[redacted]

(U) House Permanent Select Committee on Intelligence

(U) The China Deep Dive: *A Report on the Intelligence Community's Capabilities and Competencies with Respect to the People's Republic of China*

[redacted]

[redacted]

(U) **Table of Contents**

(U) Introduction

(U) For the first time in three decades the United States is confronted by the rise of a global competitor. How the United States Intelligence Community meets the challenge of China's arrival on the global stage, as well as the continued potential for highly disruptive transnational crises that originate within our competitors' borders, the profound technological change transforming societies and communication across the globe, and the international order's return to near-peer competition will have profound and long-lasting implications on our nation's continued security, economic prosperity, and ability to preserve America's democratic way of life.

(U) In late 2019, the emergence of a novel coronavirus in Wuhan, China demonstrated to the world the profound danger associated with transnational crises originating within China's borders. China's enduring interest in preserving its own domestic political stability and international image in lieu of fostering a transparent and effective approach to public health, placed the United States, our allies, and the world at risk. Moreover, China's public response has been to further obfuscate the Chinese Communist Party's role in this international health crisis through the calculated promotion of fringe conspiracy theories and misinformation seeking to shift blame to the United States, muddy the truth about the virus's origins, and promote the image of China as a responsible global leader. Beijing's complicity in stopping scientific inquiries into the origin of the virus, and its disdain for accountability, require a strong U.S. response. Any appropriate U.S. response must be coupled with a rededication to ensuring that collection and analysis of activities within China remains robust, particularly in light of Beijing's opacity and global relevance.

(U) The United States, and its intelligence community, are no stranger to these moments. When the Berlin Wall fell in 1989, followed soon after by the end of the Cold War and the

collapse of the Soviet Union, the central organizing principle of American national security in the postwar world—the United States' superpower rivalry with the USSR—disappeared. As we entered this new era and a unipolar moment with the United States as global hegemon, the Intelligence Community, like the Department of Defense and other elements of the foreign policy establishment, found itself struggling for relevance and increasingly scarce resources in a country more focused on economic prosperity than security. Budget cuts, staffing reductions, and low morale were compounded by a sense that the CIA and its sister agencies no longer were essential elements of our national power.

(U) The September 11th attacks on New York and Washington shattered the post-Cold War abeyance, and the Intelligence Community was suddenly thrust into the lead role in a new counterterrorism role: defeating al Qaeda and other violent Islamist groups. From Afghanistan to Iraq, the Arabian Peninsula, and Africa, the IC, bolstered by billions in taxpayer dollars and a renewed sense of purpose, took the fight to America's enemies. As the counterterrorism mission expanded, the House Permanent Select Committee on Intelligence (HPSCI or the Committee) assesses that the IC treated traditional intelligence missions as secondary to counterterrorism. **The inattention of the 1990s to strategic and emerging threats remained largely unreversed**.

(U) But while the United States was busy engaging al Qaeda, ISIS, and their affiliates, offshoots, and acolytes, Washington's unchallenged dominance over the global system slipped away. Russia, while weaker than it had been during the days of the Soviet Union, remained a strategic challenge with a formidable nuclear arsenal and a revanchist ambition to match. Vladimir Putin was and remains committed to recapturing the power and prestige that the country had enjoyed during the Cold War and sought to rebuild the Russian military while taking advantage of every opportunity to confront the United States and its NATO partners. Iran and North Korea, both of which remain fundamentally weak states with sclerotic economies, tied their security to the pursuit of nuclear weapons and, in Iran's case, the sponsorship of a range of proxy terror organizations to extend its influence in the region.

(U) It was China, however, that has used the past two decades to transform itself into a nation potentially capable of supplanting the United States as the leading power in the world.

China's ascendance has been spectacular in its scale and far less benign than initially expected. During the 1990s and 2000s there was a consensus in the West that, as China became more prosperous and developed, it would also become freer and play a constructive role in international relations in the 21st Century.[1] Observers convinced themselves that the leadership in Beijing learned the "right" lessons from the international and domestic reaction to the Tiananmen Square crackdown in 1989. As a result, the broad trend as one of convergence between China and the West was assumed. Confidence that China would choose to liberalize was central to the decision to admit China to the WTO and to award the 2008 Summer Olympics to Beijing. This optimism was not entirely unfounded. Indeed, the introduction of village elections within China was considered by some to be a harbinger of liberalization.[2]

(U) However, the last decade has shown those expectations to have been deeply misplaced. Western policy-makers' belief that our own democratic systems were globally inevitable blinded observers to the Chinese Communist Party's overriding objective of retaining and growing its power. In the interim, the People's Republic of China (PRC) has increasingly sought to revise the international order and global norms in a way that furthers its own strategic interests and undermines those of the United States specifically, and the West generally.[3] Beijing has sought to expand its economic and political influence through its "One Belt, One Road" Initiative and the large-scale cooption of media outlets throughout the world.[4] Militarily, China has embarked on a massive modernization drive - creating a "blue water" navy, investing heavily in hypersonic weapons, developing its own fifth-generation fighter, militarizing a series of atolls and islets in the South China Sea to strengthen its claims in the region, and building its first overseas military base in Djibouti. Perhaps most consequential in the decades to come will be China's investment of resources, technology, and will into the creation of a post-modern authoritarian state in which the country's population is monitored around the clock through their

[1] (U) Kurt M. Campbell and Ely Ratner, "The China Reckoning: How Beijing Defied American Expectations," *Foreign Affairs,* March/April 2018.
[2] (U) "The Role of Elections in Representing the Chinese People and Advancing Democracy," Public Broadcasting System, January 9, 2007.
[3] (U) "Schieffer Series: China's Rise," Center for Strategic and International Studies, March 20, 2019.
[4] (U) Sarah Cook, "Beijing's Global Megaphone: The Expansion of Chinese Communist Party Media Influence since 2017," *Freedom House*, January 2020.

phones and an ever-growing network of surveillance cameras equipped with facial-recognition technology. Initially fueled by stolen U.S. technology and intellectual property, it is now driven by its own indigenous innovation. Beijing's expanding technological prowess will enable the Chinese Communist Party to improve its ability to watch, and therefore control, its own population. This "digital authoritarianism" has not only been deployed at home, but has been increasingly marketed to aspiring authoritarians abroad.[5]

(U) The confluence of a prolonged overweighting of American intelligence resources towards counterterrorism, the emergence of a global competitor in China, and the widespread, if not yet fully understood, global impact of COVID-19 and other transnational events make this both an opportune and urgent moment to assess our intelligence posture towards China and to provide strategic guidance to the IC as it repositions itself to better understand China's domestic environment, capabilities, plans, and intentions. Safeguarding U.S. national security requires the capacity to understand Chinese military capabilities, elite political dynamics, and international posture, but also, as the utter devastation of the pandemic has brought home, to provide sufficient indications and warnings for events of global impact, such as a disease outbreak. Notwithstanding the ongoing public debate on the advisability of interdependence, today's globalized world necessitates thoughtful, detailed, and expansive analysis of how events within China, and how China's leadership decides to react to those events, have the potential to meaningfully alter the world's course.

(U) To address this strategic challenge, wise and effective national policy will be critical. Its formulation and implementation in turn will depend on the U.S. Intelligence Community's (IC) collection, and provision to policymakers, of intelligence of the highest quality. Regardless of what tack U.S. policy takes in the coming decades, a strong IC capability to accurately assess China's motives and behavior necessitates prioritization and rigorous oversight. If bilateral relations continue to degrade, U.S. leaders must have a clear understanding of the second- and third-order impacts of decisions made both in Washington and Beijing.

[5] (U) Naazneen Barma, Brent Durbin, and Andrea Kendall-Taylor, "Digital Authoritarianism: Finding Our Way Out of the Darkness," War on the Rocks, February 10, 2020.

