), 30.
- 58 Xi announced the Polar Silk Road in January 2018; see, “China unveils vision for ‘Polar Silk Road’ across Arctic,” Reuters, January 26, 2018, <https://www.reuters.com/article/us-china-arctic/china-unveils-vision-for-polar-silk-road-across-arctic-idUSKB-N1FF0J8>. For a recent analysis of China’s Arctic ambitions, see Rush Doshi, Alexis Dale-Huang, and Gaoqi Zhang, “Northern Expedition: China’s Arctic Activities and Ambitions,” Brookings Institution, April 2021, <https://www.brookings.edu/research/northern-expedition-chinas-arctic-activities-and-ambitions/>.
- 59 Laura Zhou, “‘Let’s build a digital Silk Road’: Xi Jinping Looks to Cement China’s Ties with ASEAN,” *South China Morning Post*, November 27, 2020, <https://www.scmp.com/news/china/diplomacy/article/3111612/lets-build-digital-silk-road-president-xi-promises-ways-china>.
- 60 “China to Further Promote Space Cooperation for UN Sustainable Development,” *Xinhua*, April 24, 2019, [http://www.xinhuanet.com/english/2019-04/24/c\\_138005579.htm](http://www.xinhuanet.com/english/2019-04/24/c_138005579.htm); and Andrew Jones, “China Launches Beidou, Its Own Version of GPS,” *IEEE Spectrum*, August 12, 2020, <https://spectrum.ieee.org/tech-talk/aerospace/satellites/final-piece-of-chinas-beidou-navigation-satellite-system-comes-online>.
- 61 Jacob Mardell, “China’s ‘Health Silk Road’: Adapting the BRI to a Pandemic-Era World,” *Merics*, November 25, 2020, <https://merics.org/en/short-analysis/chinas-health-silk-road-adapting-bri-pandemic-era-world>; and Alice Han and Eyck Freymann, “Coronavirus Hasn’t Killed Belt and Road,” *Foreign Policy*, January 6, 2021, <https://foreignpolicy.com/2021/01/06/coronavirus-hasnt-killed-belt-and-road/>.
- 62 *China’s Belt and Road: Implications for the United States* (New York: Council on Foreign Relations, 2021), <https://www.cfr.org/report/chinas-belt-and-road-implications-for-the-united-states/>.
- 63 Brahma Chellaney, “Colonization by Other Means: China’s Debt-Trap Diplomacy,” *Japan Times*, May 9, 2021, <https://www.japan-times.co.jp/opinion/2021/05/09/commentary/world-commentary/china-debt-trap-development-aid/>.
- 64 Robert Potter, “Papua New Guinea and China’s Debt Squeeze,” *The Diplomat*, February 2, 2021, <https://thediplomat.com/2021/02/papua-new-guinea-and-chinas-debt-squeeze/>.
- 65 Anna Gelpern, S. Horn, S. Morris, B. Parks, and C. Trebesch, *How China Lends: A Rare Look into 100 Debt Contracts with Foreign Governments* (Williamsburg, VA: AidData, 2021), <https://docs.aiddata.org/reports/how-china-lends.html>.
- 66 Murray Hiebert, “China’s Belt and Road Finds Southeast Asia a Tough Slog,” *ISEAS Perspective*, (Issue 2020, no. 95, August 31, 2020), [https://www.iseas.edu.sg/wp-content/uploads/2020/08/ISEAS\\_Perspective\\_2020\\_95.pdf](https://www.iseas.edu.sg/wp-content/uploads/2020/08/ISEAS_Perspective_2020_95.pdf).
- 67 William Zheng, “China’s Officials Play up ‘Rise of the East, Decline of the West,’” *South China Morning Post*, March 9, 2021, <https://www.scmp.com/news/china/diplomacy/article/3124752/chinas-officials-play-rise-east-decline-west>.
- 68 Clive Cookson, “WHO and Global Leaders Could Have Averted Covid Calamity, Experts Say,” *Financial Times*, May 12, 2021, <https://www.ft.com/content/fb698a43-0f97-4142-9ff5-15dde66f-fae0>.

- 69 Seichiro Takeuchi, "China's Communist Party Risks Falling into Trap with Its Myth of Infallibility," *Yomiuri Shimbun*, April 13, 2020, <https://the-japan-news.com/news/article/0006484510>.
- 70 "US Official, NYT Continue to Mislead Americans over China," *Global Times*, February 14, 2021, <https://www.globaltimes.cn/page/202102/1215624.shtml>; and Michael R. Gordon, Warren P. Strobel, and Drew Hinshaw, "Intelligence on Sick Staff at Wuhan Lab Fuels Debate on Covid-19 Origin," *The Wall Street Journal*, May 23, 2021, <https://www.wsj.com/articles/intelligence-on-sick-staff-at-wuhan-lab-fuels-debate-on-covid-19-origin-11621796228?page=1>.
- 71 Brian Wong, "China's Mask Diplomacy," *The Diplomat*, March 25, 2020, <https://thediplomat.com/2020/03/chinas-mask-diplomacy/>.
- 72 Li Hong, "Trump Weirdly Shifts COVID-19 Blame to China," *Global Times*, October 8, 2020, <https://www.globaltimes.cn/content/1202924.shtml>.
- 73 Paul Karp and Helen Davidson, "China Bristles at Australia's Call for Investigation into Coronavirus Origin," *The Guardian*, April 29, 2020, <https://www.theguardian.com/world/2020/apr/29/australia-defends-plan-to-investigate-china-over-covid-19-outbreak-as-row-deepens>.
- 74 ABC, "Why is China Punishing Australia? The Human Impact of the Trade War," *Four Corners*, April 26, 2021, <https://www.youtube.com/watch?v=SShVYq5gQ2U>.
