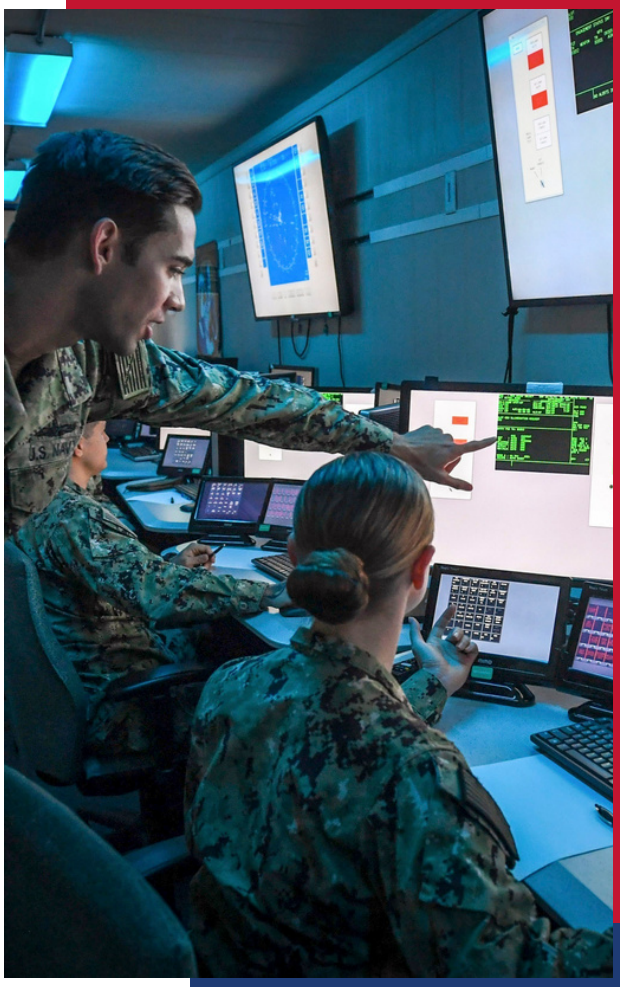
October 2023

CODE WAR: How China's AI Ambitions Threaten U.S. National Security

PERSPECTIVE



American Security Project

In Brief:

China's aggressive pursuit of artificial intelligence harkens a future where bytes and algorithms challenge traditional battlefield superiority. Through overt and covert centralization of foreign technology and expertise, dual-use artificial intelligence tools flow uninterrupted from America's commercial sector into China's state security, intelligence, and defense agencies. If the U.S. government doesn't set guardrails now, American firms pursuing lucrative Chinese markets may vanguard the Chinese Communist Party's transition to fifth-generation warfare. This report explores China's technocratic vision, its militarization of civilian and commercial infrastructure, and how U.S. firms are advancing its national security goals.

IN THIS REPORT

About the Author

Courtney Manning is a National Security Research Fellow at the American Security Project. She currently leads ASP's research portfolios on military recruitment and readiness, strategic competition with China, and emerging technology risks. Before ASP, she worked as a consultant on international human rights law, geopolitical risk, and climate security in New York and spent seven years in public sector nutrition analysis. She holds an M.I.A. in international security policy from Columbia University and a B.A. in international relations from the University of Denver.

Introduction

Against the impending global disruption of artificial intelligence, some members of Congress claim they are ill-equipped to prevent new and destabilizing technologies from jeopardizing national security. "When you look at the record of Congress in dealing with innovation, technology, and rapid change," stated Sen. Dick Durbin in May, "We're not designed for that."[1] "We're still in the early days of understanding how AI systems work and how to effectively govern them," stated Rep. Zoe Lofgren in a House hearing.[2] One month later, Sen. Ted Cruz told *Politico*, "To be honest, Congress doesn't know what the hell it's doing in this area."[3]

Innovations in critical sectors will continue to outpace comprehension of their long-term implications. While policymakers debate whether it's possible to stay abreast of new developments, artificial intelligence is impacting warfare outcomes in Ukraine, Syria, and Yemen. American individuals and firms are having their intellectual property adapted for use in political oppression, mass surveillance, and information warfare. Revisionist states are exploiting the inaction of U.S. policymakers to violate global laws and norms, infiltrate American firms and networks, and develop advanced weaponry targeted at the United States and its allies. Ignorance of the science behind emerging technologies is no longer an excuse to delay mitigation of these risks.