(U) In May 2019, the Committee initiated a review to assess the IC's ability to execute, with respect to China, its core mission of "collecting, analyzing, and delivering foreign intelligence and counterintelligence….to America's leaders so they can make sound decisions."[6] This review was motivated by two prevailing factors. First, the Committee assessed that the IC's ability to fulfill emerging intelligence requirements regarding near-peer nation states had atrophied, in part because of the United States' long-standing focus on counterterrorism and Middle East regional issues. Second, the Committee believes that China poses a unique and growing strategic challenge to U.S. national security. The prevailing factors, combined with the real-time implications of disease that emerged in China's Hubei Province, lead the Committee to conclude that it is imperative that U.S. policymakers have the fullest possible understanding of China's plans, intentions, capabilities, and public health crises.

(U) Over the course of the review, Committee staff on a bipartisan basis conducted hundreds of hours of interviews with IC officers, examined thousands of analytic assessments, and visited facilities operated by over a dozen IC elements. Additionally, Committee staff solicited feedback on the IC's performance from customers throughout several departments and agencies. The goals of the Committee's review were:

(1) (U) assess, with respect to China, the IC's performance within each of the so-called "intelligence cycle's" six phases;

(2) (U) to make recommendations to increase the quality of raw intelligence reports and finished analytic products; and

(3) (U) to assess the adequacy of current IC resource levels.

(U) The review resulted in 23 public findings regarding the IC's activities with respect to China, 36 public recommendations, and over 100 classified recommendations. While the Committee's inquiry was focused solely on China, in the course of its review, the Committee identified several items of relevance to the broader structure and governance of the Intelligence Community.

[6] (U) "Mission," Intel.gov, January 3, 2020, www.intelligence.gov/mission.

(U) The Committee's central finding of this report is that the United States' intelligence community has not sufficiently adapted to a changing geopolitical and technological environment increasingly shaped by a rising China and the growing importance of interlocking non-military transnational threats, such as global health, economic security, and climate change. **Absent a significant realignment of resources, the U.S. government and intelligence community will fail to achieve the outcomes required to enable continued U.S. competition with China on the global stage for decades to come, and to protect the U.S. health and security.**

(U) The People's Republic of China in 2020

(U) The nature and pace of China's transformation into a near-peer, global competitor demands the focused attention of the U.S. intelligence community. Under the leadership of Chinese Communist Party (CCP) General Secretary Xi Jinping, China has sought to expand its global influence through the modernization of the People's Liberation Army (PLA), the growth of the "One Belt, One Road" Initiative, the cultivation of foreign sub-national and civic organizations, and the propagation of disinformation. Moreover, important Chinese technological advances in key fields, such as artificial intelligence, quantum computing, and 5G telecommunications call into question the self-assured preeminence of U.S. technology in the rapidly changing technological landscape. Finally, the emergence of COVID-19 in Wuhan, and Beijing's reactions to the virus's early spread, underscore the continued potential for devastating and destabilizing global events originating in China.

(U) These and other developments challenge analysts to synthesize and assess disparate streams of information. The stakes are high. If the IC does not accurately characterize and contextualize Beijing's intent, America's leaders will fail to understand the factors that motivate Chinese decision-making. If policymakers do not understand how and why Beijing makes decisions, they will struggle to develop policies that result in outcomes favorable to U.S.

interests and global security overall. And if the IC does not, in close collaboration with the whole of government, identify early future transnational threats, such as a disease with pandemic potential, history might disastrously repeat itself.

(U) The Chinese Communist Party's Ideological Vision for the 21st Century

(U) Under the leadership of Chairman Xi Jinping, China has reasserted its ideological commitment to Marxist-Leninism and sought to further cement the Chinese Communist Party within the Chinese state apparatus.[7] At the November 2017 19th Party Congress, Xi successfully incorporated his eponymous "Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era," into the Chinese Communist Party's constitution. This feat, placing him on par with Mao Zedong and Deng Xiaoping, is representative of Xi's increasingly singular ability to shape the ideological trajectory of the Party, and therefore China writ-large.[8] Inextricably linked to this is the achievement of the "China Dream," a concept that Xi has tied to the rejuvenation of the Chinese nation, the development of a powerful military capable of defending China's core interests, the achievement of "one country, two systems" in Hong Kong and Taiwan, and the elimination of "lax and weak governance" over the Party through adherence to the mass line.[9]

(U) Domestically, China has taken new steps to integrate the role of ideological education into daily life. The "Little Red App" is a Chinese smartphone application that synthesizes social network, indoctrination, and surveillance into a single app extoling the CCP and Xi himself.[10] The app, which has been downloaded ninety million times, has been subsequently used as a tool to assess Chinese citizens' ideological commitment to the Party.[11] Quizzes test app users' understanding of CCP ideological concepts and monitor the amount of time users have spent engaging with key propaganda themes. Android versions reportedly contain powerful spyware tools, giving the app "administrator-level access" on the phone, which enables developers to

[7] (U) Lucy Hornby, "Xi Jinping pledges return to Marxist roots for China's Communists," Financial Times, July 1, 2016.
[8] (U) Michael A. Peters, The Chinese Dream: Xi Jinping thought on Socialism with Chinese characteristics for a new era," Educational Philosophy and Theory, 49:14, 1299-1304, 2017.
[9] (U) Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era," October 18, 2017.
[10] (U) Raymond Zhong, "Little Red App: Xi's Thoughts are (Surprise!) a Hit in China," The New York Times, February 14, 2019.
[11] (U) Evan Osnos, "The Future of America's Contest with China," the New Yorker, January 6, 2020.

download software, take photos and videos from the phone, transmit the users' location, or even install a program to log keystrokes.[12] In short, the CCP is seeking to expand its control of China's population through technologically-enhanced authoritarianism.[13]

(U) We expect China's use of digital authoritarianism to continue to be exported beyond its own borders. While China's leadership asserts that its pursuit of the Chinese Dream has led China to make "great new contributions to global peace and development," the "peace and development" that Beijing seeks to promote is defined in ways that preference Beijing's objectives. Indeed, Xi Jinping's signature foreign policy concept, the creation of "a community of shared future for mankind," is considered to be foundational to the creation of a "new type of international relations" in which the external international environment is favorably disposed to the achievement of the China Dream.[14] Worryingly, it appears as if those outside of Beijing have little opportunity to define what this "community of shared future for mankind" might consist of, particularly as China continues to pressure international organizations to integrate its own ideological maxims into multilateral agreements.[15] This raises the specter of the further globalization of Beijing's ideology, potentially degrading longstanding international norms concerning the rights of the individual, and the very idea of liberal and free societies.

(U) Chinese officials' belief that China's model and system of governance are exceptional and infallible has helped to fuel China's recent advancements in the military, technological, and information domains. Chinese commentators have painted the United States' commitment to democracy as outdated and violent, championing their own interpretation of "democracy" as an appropriate model for the international system.[16] However, recent events in Hong Kong demonstrate that, even under the remit of "one country, two systems," it is unlikely

[12] (U) Anna Fifield, "Chinese app on Xi's ideology allows data access to users' phones, report says," The Washington Post, October 12, 2019.
[13] (U) Samantha Hoffman, "Testimony before the House Permanent Select Committee on Intelligence Hearing on 'China's Digital Authoritarianism: Surveillance, Influence, and Political Control,'" May 16, 2019.
[14] (U) Liza Tobin, "Xi's Vision for Transforming Global Governance: A strategic Challenge for Washington and Its Allies," Texas National Security Review, 2:1, November 2018.
[15] (U) Colum Lynch, Robbie Gramer, "Senior Officials Concede Loss of U.S. Clout as Trump Prepares for U.N. Summit," Foreign Policy, September 5, 2019.
[16] (U) Ai Jun, "Washington not world's 'beacon of democracy,'" The Global Times, September 16, 2019.
Tobin, ""Xi's Vision for Transforming Global Governance: A strategic Challenge for Washington and Its Allies."

that true democratic life and the CCP in its current form can coexist in a peaceful and constructive way.[17] The mass internment of over one million ethnic Muslims in Xinjiang province demonstrates the CCP's willingness to engage in gross human rights abuses, in a fashion so pervasive and widespread as to potentially implicate the government in crimes against humanity.[18] The U.S. must summon the moral courage to condemn these heinous crimes in the strongest terms and rally the world to join.