- 75 Huizhong Wu and Kristen Gelineau, "Chinese Vaccines Sweep Much of the World, Despite Concerns," Associated Press, March 2, 2021, <https://apnews.com/article/china-vaccines-world-wide-0382aefa52c75b834fbaf6d869808f51>; and Yanzhong Huang, "Vaccine Diplomacy is Paying Off for China," *Foreign Affairs*, March 11, 2021, <https://www.foreignaffairs.com/articles/china/2021-03-11/vaccine-diplomacy-paying-china>.
- 76 Qing Ming, "Still Indulging in Vaccine Supremacy, US Now Itches for Vaccine Diplomacy," *People's Daily Online*, May 9, 2021, <http://en.people.cn/n3/2021/0509/c90000-9847856.html>.
- 77 Louisa Lim, Julia Bergin and Johan Lidberg, *The Covid-19 Story: Unmasking China's Global Strategy*, International Federation of Journalists, May 12, 2021, 2; [https://www.ifj.org/fileadmin/user\\_upload/IFJ\\_-\\_The\\_Covid\\_Story\\_Report.pdf](https://www.ifj.org/fileadmin/user_upload/IFJ_-_The_Covid_Story_Report.pdf), <https://www.nytimes.com/2021/05/09/business/media/china-beijing-coronavirus-media.html>.
- 78 Lim et al., 2.
- 79 Lim et al., 5.
- 80 Ben Smith, "When Covid Hit, China Was Ready to Tell Its Sides of the Story," *The New York Times*, May 9, 2021.
- 81 "The Worshipping America and Kneeling America Soft-Bone Disease Must be Cured!," Xinhua, December 16, 2020, [http://www.xinhuanet.com/world/2020-12/16/c\\_1126869721.htm?mc\\_cid=a8895f4822&mc\\_eid=ef0502fbf0](http://www.xinhuanet.com/world/2020-12/16/c_1126869721.htm?mc_cid=a8895f4822&mc_eid=ef0502fbf0), translated by Bill Bishop, *Sinocism*, December 17, 2020.
- 82 Nadège Rolland, "China's Counteroffensive in the War of Ideas," *The Interpreter* (Lowy Institute, February 24, 2020), <https://www.lowyinstitute.org/the-interpreter/china-s-counteroffensive-war-ideas>.
- 83 Rolland.
- 84 Ben Smith, "When Covid Hit, China Was Ready to Tell Its Side of the Story," *The New York Times*, May 9, 2021, <https://www.nytimes.com/2021/05/09/business/media/china-beijing-coronavirus-media.html?smid=tw-share>.
- 85 "Ants in a Web: Deconstructing Guo Wengui's Online 'Whistleblower Movement'," *Graphika*, May 2021, [https://public-assets.graphika.com/reports/graphika\\_report\\_ants\\_in\\_a\\_web.pdf](https://public-assets.graphika.com/reports/graphika_report_ants_in_a_web.pdf).
- 86 "Declaration of the New Federal State of China," June 4, 2020, <https://s3.amazonaws.com/gnews-media-offload/wp-content/uploads/2020/06/03195945/【英文】Declaration-of-the-New-Federal-State-of-China.pdf>.
- 87 See Lee McIntyre, *Post-Truth* (Cambridge, MA: MIT Press, 2018).
- 88 "Ants in a Web," 4.
- 89 "Ants in a Web," 28.
- 90 "The Red Country Will Never Change Its Color," *Qiusi (Seeking Truth Magazine)*, May 15, 2021, [http://www.qstheory.cn/dukan/qqs/2021-05/15/c\\_1127446921.htm](http://www.qstheory.cn/dukan/qqs/2021-05/15/c_1127446921.htm).
- 91 James T. Areddy, "Digital Currency, a First for Major Economy," *The Wall Street Journal*, April 5, 2021, <https://www.wsj.com/articles/china-creates-its-own-digital-currency-a-first-for-major-economy-11617634118>; and Isabella Weber, "Why China Cracked Down on Bitcoin," *Fortune*, May 21, 2021, <https://fortune.com/2021/05/21/china-ban-bitcoin-price-bubble-crypto/>.
- 92 Ryan McMorrow and Sun Yu, "The Vanishing Billionaire: How Jack Ma Fell Foul of Xi Jinping: Alibaba Founder's Dramatic Rise and Fall Illustrates China's Wary Embrace of Tycoons Who Power Economic Growth," *Financial Times*, April 15, 2021, <https://www.ft.com/content/1fe0559f-de6d-490e-b312-abba0181da1f?segmentId=9abb79b8-254e-cfa3-594c-93c002aa043f>.
- 93 McMorrow and Yu.
- 94 McMorrow and Yu.
- 95 McMorrow and Yu.
- 96 Kendra Schaefer, head of digital research at Trivium China, quoted in "After Tech Crackdown, Xi Looking to Tap Chinese Firms' Wealth of Data," *The Japan Times*, April 23, 2021, <https://www.japantimes.co.jp/news/2021/04/23/business/china-big-data-crackdown/>.
- 97 Jack Nicas, Raymond Zhong, and Daisuke Wakabayashi, "Censorship, Surveillance and Profits: A Hard Bargain in China

- for Apple," *The New York Times*, May 17, 2021, <https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html?action=click&module=Well&pgtype=Homepage&section=Business>.
- 98 Nicas, Zhong, and Wakabayashi.
- 99 Nicas, Zhong, and Wakabayashi.
- 100 Diane Coyle, "The Dangers of Data-Based Certainty," *The Japan Times*, April 25, 2021, <https://www.japantimes.co.jp/opinion/2021/04/25/commentary/world-commentary/science-covid-19-artificial-intelligence-gdp-economics/>.
- 101 Judea Pearl and Dana Mackenzie, *The Book of Why: The New Science of Cause and Effect* (New York: Basic Books, 2018), ix, 6.
- 102 Pearl and Mackenzie, 24.
- 103 Pearl and Mackenzie, 11.