U.S. Airmen on patrol with a Boston Dynamics Spot robot.[a]

As discourse on AI gains nuance, one threat is apparent. Chinese Communist Party (CCP) is several years into its whole-of-government plan to militarize American technology and expertise to achieve its strategic aims. Artificial intelligence siphoned from China's international and commercial partnerships is being leveraged to oppress ethnic minorities, control foreign critical infrastructure, and conduct pervasive espionage against American individuals and firms. While some companies are scaling back their investments, prominent United States firms at the cutting edge of global artificial intelligence have increased their commercial and academic partnerships in Beijing, contributing to universities and firms with a federal obligation to support the CCP's military development and strategic goals.

Critical technology innovations will continue to outpace comprehension of their implications. Wittingly or unwittingly, U.S.-China partnerships in strategic sectors compromise U.S. national security and will only escalate without immediate intervention by U.S. legislators. It is possible and necessary for the Department of Defense and Congress to oversee research and development, introduce ethical and responsible legislation, and enforce auditing and oversight mechanisms of artificial intelligence technologies with explicit military capabilities. If roadblocks are not applied now, American AI innovators may be the vanguards leading the Chinese Communist Party's transition to fifth-generation warfare.

A Note on Defining AI: In this paper, the term artificial intelligence (AI) denotes deep learning systems that rapidly and autonomously identify patterns across large sets of data.[4] As trend detection and data analysis are universal tasks across disciplines, machine learning algorithms serve as force multipliers of cognitive processing.[5] One application of deep learning is generative AI, which is trained to produce sophisticated text, audio, and visual outputs based on human inputs.

China's Informatized Warfare Objectives

Global leadership in critical technologies has been a focal point of China's national security strategy since General Secretary Xi Jinping took office in 2013. Through a combination of technonationalism and developmentalism, Xi's Innovation-Driven Development Plan catalyzed a transition "from mechanization to informatization" of China's state security apparatus.[6] The first phase of Xi's "informatized" warfare incorporates information and communications-based technologies (ICT) into conventional weapons and tactics. The second is a paradigm shift to fifth-generation warfare tactics such as cyber attacks, espionage, psychological warfare, and autonomous weapons.[7]

U.S. Sailors using augmented reality AI for navigation.

The Chinese Communist Party aims to lead the world in new artificial intelligence developments by 2030.[8] Through strategic investments in artificial intelligence, the CCP aims to attain "intelligence supremacy": complete command and control over the global information space. This one-way innovation flow will enable China to "leapfrog" the technological advancement of the United States, establish control over foreign claimed territories, and secure global leadership in innovation and cognition. According to PLA spokespersons, "Once intelligence supremacy is lost, supremacy of other spaces is meaningless."[9]

Meeting this goal requires massive state investment in critical technology acquisition and new policies centered on artificial intelligence. These activities are centralized within three state initiatives:

1. **Indigenous innovation**: the transition from reliance on foreign technology to state-subsidized research and development (R&D).
2. **Military intelligentization**: the integration of AI and other information technologies into conventional weapons, strategy and tactics.
3. **Civil-military fusion**: the transfer of technologies from international markets and commercial entities into China's state security apparatus.

Key Advancements and Advantages

China's potential realization of fifth-generation warfare is amplified by its ambitious, whole-of-state investment in artificial intelligence. The following sections evaluate how Beijing's proportional spending on research and development, early release of regulations and roadmaps, centralization of foreign and civilian innovations, and sanction of illicit and grey-zone tactics give it an advantage in the global race for AI.

State Spending

The CCP is granted absolute authority and autonomy over the nation's economic priorities, enabling high state spending in niche areas. As a result, China's proportional defense spending on artificial intelligence greatly exceeds that of the United States. Research by the Center for Security and Emerging Technology suggests that the PLA spent between $1.6 and $2.7 billion, or about 1.2% of their annual defense budget, on artificial intelligence in 2020.[10] That same year, the U.S. Department of Defense (DoD) spent between $800 million and $1.3 billion on AI, one-tenth of China's proportional defense spending.[11] Looking ahead, the DoD's FY24 budget request for AI initiatives is approximately $1.8 billion.[12] China's AI industry—which its military and intelligence agencies are able to siphon from without the consent of foreign firms and benefactors—is projected to reach $14.75 billion.[13]

Early Regulations

China's early release of regulatory policies provides a "first-mover" advantage in setting global AI norms. From 2012 to 2017, Xi Jinping raised the proportion of emerging industry technocrats in provincial positions from less than 20% to 62%.[14] As a result, China's New Generation Artificial Intelligence Development Plan met or exceeded the sophistication and precision of the Obama Administration's Artificial Intelligence Research and Development Strategic Plan.[15] Years before the European Union's AI Act and NIST's AI Risk Management Framework, the Cyberspace Administration of China (CAC) established regulations on AI externalities affecting deep synthesis and generative AI.[16] These policies will inevitably influence global norms, beginning with the 120 countries for whom China is their primary trading partner.[17]