(U) The Emergence of COVID-19 and Transnational Implications of China's Reach

(U) As evidenced by the global COVID-19 pandemic, the United States would be remiss to assume that the totality of events originating within China with national security or economic implications emanate solely from Beijing and Shanghai. In late 2019, a strain of novel coronavirus emerged in Wuhan, China. Notwithstanding Wuhan's large population and regional prominence in central China, Wuhan is in many respects a typical Chinese city. The average annual income for workers in Wuhan is approximately $12,600 USD. Several large multinational corporations such as General Motors, Starbucks, and McDonalds have locations in the Wuhan area.[19] Regular direct flights left Wuhan's international airport for New York, San Francisco, and other global destinations as the virus spread undetected from December 2019 to January 2020.[20] This global connection does not make Wuhan exceptional. In fact, its trajectory closely mirrors many mega-cities in contemporary China. However, despite the city's growing engagement with the global economy and its population of approximately 11 million—several million more than New York City—most Americans were unfamiliar with Wuhan. The emergence of COVID-19 underscores that, notwithstanding the global focus on Beijing, Shanghai, and Hong Kong, there are a significant number of cities throughout China that could – and in the case of COVID-19 do – independently impact the world and our own country's trajectory in dramatic ways.

[17] (U) Peter S. Goodman and Austin Ramzy, "Hong Kong's Status as Neutral Ground at Risk as China Asserts Power," The New York Times, October 1, 2019.
[18] (U) "Annual Report: 2019," Congressional-Executive Commission on China, 116th Congress, November 18, 2019.
[19] (U) Jordan Valinsky, "These American brands have the biggest exposure to China's economy, CNN, January 28, 2020, https://www.cnn.com/2020/01/28/business/american-businesses-china-coronavirus/index html.
[20] (U) John Kelly and Pierre Thomas, "Disaster in motion: Where flights from coronavirus-ravaged countries landed in US," ABC News, April 7, 2020, https://abcnews.go.com/Health/disaster-motion-flights-coronavirus-ravaged-countries-landed-us/story?id=70025470.

(U) While the initial point of transmission of COVID-19 has not yet been definitively identified, the first documented location of community spread occurred at the Huanan Seafood Wholesale Market, a prominent wet market in Wuhan.[21] Subsequent academic reports judge that the first known individual to have contracted the disease was reportedly infected on November 17, 2019, although case clusters did not begin to emerge in Wuhan hospitals until mid-December 2019.[22] It was not until December 31, 2019 that the World Health Organization was formally notified of this outbreak, in response to WHO employees independently noting a media statement from the Wuhan Municipal Health Commission.[23] The Committee continues to conduct a separate comprehensive review into COVID, and the IC response to it.

(U) The intervening period from the initial detection of a cluster of pneumonia cases in Wuhan in mid-December 2019, to the CCP's January 22, 2020 decision to quarantine Wuhan raises profound questions about China's ability to mount an effective response to a transnational crisis emanating from within its borders. To that end, there has been significant debate surrounding what President Xi Jinping and other key leaders in Beijing knew, and when they knew it.[24] On February 15, Qiushi, an authoritative Chinese journal, published commentary stating that President Xi Jinping issued guidance on the prevention and control (*fangkong)* of the outbreak at a January 7, 2020 meeting.[25] However, neither Qiushi's promulgation, nor documents released in conjunction with the January 7 meeting, provide details on the content of Xi's guidance. Moreover, based on systemic flaws within the Chinese Communist Party's (CCP) own governance structures, there is reason to believe that the information presented to Xi was incomplete or biased. Within the CCP, provincial and municipal leaders have been historically

[21] (U) Dina Fine Maron, "Wet markets' likely launched the coronavirus. Here's what you need to know," April 15, 2020, https://www.nationalgeographic.com/animals/2020/04/coronavirus-linked-to-chinese-wet-markets/.
[22] (U) Josephine Ma, "Coronavirus: China's first confirmed Covid-19 case traced back to November 17," South China Morning Post, March 13, 2020, https://www.scmp.com/news/china/society/article/3074991/coronavirus-chinas-first-confirmed-covid-19-case-traced-back.
[23] (U) "Timeline of WHO's response to COVID-19," The World Health Organization, June 30, 2020, https://www.who.int/news-room/detail/29-06-2020-covidtimeline.
[24] (U) Editorial Board, "What did Xi Jinping know about the coronavirus, and when did he know it?" The Washington, Post, February 19, 2020, https://www.washingtonpost.com/opinions/global-opinions/what-did-xi-jinping-know-about-the-coronavirus-and-when-did-he-know-it/2020/02/19/35482fe2-5340-11ea-b119-4faabac6674f_story.html.
[25] (U) "*Zai Zhongyang Zhengzhi Ju Changwei Hui Huiyi Yanjiu Yingdui Xinxing Guanzhuang Bingdu Feiyan Yiqing Gongzuo Shi de Jianghua,"* Qiushi, February 15, 2020, www.qstheory.cn/dukan/qs/2020-02/15/c_1125572832.htm

incentivized to engage in inter-locality competition and political interventions in order to win the favor of the central government, thereby securing the political futures of the individual leaders placed in positions of power.[26] Hubei province's officials handling of the emergence of COVID-19 followed this pattern.[27] In an effort to identify a scapegoat, senior officials in Hubei were removed from their posts in mid-February.[28]

(U) Overall, COVID-19's emergence in China created plausible conditions under which provincial party leadership and governments, fearful of higher-level retribution, failed to take action. These provincial entities, who in actuality retain responsibility for large populations, merit further attention and analysis from international onlookers given their potential for impacting global affairs. Indeed, COVID-19 has only underscored the criticality of U.S. decision-makers having a strong grasp of and insights into provincial dynamics, particularly as they relate to the central leadership's relationship with provincial entities.[29] Conversely, the PRC has consistently demonstrated interest in developing ties with state- and municipal-level decision-makers in the United States, underscoring the importance that Beijing places on developing a comprehensive picture of sub-national dynamics in America.[30] While there have been calls for a reexamination of the high degrees of interdependence between the United States and China, it would be counterproductive for the United States to completely shy away from a close and careful examination of the domestic nuances and complexities within the PRC.[31] Certainly, there will be some domains of interaction, such as public health and climate change, that necessitate a degree of cooperation between the United States and China. U.S. decision makers seeking to cooperatively engage must be well-informed to enter into negotiations from a

[26] (U) Yi Li and Fulong Wu, "Understanding city-regionalism in China: regional cooperation in the Yangtze River Delta," *Regional Studies* 52, no. 3 (April 2015), 313-324.
[27] (U) Steven Lee Myers, "China Created a Fail-Safe System to Track Contagions. It Failed," The New York Times, March 29, 2020, updated April 17, 2020, https://www nytimes.com/2020/03/29/world/asia/coronavirus-china.html.
[28] (U) Cissy Zhou and William Zheng, "Coronavirus: Heads Roll in Hubei as Beijing's patience runs out," South China Morning Post, February 11, 2020.
[29] (U) For more information on how national-level political dynamics within China impacted local-level work on the COVID-19 response, see: "China Delayed Releasing Coronavirus Info, frustrating WHO," The Associated Press, June 2, 2020.
[30] (U) "Chinese Influence & American Interests: Promoting Constructive Vigilance," Hoover Institution Press, October 24, 2018.
[31] (U) For information on Chinese perceptions of decoupling, see: Julian Gewirtz, "The Chinese Reassessment of Interdependence," China Leadership Monitor, issue 64, June 1, 2020.