- 104 The public interest firm Anthropic is raising money based on its mission to "make sure that superintelligent AI systems do not...run amok and harm their makers." Richard Waters and Miles Kruppa, "Rebel AI Group Raises Record Cash after Machine Learning Schism," *Financial Times*, May 28, 2021, <https://www.ft.com/content/8de92f3a-228e-4bb8-961f-96f2dce70ebb>.
- 105 Waters and Kruppa, ix.
- 106 Simon Benson, "Record \$1.3bn boost for ASIO's war on spies and hackers" *The Weekend Australian*, May 15, 2021, <https://www.theaustralian.com.au/nation/politics/record-13bn-boost-for-asios-war-on-spies-and-hackers/news-story/7eba87f41b80c0c89ca87513e2a6fe08>.
- 107 David Meyer, "Vladimir Putin Says Whoever Leads in Artificial Intelligence Will Rule the World," *Fortune*, September 4, 2017, <https://fortune.com/2017/09/04/ai-artificial-intelligence-putin-rule-world/>.
- 108 Xie Yu and Meng Jing, "China Aims to Outspend the World in Artificial Intelligence, and Xi Jinping Just Green Lit the Plan," *South China Morning Post*, October 18, 2017, <https://www.scmp.com/business/china-business/article/2115935/chinas-xi-jinping-highlights-ai-big-data-and-shared-economy>.
- 109 Ian Burrows, "Made in China 2025: Xi Jinping's Plan to Turn China into the AI World Leader," ABC News, October 5, 2018, <https://www.abc.net.au/news/2018-10-06/china-plans-to-become-ai-world-leader/10332614>.
- 110 Gregory C. Allen, *Understanding China's AI Strategy*, February 6, 2019, Center for a New American Security, <https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy>.
- 111 *National Security Commission on Artificial Intelligence Final Report*, March 2021, 4, <https://www.nsc.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf>.
- 112 Craig A. Dudley, "Lessons from SABLE SPEAR: The Application of an Artificial Intelligence Methodology in the Business of Intelligence," extract, *Studies in Intelligence* 65, no. 1 (March 2021):12-14.
- 113 Dudley.
- 114 See Elsa B. Kania, "Chinese Military Innovation in Artificial Intelligence," (testimony before the US-China Economic and Security Review Commission Hearing on Trade, Technology, and Military-Civil Fusion, Center for a New American Security, June 7, 2019), [https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/June-7-Hearing\\_Panel-1\\_Elsa-Kania\\_Chinese-Military-Innovation-in-Artificial-Intelligence.pdf?mtime=20190617115242&focal=none](https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/June-7-Hearing_Panel-1_Elsa-Kania_Chinese-Military-Innovation-in-Artificial-Intelligence.pdf?mtime=20190617115242&focal=none).
- 115 *NSCAI Final Report*, 77, <https://www.nsc.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf>.
- 116 Matt O'Brien, "Gov't Use of Chinese Drones in Limbo as Congress Weighs Ban," Associated Press, June 1, 2021, <https://apnews.com/article/donald-trump-technology-government-and-politics-business-5854cf8b5eccd03f85d5eba2aef10a22>.
- 117 David Shepardson, "DHS Warns of Data Threat from Chinese-Made Drones," Reuters, May 20, 2019, [https://www.reuters.com/article/us-usa-drones-china/dhs-warns-of-data-threat-from-chinese-made-drones-idUSKCN1SQ1ZY?feed-Type=RSS&feedName=technologyNews&utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed%3A+reuters%2FtechnologyNews+%28Reuters+Technology+News%29](https://www.reuters.com/article/us-usa-drones-china/dhs-warns-of-data-threat-from-chinese-made-drones-idUSKCN1SQ1ZY?feed-Type=RSS&feedName=technologyNews&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+reuters%2FtechnologyNews+%28Reuters+Technology+News%29).
- 118 Jeanne Whalen and Ellen Nakashima, "US Bans Technology Exports to Chinese Semiconductor and Drone Companies, Calling Them Security Threats," *Washington Post*, December 18, 2020, <https://www.washingtonpost.com/technology/2020/12/18/china-smic-entity-list-ban/>.
- 119 "Japan Coast Guard to 'Eliminate' Chinese Drones," *Nikkei Asia*, December 9, 2020, <https://asia.nikkei.com/Politics/International-relations/Japan-Coast-Guard-to-eliminate-Chinese-drones>.
- 120 Gen Nakamura, Risa Kawaba, and Kiu Sugano, "Japanese Companies Ditch Chinese Drones over Security Concerns," *Nikkei Asia*, May 4, 2021, <https://asia.nikkei.com/Business/Technology/Japanese-companies-ditch-Chinese-drones-over-security-concerns>.
- 121 Murray Scott Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," *Lawfare*, July 20, 2017, <https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense>.
- 122 Jude Blanchette, "Confronting the Challenge of Chinese State Capitalism," January 22, 2021, <https://www.csis.org/analysis/confronting-challenge-chinese-state-capitalism>.
- 123 For instance, see Tom Gjelten, "US Turns up the Heat on Costly Commercial Cyber Theft in China," National Public Radio, May 7, 2013, <https://www.npr.org/2013/05/07/181668369/u-s-turns-up-heat-on-costly-commercial-cyber-theft-in-china>.

- 124 *Update to the IP Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy* (National Bureau of Asian Research, February 2017), [https://www.nbr.org/wp-content/uploads/pdfs/publications/IP\\_Commission\\_Report\\_Update.pdf](https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report_Update.pdf).
- 125 *Foreign Economic Espionage in Cyberspace* (Washington, DC: National Counterintelligence and Security Center, 2018), 7; <https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf>.
- 126 *Foreign Economic Espionage in Cyberspace*, 5.
- 127 *Foreign Economic Espionage in Cyberspace*, 6. Chart is from the ODNI 2018 report.
- 128 Michael Adams, "Why the OPM Hack is Far Worse Than You Imagine," *Lawfare*, March 11, 2016, <https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine>.