Foreign Investment

Despite its research activities being significantly less transparent than global standards, Chinese companies secure around 60% of the world's funding in an AI research and development market that exceeds $281 billion.[18] China's lead in 37 of 44 technologies considered "critical" and "emerging" allows it to create strangleholds within global defense, space, and communications supply chains.[19] Amplified by the CCP's cooperative agreements throughout the Indo-Pacific region and its position as a major provider of ICT infrastructure in Latin America and Africa, global dependence on China's information and communications exports is rapidly expanding.[20]

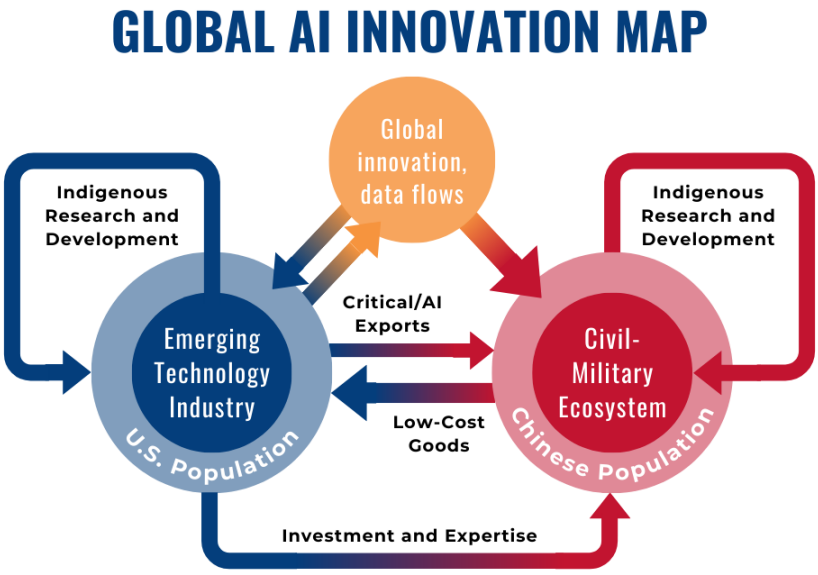


Figure 1. China's data localization policies affect global innovation flows.

Data Localization

Despite benefiting from global information sharing networks cultivated by the U.S. and its allies, China's national security ecosystem localizes and militarizes new innovations (fig. 1). While more than 20% of Chinese authors of high-impact research papers obtained post-graduate education in a Five-Eyes country, the CCP's 2017 Cybersecurity Law and 2021 Data Security Law mandate that all data stored in China—plus all foreign data pertaining to Chinese national security—must be transferred to the CCP.[21] Research and development in China cannot be shared with foreign actors and is exported only under strict controls. As a result, American and other foreign innovators receive fewer reciprocal benefits from their U.S.-China collaborations, slowing the global pace of innovation and giving Beijing the upper hand.[22] Foreign critical technologies are categorized as national security assets and used for military purposes in violation of U.S.-China trade agreements, leading to U.S. tariffs in 2018 and 2023.[23]

Asymmetric Steps

Xi Jinping sanctions the use of "asymmetric steps" to realize his technonationalist ambitions. Derived from normative Marxist beliefs about rectifying imperialist and capitalist exploitation, "asymmetric steps" comprise both the licit and illicit activities that enable weaker states to overcome the advantages of the West.[24] Examples of this "whole nation" approach include cyber operations, technology transfer programs, poaching technical experts from U.S. firms and universities, and economic espionage, among other grey-zone activities.[25] The impact of Chinese economic espionage on the U.S. economy has been conservatively estimated at $320 billion annually.[26]