position of strength. Although the CCP is careful to project a steely veneer of monolithic policy preferences, failing to understand the competing perspectives, different centers of gravity, and diverse viewpoints within China's vast internal bureaucracy and different regions will cheapen U.S. analysis of internal PRC dynamics – dynamics that plausibly set the trajectory for the early stages of the novel coronavirus outbreak in Hubei Province.[32]

(U) COVID-19 and Domestic Information Control

(U) Once it became clear that a response to COVID-19 would require sacrifices from and the active participation of its population, CCP officials began seeking to control the COVID-19 narrative in a way designed to engender support for the Party's actions. The cooption of Dr. Li Wenliang's memory is the most striking example of how the CCP seeks to rehabilitate and exploit key events to drive narratives designed to maintain internal stability, often at the expense of the truth. On December 30, 2019, Dr. Li informed former classmates that he had treated several cases resembling SARS. Days later, he was forced by the Public Security Bureau to sign an apology for "disturbing the social order" and was publicly reprimanded. Dr. Li subsequently contracted COVID-19 and became known as a folk hero on Chinese social media for his early warnings. Dr. Li subsequently passed away from the virus on February 6, 2020.[33] Immediately after Dr. Li's death, Chinese social media sites were overtaken with exceedingly critical comments targeting the CCP. China's public mourned Dr. Li, publicly calling for the freedom of speech and the end of censorship.[34] However, attempts to use Dr. Li's death as a galvanizing force for change were quickly stymied. CCP leadership soon acted to paint Dr. Li as a patriot,

[32] (U) For further discussion of "collusion" between local officials and higher-level authorities to locally adapt national-level policy directives, see: "CLM Insights: Interview with Xueguang Zhou," China Leadership Monitor, June 1, 2020.
[33] (U) "Li Wenliang: Coronavirus kills Chinese whistleblower doctor," BBC News, February 7, 2020, https://www.bbc.com/news/world-asia-china-51403795.
[34] (U) Huileng Tan, "Coronavirus whistleblower doctor dies, sparking outpouring--and censorship—on social media," CNBC News, February 7, 2020, https://www.cnbc.com/2020/02/07/hashtag-censored-after-coronavirus-whistleblower-doctors-death.html.

whitewashing the initial criminalization of Dr. Li's reports and hailing him as a hero in the CCP's fight against COVID-19.[35]

(U) The CCP's dedication to strict information control – and even recasting its own past actions to warp the record – has profound effects on how the United States should track and evaluate events occurring within China, all of which extend beyond after-action analyses of the emergence of COVID-19. Statements and articles emerging from China's vast propaganda apparatus must be analyzed through the prism of narrative control, rather than uncritically accepted as fact or reflexively assumed as false. Within academia and China scholarship broadly, there is a long tradition of utilizing careful propaganda analysis as a method to discern CCP policy preferences and priorities.[36] Understanding what information the CCP seeks to suppress or amplify, and at which inflection points, provides critical insights into the Party's objectives both domestically and abroad. The emergence of COVID-19 provides observers with an important template to understand how the CCP can rapidly mitigate and manage "black swan" events and internal popular dissent.

(U) Chinese Military Might

(U) In service of achieving the "Chinese Dream," China's People's Liberation Army has continued "to implement the most comprehensive restructuring in its history to become a force capable of conducting complex joint operations."[37] This evolution in the force, initiated to enhance China's military services' ability to mitigate historic interoperability challenges, likely enhances China's confidence in its ability to project power regionally, particularly with respect to Taiwan.[38] Moreover, China's illegitimate territorial claims in the South China Sea and unprofessional maneuvers present continued challenges to the safe execution of U.S. Navy

[35] (U) "China Media Bulletin: Coronavirus-era repression, propaganda, censorship, surveillance and more," Freedom House, March 2020, https://freedomhouse.org/report/china-media-bulletin/2020/china-media-bulletin-coronavirus-era-repression-propaganda
[36] (U) Alice Miller, "Valedictory: Analyzing the Chinese Leadership in an Era of Sex, Money, and Power," China Leadership Monitor, no. 57, August 2018, https://www.hoover.org/sites/default/files/research/docs/clm57-am-final.pdf.
[37] (U) "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019," The Office of the Secretary of Defense, The Department of Defense, 2019, pg. ii.
[38] (U) Kathrin Hille, "China military build-up makes attack on Taiwan more likely, says US," Financial Times, January 16, 2019.

operations in the Pacific.[39] Despite public and contrary assurances from Xi to former U.S. President Barack Obama, China has deployed surface-to-air missiles and fighter aircraft on Woody Island, an island enlarged through environmentally harmful land reclamation practices.[40] Beyond the Indo-Pacific, China has opened its first overseas military base in Djibouti, and is allegedly seeking a base in Cambodia, both of which could provide additional logistical support for overseas Chinese military operations and challenge U.S. and allied freedom of navigation.[41] In the event of a contingency or other crisis, instability in the Pacific could choke key shipping lanes, threatening the $3.37 trillion dollars of global commercial trade that traverses these waters every year.[42]

(U) The Department of Defense further assesses that, "PLA capabilities in development provide options for China to dissuade, deter, or, if ordered, defeat third-party intervention during a large-scale, theater campaign such as a Taiwan contingency.[43]" Key systems such as the H-6K bomber aircraft, demonstrate China's ability to hold Guam at risk with land-attack cruise missiles.[44] The DF-21D, a land-based intermediate-range ballistic missile has been labeled "the carrier killer" by some analysts who assess that the missile's primary purpose is to deter, and potentially defeat, U.S. aircraft carriers in the Pacific.[45] Moreover, China continues to invest in technologically innovative weapons systems. In the October 2019 parade commemorating the 70th anniversary of the founding of the People's Republic of China, the PLA publicly presented hypersonic cruise missiles, new unmanned aerial vehicles (UAVs), and long-range submarine launched cruise missiles.[46] China's continued advancements in cyber and space-based systems

[39] (U) Steven Lee Myers, "American and Chinese Warships Narrowly Avoid High-Seas collision," The New York Times, October 2, 2018.
[40] (U) "Update: China's Continuing Reclamation in the Paracels," Asia Maritime Transparency Initiative, Center for Strategic and International Studies, August 9, 2017.
[41] (U) Timothy R. Heath, "The Ramifications of China's Reported Naval Base in Cambodia," World Politics Review, August 5, 2019.
[42] (U) China Power Team. "How much trade transits the South China Sea?" China Power. August 2, 2017. Updated October 10, 2019.
[43] (U) "Annual Report to Congress," p. 54.
[44] (U) Derek Grossman, Nathan Beauchamp-Mustafaga, Logan Ma, and Michael S. Chase, "China's Long-Range Bomber Flights: Drivers and Implications," RAND Corporation, 2018.
[45] (U) David Lague, Benjamin Kang Kim, "Special Report: New missile gap leaves U.S. scrambling to counter China," Reuters, April 25, 2019.
[46] (U) Michael Martina, "China showcases fearsome new missiles to counter U.S. at military parade," Reuters, October 1, 2019.

also introduce the likelihood of entirely new domains of conflict in the event of a contingency. [47] These new domains could redefine existing conceptions of how a 21st century war would unfold, extending the battlefield to our political discourse, mobile devices, and the very infrastructure that modern digital communication and communities rely upon.