- 129 Devlin Barrett, "Chinese National Arrested for Using Malware Linked to OPM Hack," *The Washington Post*, August 24, 2017, [https://www.washingtonpost.com/world/national-security/chinese-national-arrested-for-using-malware-linked-to-opm-hack/2017/08/24/746cbdc2-8931-11e7-a50f-e0d4e6ec070a\\_story.html](https://www.washingtonpost.com/world/national-security/chinese-national-arrested-for-using-malware-linked-to-opm-hack/2017/08/24/746cbdc2-8931-11e7-a50f-e0d4e6ec070a_story.html).
- 130 Byron Tau, "The Ease of Tracking Mobile Phones of US Soldiers in Hot Spots," *Wall Street Journal*, April 26, 2021, <https://www.wsj.com/articles/the-ease-of-tracking-mobile-phones-of-u-s-soldiers-in-hot-spots-11619429402?page=1>.
- 131 Alex Joske, *Picking Flowers, Making Honey: The Chinese Military's Collaboration with Foreign Universities* (Canberra: ASPI, October 30, 2018), <https://www.aspi.org.au/report/picking-flowers-making-honey>.
- 132 Ibid.
- 133 Alex Joske, *The China Defence Universities Tracker* (Canberra: Australian Strategic Policy Institute, November 25, 2019), <https://www.aspi.org.au/report/china-defence-universities-tracker>.
- 134 Ryan Fedasiuk and Emily Weinstein, *Universities and the Chinese Defense Technology Workforce* (Washington, DC: Center for Security and Emerging Technology, Georgetown University, December 2020), 3-4, <https://cset.georgetown.edu/wp-content/uploads/CSET-Universities-and-the-Chinese-Defense-Technology-Workforce.pdf>.
- 135 Radomir Tylecote and Robert Clark, *Inadvertently Arming China? The Chinese Military Complex and Its Potential Exploitation of Scientific Research at UK Universities* (London: Civitas, revised February 24, 2021), <https://www.civitas.org.uk/content/files/ChinaReport.pdf>.
- 136 For a useful synopsis, see "'Made in China 2025' Industrial Policies: Issues for Congress," Congressional Research Service, August 11, 2020, <https://fas.org/sgp/crs/row/IF10964.pdf>.
- 137 "'Made in China 2025' Industrial Policies: Issues for Congress."
- 138 Zhou Xin and Choi Chi-yuk, "Develop and Control: Xi Jinping Urges China to Use Artificial Intelligence in Race for Tech Future," *South China Morning Post*, October 31, 2018, <https://www.scmp.com/economy/china-economy/article/2171102/develop-and-control-xi-jinping-urges-china-use-artificial>.
- 139 "Asia Speeds Up Inclusive 5G, but Washington Poses Risk," *Global Times*, April 12, 2021, <https://www.globaltimes.cn/page/202104/1220858.shtml>; and Brian Fund, "How China's Huawei Took the Lead over US Companies in 5G," *The Washington Post*, April 10, 2019, <https://www.washingtonpost.com/technology/2019/04/10/us-spat-with-huawei-explained/>.
- 140 Yusho Cho, "China's Progress in Advanced Semiconductor Technology Slows," *Nikkei Asia*, May 9, 2021, <https://asia.nikkei.com/Business/Tech/Semiconductors/China-s-progress-in-advanced-semiconductor-technology-slows>.
- 141 Elsa B. Kania and Lorand Laskai, "Myths and Realities of China's Military-Civil Fusion Strategy (Washington, D.C.: Center for a New American Security, January 28, 2021), [https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Myths-and-Realities-of-China's-Military-Civil-Fusion-Strategy\\_FINAL-min.pdf?mtime=20210127133521&focal=none](https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Myths-and-Realities-of-China's-Military-Civil-Fusion-Strategy_FINAL-min.pdf?mtime=20210127133521&focal=none).
- 142 Xi Jinping quoted in Zhang Xiaosong and Zhu Jiwei, "Xi Jinping: Independent Innovation to Promote the Construction of Network Power," *Ashining*, June 21, 2018, <http://en.ashining.com/detail/336.html>. Xi Jinping was giving a speech to the National Conference on Cyber Security and Informatization, held April 20-21, 2018. Originally published in *Xinhua*, April 21, 2018, it was then republished on the Ashining website.
- 143 Xi Jinping.
- 144 "Xi Jinping: The Full Text of Speech at the Forum on Cybersecurity and Informatization Work" *China Copyright and Media* (English translation April 19, 2016), <https://chinacopyrightandmedia.wordpress.com/2016/04/19/speech-at-the-work-conference-for-cybersecurity-and-informatization/>.
- 145 Jinping, <https://chinacopyrightandmedia.wordpress.com/2016/04/19/speech-at-the-work-conference-for-cybersecurity-and-informatization/>.
- 146 For instance, see Lorand Laskai, "Civil-Military Fusion: The Missing Link Between China's Technological and Military Rise," *Council on Foreign Relations* (blog), January 29, 2018, <https://www.cfr.org/blog/civil-military-fusion-missing-link-between-chinas-technological-and-military-rise>.
- 147 Wang Cong, Cao Siqi, and Chen Qingqing, "China Sets 'Pragmatic' Targets Through 2035," *Global Times*, October 29, 2020, <https://www.globaltimes.cn/content/1205131.shtml>.
- 148 Bob Savic, "China's Vision 2035: From Beijing's Forbidden City to Interconnected Eurasian Megacity," *China Briefing*, March 24, 2021, <https://www.china-briefing.com/news/chinas-vi>



- sion-2035-from-beijings-forbidden-city-to-interconnected-eurasian-megacity/.
- 149 Savic, <https://www.china-briefing.com/news/chinas-vision-2035-from-beijings-forbidden-city-to-interconnected-eurasian-megacity/>.