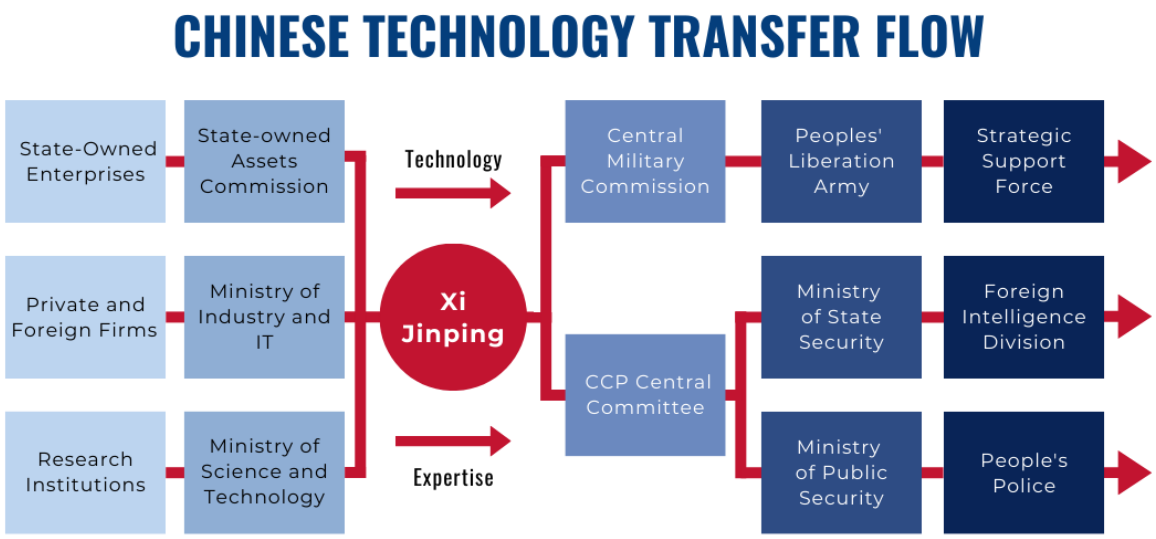


Figure 2. The CCP transfers technology and expertise from its firms and institutions to its defense and security agencies.

China's Civil-Military Technology Pipeline

The Chinese Communist Party grants itself the right to transfer indigenous intelligence technologies from all commercial activities in China.[27] Critical ICT—including artificial intelligence expertise and proprietary technology—is seized and designated a national security asset (fig. 2). In addition to providing strategic economic advantages, this ICT is utilized by The People's Liberation Army, Ministry of State Security, and Ministry of Public Security to facilitate international mass surveillance as well as domestic mass incarceration, forced labor, and "re-education" programs targeting Uyghur and other ethnic minorities.

American technology companies operating in or seeking to access the Chinese market do so at significant risk to their proprietary technologies and to U.S. national security. It is impossible to guarantee that high-tech intellectual property will not be seized by the CCP, enabling it to benefit from the technological advantages held by the United States while bypassing the research and development costs that would otherwise be incurred. Despite this, technology companies continue to comply with new restrictions to access Chinese markets. To facilitate state adoption of its Windows 10 operating system, Microsoft entered a joint venture to modify the software in 2016.[28] In 2018, Google attempted to develop a censored Chinese search engine but had to cancel the program due to security and privacy concerns.[29] In partnership with Alibaba in 2023, Meta modified its AI model Llama2 to "adhere to the core values of socialism" and "not generate incitement to subvert state power, overthrow the socialist system, endanger national security and interests, damage national image, incite secession, [or] undermine national unity and social stability."[30]

The Impact of State-Owned Enterprises

As Chinese firms receive preferential treatment in state financing and subsidy regimes, it is financially lucrative and logistically preferable to partner with state-owned enterprises (SOE) that facilitate civil-military fusion avoid adverse effects on commercial operations. In some industries, such as telecommunications, partnering with domestic enterprises is the only option for foreign firms to enter the Chinese market.

The State-Owned Asset Supervision and Administration Commission (SASAC) oversees China's major industries and invests in strategic economic sectors, including bioengineering, critical minerals, and artificial intelligence. The largest economic entity in the world, SASAC governs 97 state-owned enterprises with $30 trillion in combined assets.[31] SOEs under SASAC receive preferential lines of credit, increased public sector investment, and greater legal protections than private enterprises. In return, Beijing requires its SOEs to support its defense institutions and further its national security and development strategies.

SASAC Xibianmen Office entrance. Photo by N509FZ.