(U) Technological Advancements and Export of Digital Authoritarianism

(U) At the center of the CCP's ambitions to achieve the China Dream is Beijing's quest to become a "science and technology world superpower.[48]" Key Chinese directives and initiatives, including "Made in China 2025" and the "Thousand Talents Program," have ensured CCP support for critical sectors. While initially fueled by illicitly acquired technology from foreign entities as well as billions of dollars of state-directed subsidies to priority sectors, Chinese technology firms, including Huawei and ZTE, are now successfully competing in international markets.[49] As China now seeks to build on these initial gains, U.S. leadership in key fields, such as quantum computing and artificial intelligence, is no longer assured. Moreover, findings from a U.S. Senate inquiry noted that federal agencies were unprepared to prevent China from illicitly acquiring U.S. taxpayer-funded research.[50]

(U) In recent years, China's advancements in quantum sciences have enabled new innovation in quantum-based cryptography, networks, computing, and space experiments, all of which are fields with clear dual-use military applications.[51] China's artificial intelligence sector has seen rapid growth in recent years, producing over a dozen billion-dollar companies.[52] China is also using this technology to monitor its population, including installing hundreds of millions

[47] (U) Daniel R. Coats, "Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community," The Office of the Director of National Intelligence, Senate Select Committee on Intelligence, January 29, 2019, p. 5, 17.
[48] (U) "*Jianshe shijie keji qiangguo, kan xijinping shi da guanjian ci,"* Xinhua News, May 30, 2018.
[49] (U) For a comprehensive assessment of China's technology transfer practices, see: "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, intellectual Property, And Innovation Under Section 301 of the Trade Act of 1974," Office of the United States Trade Representative, Executive Office of the President, March 22, 2018.
[50] (U) Senate Homeland Security and Government Affairs Permanent Subcommittee on Investigations, "Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans," November 18, 2019.
[51] (U) Elsa B. Kania and John K. Costello, "Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership," The Center for a New American Security, September 2018.
[52] (U) Will Knight, "China's AI Unicorns Can Spot Faces. Now They Need New Tricks," Wired, December 12, 2019.

of surveillance cameras throughout the country, many equipped with facial recognition technology.[53] The Chinese government has long used technology to control and manipulate its population online, and its aggressive pursuit of artificial intelligence is helping move that control into the physical world.[54] Within Xinjiang province, predictive algorithms have been used to identify candidates to detain in the CCP's "re-education camps."[55] Chinese companies are also increasingly exporting this digital authoritarianism abroad, selling artificial intelligence surveillance products to over 60 countries.[56] One striking example was Ecuador's 2011 adoption of Chinese surveillance technology, which subsequently enabled the domestic intelligence service to monitor dissidents' every movement.[57] In a 2016 visit to Ecuador, President Xi visited the surveillance center's headquarters, demonstrating the high degree of political support for the continued development and export of these products.

(U) Of importance to U.S. multinational corporations and the global economy is the role of the Chinese Communist Party within these ostensibly private corporations. According to the Australian Strategic Policy Institute, China has sought to extend the Party's reach into key private firms; as of 2016, there were approximately 1.3 million Chinese Communist Party committees within private firms, a sevenfold increase from 2006.[58] While the American private sector should welcome competition, the CCP's integration into private firms' decision-making structures constitutes an inherently unfair and inappropriate intervention into some of the world's most critical sectors and markets. More critically for U.S. national security interests, the Committee's 2012 report on Huawei made clear the potential risks to U.S. telecommunications infrastructure in the event that a purportedly private Chinese company has the capacity to be

[53] (U) Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," The New York Times, July 8, 2018.
[54] (U) Elizabeth C Economy, "The Great Firewall of China: Xi Jinping's Internet Shutdown," The Guardian, June 29, 2018.
[55] (U) "China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App," Human Rights Watch, May 1, 2019.
[56] (U) Steven Feldstein, "The Global Expansion of AI Surveillance," Carnegie Endowment for International Peace, September 17, 2019.
[57] (U) Paul Mozur, Jonah M. Kessel, and Melissa Chan, "Made in China, Exported to the World: The Surveillance State," The New York Times, April 24, 2019.
[58] (U) Danielle Cave, Samantha Hoffman, Alex Joske, Fergus Ryan, and Elise Thomas, "Mapping China's Tech Giants," Australian Strategic Policy Institute, April 18, 2019.

compelled or coerced by the Chinese Communist Party.[59] These findings, while drafted in reference to Huawei and ZTE, contain broadly generalizable implications for U.S. and allied adoption of software and hardware originating from Chinese companies with similar relationship structures to the CCP.

(U) The Post-COVID-19 Authoritarian Playbook: Public Health, Surveillance, and Social Control

(U) China's domestic response to COVID-19 has created new opportunities for the CCP to introduce authoritarian tactics in the digital realm. Alipay Health Code, a new smartphone application designed to inform users of their self-quarantine status, harvests vast amounts of user data and transmits it to local police.[60] Using opaque algorithms, Alipay Health Code processes harvested data to assign users with a green, yellow, or red QR code, which corresponds to the users' self-quarantine status. In large Chinese cities, it is routine for businesses to require patrons to display their Alipay Health Code, ensuring widespread adoption of the app. Analysts have noted the blurred lines between the role of Alibaba, a private enterprise, and the PRC's security apparatus, raising concerns about the ultimate use of the data.[61] The city of Hangzhou, where the applications were initially developed, has announced that it intends to continue usage of the application even after the COVID-19 pandemic.[62] It is unclear what, if any, privacy safeguards are included within the application, providing the CCP another detailed window into the activities and associations of all PRC residents.

(U) There is evidence to suggest that China's attempts to integrate public health and security are indicative of a broader campaign to normalize the security apparatus' intervention into PRC citizens' everyday lives as a matter of public health. Recent work on the CCP concept of "prevention and control" (*fangkong)* identified disturbing instances in which the CCP

[59] (U) "The U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," The House Permanent Select Committee on Intelligence, October 8, 2012.
[60] (U) Paul Mozur, Raymond Zhong, and Aaron Krolik, "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags," The New York Times, March 1, 2020, https://www nytimes.com/2020/03/01/business/china-coronavirus-surveillance html
[61] (U) Jordan Schneider, "China Voices | How Alibaba built China's health code," Technode, April 7, 2020, https://technode.com/2020/04/07/china-voices-how-alibaba-built-chinas-health-code/.
[62] (U) Jane Li, "China's health scores for citizens won't go away when coronavirus does," Quartz, May 25, 2020, https://qz.com/1860453/chinese-city-will-use-health-scores-for-citizens-even-after-covid-19/.

promotes inoculating the population against ideological viruses, normalizing discourse that describes national security and public health interchangeably.[63] This intertwining of public health and national security further empowers the CCP to use COVID-19 as a means through which it enhances and extends its growing network of invasive surveillance. Moreover, given the international demand for tools to quickly and effectively combat COVID-19, China's development of a fused public health and national security doctrine opens the door to increased export of digital authoritarianism. China has sought to increase focus on the Health Silk Road and Digital Silk Road components of One Belt, One Road, in the wake of the pandemic, acknowledging the global demand for cooperation on health technology issues.[64] This raises the specter of a surveillance state fueled by increasingly personalized data sources. It is incumbent upon the United States to identify digital solutions to public health crises that adequately balance citizens' right to privacy with the need to protect the public.