  - 150 John Seaman, *China and the New Geopolitics of Technical Standardization* (Paris: Institut Français Relations des Internationales, January 2020), [https://www.ifri.org/sites/default/files/atoms/files/seaman\\_china\\_standardization\\_2020.pdf](https://www.ifri.org/sites/default/files/atoms/files/seaman_china_standardization_2020.pdf).
  - 151 Scott Bade, "Is Washington Prepared for a Geopolitical 'Tech Race?'" *TechCrunch*, May 1, 2021, <https://techcrunch.com/2021/05/01/is-washington-prepared-for-a-geopolitical-tech-race/>.
  - 152 Tianjie Ma, "Belt and Road Initiative in the 14th Five-Year Plan: An Explainer," *Panda Paw Dragon Claw*, April 13, 2021, <https://pandapawdragonclaw.blog/2021/04/13/belt-and-road-initiative-in-the-14th-five-year-plan-an-explainer/>.
  - 153 Ma, <https://pandapawdragonclaw.blog/2021/04/13/belt-and-road-initiative-in-the-14th-five-year-plan-an-explainer/>.
  - 154 Ma, <https://pandapawdragonclaw.blog/2021/04/13/belt-and-road-initiative-in-the-14th-five-year-plan-an-explainer/>.
  - 155 Stu Woo, "In the Race to Dominate 5G, China Sprints Ahead," *The Wall Street Journal*, September 7, 2019, <https://www.wsj.com/articles/in-the-race-to-dominate-5g-china-has-an-edge-11567828888>.
  - 156 Joshua Kurlantzick, "China's Digital Silk Road Initiative: A Boon to Developing Countries or a Threat to Freedom?" *The Diplomat*, December 17, 2020, <https://thediplomat.com/2020/12/chinas-digital-silk-road-initiative-a-boon-for-developing-countries-or-a-danger-to-freedom/>.
  - 157 Paul Mozur, "Beijing Wants A.I. to be Made in China by 2030," *The New York Times*, July 20, 2017, <https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html>.
  - 158 Dorothy E. Denning, "Is Quantum Computing a Cybersecurity Threat?" *American Scientist*, March-April 2019, <https://www.americanscientist.org/article/is-quantum-computing-a-cybersecurity-threat>.
  - 159 Tom Stefanick, "The State of US-China Quantum Data Security Competition," *Brookings Tech*, September 18, 2020, <https://www.brookings.edu/techstream/the-state-of-u-s-china-quantum-data-security-competition/>; and Ali El Kaafarani, "Why Quantum Computers Pose a Very Real Risk to Cyber Security," *Info Security*, March 10, 2021, <https://www.infosecurity-magazine.com/blogs/quantum-computers-risk/>.
  - 160 Gavin Brennen Simon Devitt, Tara Roberson, and Peter Rohde, *An Australian Strategy for the Quantum Revolution*, Policy Brief Report 43 (Canberra: Australian Strategic Policy Institute, May 2021), 3; <https://www.aspi.org.au/report/australian-strategy-quantum-revolution>.
  - 161 "Remarks by President Biden Press Conference," The White House, March 25, 2021, <https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/03/25/remarks-by-president-biden-in-press-conference/>.
  - 162 "China to Include Quantum Technology in its 14th Five-Year Plan," PRC State Council, October 22, 2020, [http://english.www.gov.cn/news/videos/202010/22/content\\_WS5f90e700c6d0f7257693e3fe.html](http://english.www.gov.cn/news/videos/202010/22/content_WS5f90e700c6d0f7257693e3fe.html).
  - 163 Brad Smith and Carol Ann Browne, *Tools and Weapons: The Promise and the Peril of the Digital Age* (New York: Penguin Press, 2019), 252-253.
  - 164 For example, see Nicholas Fern, "Can the UK Develop a 5G Giant to Take on Huawei," *ITPro*, July 17, 2020, <https://www.itpro.com/mobile/5g/356479/can-the-uk-develop-a-5g-giant-to-take-on-huawei>; and Tyson Barker, "Europe Can't Win the Tech War It Just Started," *Foreign Policy*, January 16, 2020, <https://foreignpolicy.com/2020/01/16/europe-technology-sovereignty-von-der-leyen/>.
  - 165 Keumars Afifi-Sebet, "The West Faces 'A moment of Reckoning' in Technology and Cyber Security," *ITPro*, April 23, 2021, <https://www.itpro.co.uk/security/cyber-security/359317/the-west-faces-a-moment-of-reckoning-in-technology-and-cyber>.
  - 166 Xi Jinping, "Uphold and Develop Socialism with Chinese Characteristics," Tanner Greer (trans.), [palladiummag.com/2019/05/31/xi-jinping-in-translation-chinas-guiding-ideology/](https://palladiummag.com/2019/05/31/xi-jinping-in-translation-chinas-guiding-ideology/); quoted in Daniel Tobin, "How Xi Jinping's 'New Era' Should Have Ended Debate on Beijing's Ambitions," *CSIS*, May 2020, 12-13, [https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200508\\_Tobin\\_NewEra\\_v4%5B2%5D.pdf?nnVQusek-8pUo8vt9YGwAW9B6E\\_itLPV6](https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200508_Tobin_NewEra_v4%5B2%5D.pdf?nnVQusek-8pUo8vt9YGwAW9B6E_itLPV6).
  - 167 Matthew D. Johnson, "Safeguarding Socialism: The Origins, Evolution, and Expansion of China's Total Security Paradigm," *Sinopsis*, June 16, 2020, <https://sinopsis.cz/wp-content/uploads/2020/06/safeguarding-socialism.pdf>.
  - 168 Xi Jinping, "Explanatory Notes for the 'Decision of the Central Committee of the Communist Party of China on Some Major Issues Concerning Comprehensively Deepening the Reform,'" *China.org.cn*, January 16, 2014, [http://www.china.org.cn/china/third\\_plenary\\_session/2014-01/16/content\\_31210122.htm](http://www.china.org.cn/china/third_plenary_session/2014-01/16/content_31210122.htm). The notes were originally delivered on November 16, 2013.