(U) Counterintelligence, Agents of Influence, and the United Front

(U) In tandem with Beijing's increasing military and technological clout, China's intelligence services continue to threaten the safety and security of U.S. personnel and national security information. In 2019, ODNI assessed that, "based on their services' capabilities, intent, and broad operational scopes," China's and Russia's intelligence services will continue to be the leading intelligence threats to the United States.[65] The 2014 breach of the Office of Personnel Management (OPM)'s federal personnel and background investigation records has been attributed to state-sponsored Chinese hacking. In February 2020, the U.S. Department of Justice indicted members of the People's Liberation Army for the Equifax breach, demonstrating the impact of Chinese espionage on nearly 150 million Americans' personal information.[66] In 2019

[63] (U) Sheena Chestnut Greitens and Julian Gewirtz, "China's Troubling Vision for the Future of Public Health," Foreign Affairs, July 10, 2020, https://www.foreignaffairs.com/articles/china/2020-07-10/chinas-troubling-vision-future-public-health.
[64] (U) "WHO Director-General's opening remarks at high-level video conference on Belt and Road International cooperation – 18 June 2020," World Health Organization, June 18, 2020, https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-high-level-video-conference-on-belt-and-road-international-cooperation---18-june-2020
[65] (U) Coats, "Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community," p. 13.
[66] (U) Aruna Viswanatha, Dustin Volz, and Kate O'Keefe, "Four Members of China's Military Indicted Over Massive Equifax Breach," The Wall Street Journal, February 11, 2020.

alone, three former Intelligence Community officers were charged by U.S. prosecutors and sentenced to prison for delivering or seeking to deliver classified information to PRC intelligence officers.[67] Moreover, the National Counterintelligence and Security Center warned in its 2018 report that, "most Chinese cyber operations against U.S. private industry that have been detected are focused on cleared defense contractors or IT and communications firms whose products and services support government and private sectors networks worldwide.[68]" As of February 2020, the Federal Bureau of Investigation is investigating China-related cases in all fifty states and each of its 56 field offices.[69] Broadly, the Committee assesses that China's intelligence services will continue to pose a formidable challenge to the U.S. intelligence community, which will require equal parts ingenuity, humility, and vigilance to address.

(U) Outside of China's conventional intelligence apparatus exists a separate layer of influence actors, many of which are funded and organized by the Chinese Communist Party's United Front Work Department, Central Propaganda Department, and the International Liaison Department.[70] To that end, Chinese influence operations in the United States intentionally obscure the line between typical civil society engagements and malign influence activities. In particular, the CCP's United Front Work Department, which Chairman Xi Jinping has referred to as one of China's "magic weapons," seeks to guide foreign governments, political parties, private entities, and the overseas Chinese diaspora community to adopt positions that are favorable to the Chinese Communist Party's interests.[71] Within the United States, Chinese influence operations have targeted cultural institutions, state- and municipal-level government offices, media organizations, educational institutions, businesses, think tanks, and policy communities.[72]

[67] (U) *See* Adam Goldman, "Former CIA Officer Sentenced to 20 Years After Spying for China," the New York Times, May 17, 2019; Mihir Zaveri and Mariel Padilla, "U.S. Intelligence Officer who Tried to Share Secrets With China is Sentenced to 10 Years," New York Times, September 24, 2019; Zach Montague, "Ex-CIA Officer Sentenced to 19 Years in Chinese Espionage Conspiracy," The New York Times, November 22, 2019.
[68] (U) "Foreign Economic Espionage in Cyberspace," National Counterintelligence and Security Center, 2018.
[69] (U) Andrew Lelling and Joseph Bonavolonta, "The intel on China's counterintelligence threat to America," the Boston Globe, February 11, 2020.
[70] (U) Anne-Marie Brady, "Magic Weapons: Chinese Political Influence Activities Under Xi Jinping," The Wilson Center, September 2017.
[71] (U) Brady, "Magic Weapons: Chinese Political Influence Activities Under Xi Jinping."
Alexander Bowe, "China's Overseas United Front Work: Background and Implications for the United States," U.S.-China Economic and Security Review Commission, August 24, 2018.
[72] (U) "Annual Report to Congress," p. 112.

(U) Chinese Propaganda & Disinformation Efforts

(U) Historically, China's external propaganda efforts have been focused on the cultivation of positive global impressions of Beijing's behavior, such as promoting the narrative of China's "peaceful rise."[73] However, in the wake of the 2019 protests in Hong Kong and the COVID-19 pandemic, China's approach to propaganda and disinformation has undergone significant transformations across several key dimensions, each of which carries the potential to further muddy the global information environment and enable Beijing to achieve its objectives.[74] The most readily visible change in China's international messaging posture is the rise in aggressive, overt, coordinated public diplomacy efforts on Western social media platforms. Research conducted by the German Marshall Fund found that China's official diplomatic presence on Twitter has increased by more than 250% in the past year.[75] Several of these new accounts have actively spread disinformation in the wake of the COVID-19 outbreak, including advancing fringe conspiracy theories that COVID-19 originated in a U.S. military lab and amplifying existing Russian and Iranian disinformation emanating from their respective state medias.[76] Official state-backed media sources have also echoed these theories, signaling broader messaging connectivity between China's MFA and the Propaganda Bureau's overseas activities.[77] This rise in overt disinformation is a stark break from past Chinese messaging tactics, which were more passive in nature and designed to shape long-term perceptions of China.

Anna Gronewold, "Pompeo to governors: China is watching you," Politico, February 8, 2020.

[73] (U) For more information on the development of the concept of China's peaceful rise, see: "China's Peaceful Rise: Speeches of Zhen Bijian, 1997-2004," The Brookings Institution, June 2005.
For information on how China's internal messaging and external propaganda efforts surrounding the "peaceful rise" concept differ, see: Anne-Marie Brady, "China's Foreign Propaganda Machine," The Wilson Center, October 26, 2015.

[74] (U) Sarah Cook, "Welcome to the New Era of Chinese Disinformation," The Diplomat, May 11, 2020.

[75] (U) Laura Rosenberger, "China's Coronavirus Information Offensive: Beijing is Using New Methods to Spin the Pandemic to Its Advantage," Foreign Affairs, April 22, 2020.

[76] (U) Rosenberger, "China's Coronavirus Information Offensive: Beijing is Using New Methods to Spin the Pandemic to Its Advantage."

[77] (U) Hadas Gold, "China is mobilizing its global media machine in the coronavirus war of words," CNN Business, May 15, 2020.
For additional information on the structure of China's propaganda apparatus, see: David Shambaugh, "China's Propaganda System: Institutions, Processes and Efficacy," *The China Journal,* no. 57, January 2007, 25-58.

(U) In addition to an uptick in overt public diplomacy activity, China has also begun to engage in coordinated inauthentic online behavior and activities to covertly and overtly shape public discourse on topics of importance to the CCP. In the midst of the Hong Kong protests in August 2019, Facebook, Twitter, and YouTube all identified and removed a series of accounts (including likely "bots"), pages, networks, and channels that were engaged in coordinated inauthentic behavior and disinformation operations targeting the Hong Kong protests.[78] This marked the first large-scale takedown of a suspected Chinese state-backed influence operation online. Subsequent open-source analyses of the associated Twitter accounts demonstrated that Chinese actors likely began building this network in early 2017, soon after the U.S. presidential election in 2016. These accounts were first deployed to denigrate Guo Wengui, a U.S.-based Chinese dissident who was targeted by a wide ranging PRC campaign in 2017, and then were subsequently used to criticize a series of December 2018 military veteran protests in the PRC, both of which were events of great political sensitivity to CCP leadership.[79]

(U) As China's propaganda and disinformation behavior and tools continue to advance and the U.S.-China relationship becomes increasingly contentious, Beijing's posture will likely continue to evolve in the coming months and years. Moreover, just as Beijing has assisted non-democratic states with the implementation of mass-surveillance systems, other aspiring authoritarian actors could seek to emulate these tactics.[80] The PRC's disinformation evolution—in conjunction with the multitude of foreign influence threats and state-backed disinformation activity emanating from Russia, Iran, and other adversaries—will set the stage for further assaults on the truth, damaging the United States' ability to advance its policies abroad and effectively engage with American citizens.

---

[78] (U) Kate Conger, "YouTube Disables 210 Channels that Spread Disinformation about Hong Kong Protests," The New York Times, August 26, 2019.
[79] (U) Daniel Wood, Sean McMinn, and Emily Feng, "China Used Twitter To Disrupt Hong Kong Protests, But Efforts Began Years Earlier," National Public Radio (NPR), September 17, 2019.
[80] (U) For information on the types of states that have imported the PRC's surveillance technology, see: Sheena Chestnut Greitens, "Dealing with Demand for China's Global Surveillance Exports," *Global China: Assessing China's Growing Role in the World,* The Brookings Institution, April 2020.

[redacted]

(U) China and the Intelligence Cycle

(U) The Committee's classified report is divided into chapters, each of which addresses a specific agency's performance throughout the "intelligence cycle" on China-related issues: planning, collection, processing, analysis, dissemination, and evaluation.[81] In conducting this assessment, the Committee took account of the activities of all intelligence community elements and all intelligence collection disciplines.[82]

(U) *Planning.* The Intelligence Community's primary customers include the President of the United States, his or her senior-most advisors, policymakers, warfighters, congressional officials, and other U.S. entities with a need-to-know. The Intelligence Community notes that, "the IC's issue coordinators interact with these officials to identify core concerns and information requirements. These needs, in turn, guide our collection strategies and allow us to produce appropriate intelligence products.[83]" Accordingly, the Committee assessed: Who are the U.S. decision-makers with core concerns and information requirements related to the China mission? How do these individuals convey their requirements to the intelligence community? How does the intelligence community subsequently prioritize these requests?

(U) *Collection.* The Intelligence Community employs numerous collection disciplines to gather information, including human intelligence, signals intelligence, geospatial intelligence, measures and signatures intelligence, and open source intelligence. With respect to the China mission, the Committee sought to identify: Is the IC executing an effective collection strategy? Does it address defined requirements in a timely fashion? Is the IC ensuring that collection requirements are met using appropriate collection methods? Is ongoing collection lawful? Does the intelligence community's collection posture appropriately manage risk? Are collection processes sufficiently resilient and innovative?

[81] (U) "How the IC Works," Intel.gov, January 3, 2020, www.intelligence.gov/how-the-ic-works#start.
[82] (U) Collection disciplines include: geospatial intelligence (GEOINT), human-source intelligence (HUMINT), imagery intelligence (IMINT), measurement and signals intelligence (MASINT), open-source intelligence (OINT), and signals intelligence (SIGINT).
[83] (U) "How the IC Works," Planning, Intel.gov, January 3, 2020, www.intelligence.gov/how-the-ic-works#start.

[redacted]

[redacted]

(U) *Processing.* Following the collection of intelligence, acquired information is processed for consumption. With the advent of big data, "the collection stage of the intelligence cycle can yield large amounts of data that require organization and refinement," creating added technical challenges to IC officers.[84] The Committee assessed: Is collected intelligence converted to a digestible format in a timely fashion? Is raw intelligence reporting stored in accessible locations? Are intelligence community processing techniques on par, or superior, to comparable commercial capabilities?

(U) *Analysis.* After intelligence is processed, all-source analysts are responsible for aggregating disparate streams of information from multiple collection sources to formulate complete analytic products. Analysts are expected to demonstrate in-depth subject-matter knowledge on their area of focus and identify intelligence gaps to inform future collection priorities.[85] Within the IC's China-focused analytic program, the Committee sought to identify: How are analytic production priorities developed? Are IC analysts able to effectively meet customer requirements within the decision-making cycle? Does the IC have sufficient analytic knowledge management practices in place? Do all-source analytic elements effectively coordinate and prioritize their production?

(U) *Dissemination.* Following the creation of analytic products, "finished intelligence is delivered to policymakers, military leaders, and other senior government leaders who then make decisions based on the information.[86]" Within this stage of the intelligence cycle, the Committee assessed: Do decision-makers receive raw and finished intelligence products relevant to their area of responsibility within a timely fashion? Are U.S. government officials with a "need-to-know" cleared into the appropriate compartmented streams of intelligence? Do IC customers possess the appropriate IT equipment to access intelligence required to effectively perform their job duties?

(U) *Evaluation.* After customers have reviewed intelligence products, they provide feedback to IC officers, which can generate new or refined intelligence requirements.[87] The Committee

[84] (U) "How the IC Works," Processing, Intel.gov, January 3, 2020, www.intelligence.gov/how-the-ic-works#start.
[85] (U) "How the IC Works," Analysis, Intel.gov, January 3, 2020, www.intelligence.gov/how-the-ic-works#start.
[86] (U) "How the IC Works," Dissemination, Intel.gov, January 3, 2020, www.intelligence.gov/how-the-ic-works#start.
[87] (U) "How the IC Works," Evaluation, Intel.gov, January 3, 2020, www.intelligence.gov/how-the-ic-works#start.

[redacted]

assessed: Do these individuals have a reliable and effective means of providing evaluative feedback to the intelligence community? How do IC analysts and briefers share feedback with core collectors? What measures of effectiveness does the IC use to capture added value to the decision-making cycle?

[redacted]

(U) Key Findings

(U) Following the Committee's evaluation of the Intelligence Community's performance in the key areas noted above, the Committee has developed the following set of unclassified key findings. While the Committee's review was scoped to assess the IC's efforts against the China target, some of its findings address not merely China, but also broader issues foundational to the IC's structure and continued ability to operate in a 21st century environment—an environment shaped by the ravages of COVID-19.

1. (U/[redacted]) Intelligence Community [redacted] compete with China. Absent a significant realignment of resources, the U.S. government will fail to achieve the outcomes required to enable U.S. competition with China on the global stage.

2. (U) The Intelligence Community places insufficient emphasis and focus on "soft," often interconnected long-term national security threats, such as infectious diseases of pandemic potential and climate change, and such threats' macroeconomic impacts on U.S. national security. This could jeopardize the future relevance of the Intelligence Community's analysis to policymakers on certain long-range challenges, particularly given the growing importance of these policy challenges to decision-makers and the public and the devastating impact of the current pandemic on U.S. national life..

3. (U) The Intelligence Community has failed to fully achieve the integration objectives outlined in the 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA) for targets and topics unrelated to counterterrorism.

4. (U/[redacted]) The Intelligence Community is struggling to adapt to the increasing availability and commodification of data, [redacted]

[redacted]

[redacted]

5. (U) The increasing pace of global events, fueled by the rise of social media and mobile communications, will continue to stress the IC's ability to provide timely and accurate analysis within customers' decision-making window.

6. (U) The future successful application of artificial intelligence, machine learning, and other advanced analytic techniques will be integral enablers for the U.S. national security enterprise. Conversely, there is a high degree of strategic risk associated with stasis and a failure to modernize.

7. (U/[redacted]) Existing intelligence requirement prioritization mechanisms [redacted] particularly with respect to decision-makers outside of the Department of Defense.

(U) The following set of unclassified findings address items of specific relevance to the China target, and are divided into enabling factors and the six phases of the intelligence cycle:

(U) *Enabling*

1. [redacted] There is [redacted] familiarity and expertise on China issues [redacted]

2. (U/[redacted]) Security clearance adjudication policies [redacted] with substantive expertise on China [redacted]

3. (U/[redacted]) Given the range of functional issues associated with high-quality collection and analysis on China, an effective and well-rounded IC workforce requires [redacted]

[redacted]

[redacted]

[redacted]

(U) *Planning*

4. (U) The multidimensional nature of the challenge that China presents requires an enhanced focus on non-defense intelligence, particularly strategic analysis in support of the Department of State, Department of Treasury, Department of Commerce, Department of Homeland Security, U.S. health and disaster preparedness agencies, and other domestic agencies who have not historically been primary customers of the intelligence community. Additional work to define detailed key requirements for non-defense customers would support more effective policy responses for matters such as future disease outbreaks, trade negotiations, and visa application determinations.

5. (U) As China continues to expand its global influence, policymakers will continue to require high-quality analysis on third-countries' own national priorities.