  - 169 Jinping, "Explanatory Notes," [http://www.china.org.cn/china/third\\_plenary\\_session/2014-01/16/content\\_31210122.htm](http://www.china.org.cn/china/third_plenary_session/2014-01/16/content_31210122.htm).
  - 170 Jinping, "Explanatory Notes," [http://www.china.org.cn/china/third\\_plenary\\_session/2014-01/16/content\\_31210122.htm](http://www.china.org.cn/china/third_plenary_session/2014-01/16/content_31210122.htm). Italics added for emphasis.
  - 171 Johnson, "Safeguarding Socialism," 3, <https://sinopsis.cz/wp-content/uploads/2020/06/safeguarding-socialism.pdf>.
  - 172 Johnson, "Safeguarding Socialism," 3, <https://sinopsis.cz/wp-content/uploads/2020/06/safeguarding-socialism.pdf>.



- 173 Ryan Fedasiuk, "A Different Kind of Army: The Militarization of China's Internet Trolls," *China Brief* 21, issue 7, April 12, 2021, <https://jamestown.org/program/a-different-kind-of-army-the-militarization-of-chinas-internet-trolls/>.
- 174 Katsuji Nakazawa, "Analysis: China's 'Wolf Warriors' Take Aim at G-7," *Nikkei Asia*, May 13, 2021, <https://asia.nikkei.com/Editor-s-Picks/China-up-close/Analysis-China-s-wolf-warriors-take-aim-at-G-7>.
- 175 "US Embassy Increasingly Offensive in Pushing 'Peaceful Evolution' in China by Roping in Activists with Money," *Global Times*, May 16, 2021, <https://www.globaltimes.cn/page/202105/1223614.shtml>.
- 176 "US Embassy Increasingly Offensive," <https://www.globaltimes.cn/page/202105/1223614.shtml>.
- 177 Peter Mattis and Matthew Brazil, *Chinese Communist Espionage: An Intelligence Primer* (Annapolis, MD: Naval Institute Press, 2019), 17-18.
- 178 Mattis and Brazil, 18.
- 179 Dorothy Denning, "Cyberwar: How Chinese Hackers Became a Major Threat to the US," *Newsweek*, October, 5, 2017, <https://www.newsweek.com/chinese-hackers-cyberwar-us-cybersecurity-threat-678378>.
- 180 For instance, see *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* (Washington, D.C.: Office of the Secretary of Defense 2020), 139-140, <https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF>.
- 181 See various posts on the Asia Maritime Transparency Initiative (AMTI) website, including "Signaling Sovereignty: Chinese Patrols at Contested Reefs," Asia Maritime Transparency Initiative, September 26, 2019, <https://amti.csis.org/signaling-sovereignty-chinese-patrols-at-contested-reefs/>.
- 182 For instance, see J. Michael Dahn, *Undersea Fiber-Optic Cable and Satellite Communications* (Laurel, MD: Johns Hopkins Applied Physics Laboratory, 2020), <https://www.jhuapl.edu/Content/documents/UnderseaFiber-OpticCableandSATCOM.pdf>.
- 183 See Jean-Pierre Cabestan, "China's Djibouti Naval Base Increasing Its Power," *East Asia Forum*, May 16, 2020, <https://www.eastasiaforum.org/2020/05/16/chinas-djibouti-naval-base-increasing-its-power/>; Celine Castronuovo, "US General Warns China is Actively Seeking to Set Up an Atlantic Naval Base," *The Hill*, May 7, 2021, <https://thehill.com/policy/defense/552331-us-general-warns-china-is-actively-seeking-to-set-up-an-atlantic-naval-base>; Chen Heang, "Would Access to Cambodia's Ream Naval Base Really Benefit China?," *The Diplomat*, April 7, 2021, <https://thediplomat.com/2021/04/would-access-to-cambodia-as-ream-naval-base-really-benefit-china/>; Jonathan Pyke, "The Risks of China's Ambitions in the South Pacific," *Brookings*, July 20, 2020, <https://www.brookings.edu/articles/the-risks-of-chinas-ambitions-in-the-south-pacific/>; and Fumi Matsumoto, "China Extends South Pacific Reach by Funding Runway Project," *Nikkei Asia*, May 19, 2021, <https://asia.nikkei.com/Politics/International-relations/Indo-Pacific/China-extends-South-Pacific-reach-by-funding-runway-project>.
- 184 David Lague and Benjamin Kang Lim, "The China Challenge: Ruling the Waves," *Reuters*, April 30, 2019, <https://www.reuters.com/investigates/special-report/china-army-navy/>; and Patrick M. Cronin, "China's Bid for Maritime Primacy in an Era of Total Competition," Center for International Maritime Security, March 2, 2020, <https://cimsec.org/chinas-bid-for-maritime-primacy-in-an-era-of-total-competition/>.
- 185 Demetri Sevastopulo, "Admiral Warns US Losing Its Edge in Indo-Pacific," *Financial Times*, March 9, 2021, <https://www.ft.com/content/61ea7ce5-7b68-459b-9a11-41cc71777de5>.
- 186 Demetri Sevastopulo, slides, <https://d1e00ek4ebabms.cloudfront.net/production/uploaded-files/Appendix%201%20to%20CDRUSINDOPACOM%20Sec.%201251%20Indendent%20Assessment%20-%20Executive%20Summary%20-%2027%20Feb%202021-c22ba69c-4e88-4d8d-90d0-1885b2589e20.pdf>.
- 187 Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (Santa Monica, CA: RAND, 2018), [https://www.rand.org/pubs/research\\_reports/RR1708.html](https://www.rand.org/pubs/research_reports/RR1708.html).
- 188 Engstrom, iii.
- 189 Hal Brands and Charles Edel, "A Grand Strategy of Democratic Solidarity," *The Washington Quarterly* 44, no. 1 (March 23, 2021): 29-47, <https://doi.org/10.1080/0163660X.2021.1893003>.
- 190 Brands and Edel, 29.
- 191 Brands and Edel, 30.
- 192 Prime Minister Scott Morrison, "Address to the 6th Raisina Dialogue," April 15, 2021, <https://www.pm.gov.au/media/address-6th-raisina-dialogue>.
- 193 Morrison.
- 194 Morrison.
- 195 President Joe Biden, "Remarks by President Biden Address to a Joint Session of Congress," US Capitol, April 28, 2021, <https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/04/29/remarks-by-president-biden-in-address-to-a-joint-session-of-congress/>.
- 196 Biden, <https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/04/29/remarks-by-president-biden-in-address-to-a-joint-session-of-congress/>.
- 197 Biden, <https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/04/29/remarks-by-president-biden-in-address-to-a-joint-session-of-congress/>.

- 198 Brand and Edel, 30-31, <https://doi.org/10.1080/0163660X.2021.1893003>.
- 199 Brand and Edel, 30-31.
- 200 "Amphibious Exercise ARC 21 Underway with Australia, France, Japan, United States," *Naval News*, May 16, 2021, <https://www.navalnews.com/naval-news/2021/05/amphibious-exercise-arc-21-underway-with-australia-france-japan-united-states/>.
- 201 "Amphibious Exercise," 33-34.
- 202 "Fact Sheet: Quad Summit," White House, March 12, 2021, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/12/fact-sheet-quad-summit/>.
- 203 Secretary Anthony J. Blinken, "Secretary Anthony J. Blinken and Australian Foreign Minister and Minister for Women Marise Payne at a Joint Press Availability," US Department of State (website), May 13, 2021, <https://www.state.gov/secretary-antony-j-blinken-and-australian-foreign-minister-and-minister-for-women-marise-payne-at-a-joint-press-availability/>.
- 204 Gordon Lubold and Alex Leary, "Biden Expands Blacklist of Chinese Companies Banned from US Investment," *The Wall Street Journal*, June 3, 2021, <https://www.wsj.com/articles/biden-expands-blacklist-of-chinese-companies-banned-from-u-s-investment-11622741711?page=1>.
- 205 See Peter Hartcher, *Red Zone: China's Challenge and Australia's Future* (Carlton VIC, Australia: Black Inc., 2021), 22-23.
- 206 Matt Perault and Sam Sacks, "A Sharper, Shrewder US Policy for Chinese Tech Firms," *Foreign Affairs*, February 19, 2021, <https://www.foreignaffairs.com/articles/unit-ed-states/2021-02-19/sharper-shrewder-us-policy-chinese-tech-firms>.
- 207 See the draft of the "Endless Frontiers Act" (<https://www.congress.gov/bill/116th-congress/senate-bill/3832>), as well as the text of the bipartisan "Democracy Technology Partnership Act": [https://www.warner.senate.gov/public/\\_cache/files/8/9/895e0a40-65ee-43cc-8629-450555faefe7/AC6A0E54D-B992E1612161C48BB34FC57.democracy-technology-partnership-act-two-pager-explainer.pdf](https://www.warner.senate.gov/public/_cache/files/8/9/895e0a40-65ee-43cc-8629-450555faefe7/AC6A0E54D-B992E1612161C48BB34FC57.democracy-technology-partnership-act-two-pager-explainer.pdf).
- 208 John D. McKinnon, "Senate Approves \$250 Bill to Boost Tech Research," *The Wall Street Journal*, June 8, 2021, <https://www.wsj.com/articles/senate-approves-250-billion-bill-to-boost-tech-research-11623192584?page=1>.
- 209 *IP Commission 2021 Review, Updated Recommendations*, (Seattle: National Bureau of Asian Research, March 2021), [https://www.nbr.org/wp-content/uploads/pdfs/publications/ip\\_commission\\_2021\\_recommendations\\_mar2021.pdf](https://www.nbr.org/wp-content/uploads/pdfs/publications/ip_commission_2021_recommendations_mar2021.pdf).
- 210 "IP Commission Background Memo," National Bureau of Asian Research, March 2021, [https://www.nbr.org/wp-content/uploads/pdfs/publications/ip\\_commission\\_2021\\_background\\_memo\\_mar21.pdf](https://www.nbr.org/wp-content/uploads/pdfs/publications/ip_commission_2021_background_memo_mar21.pdf).
- 211 Quoted in Peter Hartcher, *Red Zone: China's Challenge and Australia's Future*, 9.
- 212 CSSA-Chinese Student and Scholar Association at George Washington University, LinkedIn, <https://www.linkedin.com/company/cssa-at-gwu/about/>.
- 213 Bethany Allen-Ebrahimian, "China's Long Arm Reaches into American Campuses," *Foreign Policy*, March 7, 2018, <https://foreignpolicy.com/2018/03/07/chinas-long-arm-reaches-into-american-campuses-chinese-students-scholars-association-university-communist-party/>.
- 214 Elizabeth Redden, "The Chinese Student Threat?," *Inside HigherEd*, February 15, 2018, <https://www.insidehighered.com/news/2018/02/15/fbi-director-testifies-chinese-students-and-intelligence-threats>.
- 215 Erin Doherty and Will Cassou, "Student Advocates Call for University Support in Response to Anti-China Rhetoric," *The Hoya*, February 23, 2018, <https://thehoya.com/student-advocates-call-university-support-response-anti-china-rhetoric/>.
- 216 See Taehwa Hong, "Collectively Countering China's Influence Operations," *Asia Times*, February 6, 2021, <https://asiatimes.com/2021/02/collectively-countering-chinas-influence-operations/>.
- 217 Lyle J. Morris et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War* (Santa Monica, CA: RAND Corporation, 2019), [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR2900/RR2942/RAND\\_RR2942.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2942/RAND_RR2942.pdf).