(U) *Collection*

6. [redacted] challenge the intelligence community's ability to [redacted]

7. [redacted] open source intelligence (OSINT) will become increasingly indispensable to the formulation of analytic products. [redacted]

[redacted]

[redacted]

8. (U/[redacted]) The U.S. intelligence community has [redacted] transnational issues outside of the conventional definition of national security, [redacted]

(U) *Processing*

9. (U) Encrypted communications will continue to stress the United States' signals intelligence architecture.

(U) *Analysis*

10. [redacted] The U.S. government must prioritize developing [redacted]

11. [redacted] Existing procedures for analytic production [redacted]

(U) *Dissemination*

12. (U) The compartmentation of intelligence limits decision-makers' ability to develop a common understanding of China's intent, actions, and likely future behavior.

13. [redacted] likely limits the

[redacted]

[redacted]

timely dissemination of intelligence [redacted]

(U) *Evaluation*

14. (U) The U.S. government should strengthen its ability to categorize, disrupt, and deter the totality Chinese influence operations occurring on U.S. soil.

15. (U/[redacted]) State-backed Chinese cyber operators will continue to pose additional risks to "soft targets" of direct relevance to the U.S. national security enterprise. [redacted]

16. [redacted]

(U) Recommendations

(U) The key findings identified above raise profound questions about the structure, priorities, tradecraft, and funding profile of the Intelligence Community. While the recommendations below will not address all of this report's findings, the Committee is dedicated to working with the IC in order to take the steps necessary to achieve progress.

(U) The following unclassified Committee recommendations are significant and relevant to the governance of and authorities afforded to the IC:

1. (U) The Committee recommends the creation of a bipartisan, bicameral congressional study group to evaluate the current organization of and authorities provided to the intelligence community, with the express goal of making necessary reforms to the National Security Act of 1947 and the Intelligence Reform and Preventing Terrorism Act (IRPTA) of 2004.

[redacted]

[redacted]

2. (U) The Executive Branch, in consultation with congressional intelligence and appropriations committees, must undertake a zero-based review of all intelligence program expenditures, assess the programs' continued relevance to forward-looking mission sets, such as the increased relevance of "soft" transnational threats and continued competition with China, and take immediate corrective action to align taxpayer resources in support of strategic requirements.

3. (U) An external entity should conduct a formal review of the governance of open-source intelligence (OSINT) within the intelligence community, and submit to congressional intelligence and appropriations committees a proposal to streamline and strengthen U.S. government capabilities.

4. (U) The Office of the Director of National Intelligence (ODNI) should identify shared artificial intelligence and machine learning (AI/ML) use cases across the intelligence community and use the its coordinating and budgetary authorities to consolidate spending, expertise, and data around shared community-wide AI/ML capabilities.

(U) The below unclassified recommendations are of direct relevance to the intelligence community's capabilities vis-à-vis the China target:

(U) *Enabling*

1. (U/[redacted]) ODNI should strengthen its ability to effectively track [redacted]

2. (U/[redacted]) The IC should [redacted] existing intelligence collection prioritization frameworks, particularly to inform resource allocation decisions.

3. (U) The IC should formalize and broaden programs designed to mentor the next generation of China analysts. Agencies should leverage best practices from across the

[redacted]

[redacted]

community, and develop internal Senior Steering Groups to prioritize investments in specific China-focused programs.

4. [redacted] The IC should conduct a review of security clearance adjudication policies surrounding [redacted]

5. (U/[redacted]) If an officer possesses critical skills relevant to China mission-set, such as proficiency in Mandarin Chinese, the Intelligence Community should [redacted]

6. (U) The IC should engage in a dialogue with the U.S. Department of Education on the requirements for the future of the U.S. national security workforce.

7. (U/[redacted]) The Intelligence Community should codify and nurture cadres of officers with China-focused expertise [redacted]

8. (U) The U.S. should expand its diplomatic, economic, and defense presence in the Indo-Pacific region, to include in the Pacific Island Countries and Southeast Asia.

9. (U) The IC should consider developing a series of reskilling programs to leverage existing talent and expertise previously cultivated in counterterrorism programs.

(U) *Planning*

[redacted]

[redacted]

10. (U) The IC should streamline China-focused reporting across regional areas of responsibility.

11. (U) The IC should leverage lessons learned from providing support to the counterterrorism mission in order to identify ways in which it can embed real-time support to customers, especially those located outside of the Department of Defense, such as the Department of State, the United States Trade Representative, or U.S. health and disaster preparedness agencies.

12. (U) In recognition of the growing importance of economic and policy agencies to the overall success of the U.S. government's approach to China, the intelligence community should develop plans to increase analytic support to, or otherwise ensure consistent, agile communications and appropriate interactions with, non-traditional agencies, such as the Department of Commerce, the Department of Homeland Security, the National Science Foundation, the Department of Education, and U.S. public health agencies.

(U) *Collection*

13. (U) The IC should prioritize transferring successful "seed-funded" efforts to base funding as soon as practical to protect funding streams designated for innovation.

14. [redacted] The IC should more effectively integrate publicly available information, [redacted] The IC should seek to develop [redacted]

15. (U) The IC should conduct a review of systems and programs currently sustained by counterterrorism funding, but supporting other missions, and realign these programs to the appropriate expenditure centers.

[redacted]

[redacted]

16. (U) The ODNI should execute additional oversight of IC agencies' application of scarce resources to deconflict and reduce redundancies.

(U) *Processing*

17. [redacted] The IC should create a permanent capability [redacted]

18. (U) The IC should promote better data-sharing across the U.S. government between IC elements and non-defense agencies to inform CFIUS, sanctions, and supply chain risk management processes.

19. [redacted] The IC should prioritize developing [redacted]

20. [redacted] The IC should enhance its efforts to analyze [redacted]

(U) *Analysis*

21. (U) The IC should better align analytic resources to support diplomatic, political, economic, and global health decision-making within the U.S. federal government.

[redacted]

[redacted]

22. (U) Each Combatant Command should employ at least one subject-matter expert with previous China-focused experience to serve as a resident China analyst.

23. (U/[redacted]) The National Intelligence Council (NIC) should take a more active role in working with IC elements to strategically align [redacted] This will eliminate potentially duplicative analytic production, thereby creating additional capacity for analysis [redacted]

24. (U) The NIC should prioritize analytic questions of highest relevance to customers, not necessarily those questions that the IC might be most capable of answering with high-confidence.

25. (U) The IC should consider expanding opportunities for their analysts to complete joint duty assignments (JDAs) throughout the community.

26. (U) The IC should expand its practice of hiring technical experts, such as trained health professionals, economists, and technologists, to serve throughout the community's analytic corps. In light of such niche fields, these individuals should be permitted to narrowly specialize and carve out distinct career paths without hindering their promotion potential.

(U) *Dissemination*

27. (U) The NIC should endeavor to write and disseminate analytic products at the lowest appropriate classification levels; however, analytic products should also not prioritize releasability at the expense of sensitive intelligence analysis, particularly when compartmented analysis significantly contributes to the national security enterprise's understanding of a particular issue.

[redacted]

[redacted]

28. (U/[redacted]) The IC should conduct a zero-based review of the allocation of all [redacted]

29. (U/[redacted]) The IC and its customers should prioritize [redacted]

(U) *Evaluation*

30. (U) IC Chief Human Capital Officers should seek to ensure that IC officers receive maximum exposure to decision-makers. Subsequently, IC officers should more effectively share policymaker guidance throughout communities with a need-to-know.

31. (U) The IC, in consultation with DOD and its customer base, should develop a baseline understanding of *both* defense and non-defense indications and warnings. Non-defense indications and warning should include robust indicators of the emergence of transnational events of global concern, such as the emergence of an infectious disease with pandemic potential, or profound environmental degradation.

32. (U) The IC should develop more robust feedback mechanisms with nontraditional customers outside of the national security apparatus, particularly those with responsibility for economic and global health security issues, to ensure that the IC remains responsive to decision-maker needs.

[redacted]