- 218 See the bipartisan Senate legislation known as the "Endless Frontiers Act," which is currently under discussion in Congress: <https://www.congress.gov/bill/116th-congress/senate-bill/3832>.
- 219 Ferial Ara Saeed, "The Sino-American Race for Technology Leadership," *War on the Rocks*, April 23, 2021, <https://warontherocks.com/2021/04/the-sino-american-race-for-technology-leadership/>.
- 220 Saeed.
- 221 *2020 Human Rights Country Reports on Human Rights Practices* (Washington, D.C.: Department of State, March 30, 2021), <https://www.state.gov/reports/2020-country-reports-on-human-rights-practices/>.
- 222 *2020 Human Rights Country Reports*; and Bureau of Democracy, Human Rights, and Labor, *2020 Country Reports on Human Rights Practices: China (Includes Hong Kong, Macau, and Tibet)*, (Washington, DC: US Department of State, revised mid-2021), <https://www.state.gov/reports/2020-country-reports-on-human-rights-practices/china/>.
- 223 "Global Engagement Center," US Department of State, <https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/>.

- 224 "National Counter Foreign Influence Coordinator," Australian Government Department of Home Affairs, <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/cfi-coordinator>.
- 225 Cronin, "How to Asymmetrically Out-Compete Xi Jinping's One Belt One Road Initiative," <https://warontherocks.com/2021/03/how-to-asymmetrically-out-compete-xi-jinpings-one-belt-one-road-initiative/>.
- 226 For instance, see Lucas Irwin, "One Thousand and One Talents: The Race for AI Dominance," *JustSecurity*, April 7, 2021, <https://www.justsecurity.org/75474/one-thousand-and-one-talents-the-race-for-a-i-dominance/>.
- 227 Philip Citowicki, "Integrating Japan into an Expanded 'Five Eyes' Alliance," *The Diplomat*, April 22, 2021, <https://thediplomat.com/2021/04/integrating-japan-into-an-expanded-five-eyes-alliance/>.
- 228 David Dollar and Jonathan Stromseth, "The US Must Urgently Rethink Its Economic Policies in Asia," Brookings, February 17, 2021, <https://www.brookings.edu/blog/order-from-chaos/2021/02/17/us-must-urgently-rethink-its-economic-policies-in-asia/>.
- 229 Cindy Yu, "The Fightback Against Facial Recognition," *Spectator*, May 17, 2021, <https://www.spectator.co.uk/podcast/the-fight-back-against-facial-recognition>.
- 230 "S China's Guangdong Bans the Collection of Biometric Data from June," *Global Times*, May 18, 2021, <https://www.global-times.cn/page/202105/1223729.shtml>.
- 231 The idea for a Quad Infrastructure Hub is fleshed out in Haley Channer, *Advancing the Australia-US-Japan Infrastructure Partnership Through Private Sector Engagement* (Perth: Perth USAsia Centre, April 2021), <https://perthusasia.edu.au/our-work/pu-2021ipis-v15-hc-web.aspx>.
- 232 Michael Green and Evan Medeiros, "Can America Restore Its Credibility in Asia?" *Foreign Affairs*, February 15, 2021, <https://www.foreignaffairs.com/articles/united-states/2021-02-15/can-america-restore-its-credibility-asia>.
- 233 Jonathan E. Hillman and Maesea McCalpin, "Huawei's Global Cloud Strategy," Center for Strategic and International Studies, May 17, 2021, <https://reconasia.csis.org/huawei-global-cloud-strategy/>.
- 234 Hillman and McCalpin.
- 235 Ian Bremmer, "The Right Way to Confront China," *Nikkei Asia*, May 14, 2021, <https://asia.nikkei.com/Opinion/The-right-way-to-confront-China>.
- 236 For instance, see Michael McDevitt, "China as a Twenty First Century Naval Power," Lawrence Livermore National Laboratory's Center for Global Security Research, January 21, 2021, <https://cgsr.llnl.gov/event-calendar/2021/2021-01-21>.
- 237 South China Sea Expert Working Group, "A Blueprint for a South China Sea Code of Conduct," CSIS Asia Maritime Transparency Initiative, October 11, 2018, <https://amti.csis.org/blueprint-for-south-china-sea-code-of-conduct/>.
- 238 Hu Bo, director of Beijing-based think tank South China Sea Strategic Situation Probing Initiative, quoted in Liu Zhen, "US to Make Greater Use of Drones to Spy on China, Experts Say," *South China Morning Post*, May 16, 2021, <https://www.scmp.com/news/china/diplomacy/article/3133682/us-make-greater-use-drones-spy-china-experts-say>.
- 239 Teddy Ng and Laura Zhou, "US-China Infowar Escalates as America Deploys Task Force in Battle for Power and Influence," *South China Morning Post*, May 4, 2021, [https://www.scmp.com/news/china/military/article/3132184/us-china-infowar-escalates-america-deploys-task-force-battle?module=lead\\_hero\\_story\\_3&pgtype=homepage](https://www.scmp.com/news/china/military/article/3132184/us-china-infowar-escalates-america-deploys-task-force-battle?module=lead_hero_story_3&pgtype=homepage).
- 240 Ng and Zhou.
- 241 Ken Moriyasu, "US Eyes Using Japan's Submarines to 'Choke' Chinese Navy," *Nikkei Asia*, May 5, 2021, <https://asia.nikkei.com/Politics/International-relations/Indo-Pacific/US-eyes-using-Japan-s-submarines-to-choke-Chinese-navy>.

## Notes

This image shows a single page of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page, typical of notebook or legal stationery. There are no margins, text, or other markings on the page.

## Notes

[illegible]





Hudson Institute  
1201 Pennsylvania Avenue, Fourth Floor, Washington, D.C. 20004  
+1.202.974.2400 [www.hudson.org](http://www.hudson.org)