Due to the size and centralization of SASAC, American technology companies seeking to access the Chinese market must choose between partnering with private firms whose market penetration is federally restricted and whose freedoms are increasingly limited or large centrally owned entities that support the CCP's national security regime, including its mass surveillance and incarceration of ethnic minority populations (fig. 3). As a result, President Donald Trump and President Joe Biden each signed executive orders limiting investments in government-controlled and dual-use enterprises, including SOE partners of large American firms.[32]

Case Study 1: China's Regulatory Minefield

In 2013, the private enterprise VNET Group, Inc. (VNET) became Microsoft's exclusive operator of Cloud computing platforms in China. VNET limited CCP interference by registering as a holding company in the Cayman Islands, where it wholly owned and controlled Chinese telecommunications subsidiaries.[33]

In 2016, the CCP announced that foreign investors were prohibited from owning or controlling domestic telecommunication services. VNET complied by drafting exclusive contracts with the firms it had previously managed, reducing the risk of proprietary data transfer by holding 100% of its subsidiaries' equity interests.[34]

In 2021, the CCP prohibited foreign-based entities from owning more than a 50% equity interest in any PRC company engaging in value-added telecommunications businesses.[35] VNET and Microsoft were now limited in their ability to mitigate the intrusion of the Chinese state into VNET's operations and, by extension, Microsoft's proprietary technologies. However, VNET restructured again to comply with the new regulations by reducing its equity interest in its subsidiaries and variable interest entities.[36]

In 2022, the CCP's revised Cybersecurity Review Measures granted the CAC the authority to conduct cybersecurity reviews of ICT companies operating in China for national security purposes, including those based abroad.[37] The CCP did not specify which national security issues were grounds for review, granting itself broad authority to investigate, freeze, and seize ICT at any time and at its own discretion. If firms find new loopholes, they are likely to be closed by the state. As VNET's 2023 annual equity filing states, "government authorities have broad discretion in interpreting and applying PRC laws and regulations… which may not be published on a timely basis or at all, and which may have a retroactive effect."[38]

U.S.-China Artificial Intelligence Partnerships

Through research, investment, sales, and other ventures, foreign firms wittingly and unwittingly facilitate the CCP's civil-military fusion program. As illustrated in Case Study 1, even private firms willing to frequently and significantly alter their business model to accommodate their Western partners are unable to protect them from state interference. The following sections explore how American technology corporations enable the transfer of advanced and dual-use ICT services to China's security apparatus.

Microsoft Corporation

Microsoft is a major supplier of technology services to the U.S. government, receiving over $404 million from the Department of Defense in 2022.[39] In addition to AI development, it oversees the Navy's Flank Speed enterprises, the DoD Joint Warfighting Cloud Capability, and the Defense Information Systems Agency's Top Secret and other classified data.[40] Considering its strategic partnerships with Lockheed Martin, Raytheon Technologies, and Oshkosh, Microsoft has access to the U.S. military's most critical defense technologies and intelligence.

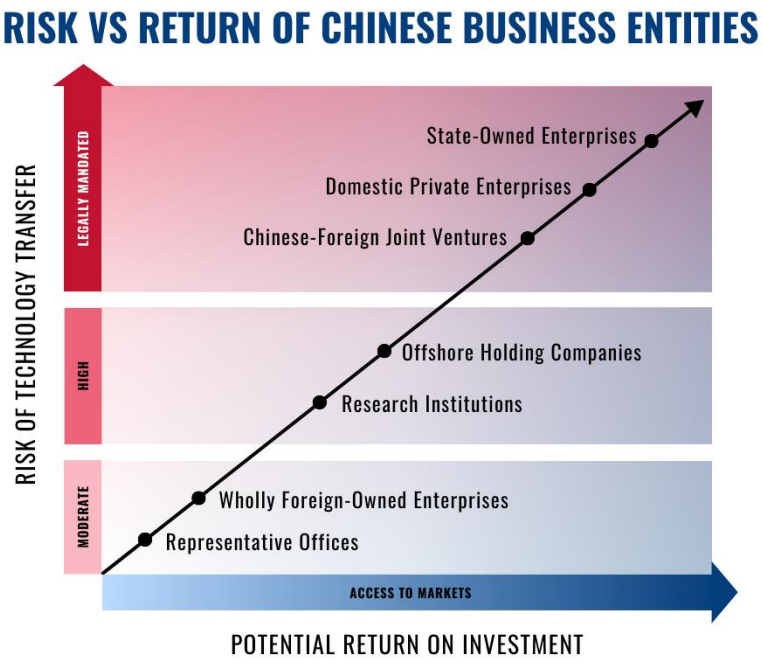


Figure 3. Tradeoffs between access to markets and tech transfer risk in China.

Microsoft also has deep historical ties to China's AI industry.[41] China is the second-largest market for Microsoft's ICT; through its cloud platform Azure PRC and its SOE partner China Mobile, over 900 million Chinese subscribers receive most of the same AI tools as those in the United States.[42] This includes those designed by ChatGPT creator OpenAI, which does not operate in China directly.[43] Over 10,000 employees in China—at least 3,000 of which focus on AI development—provide an extensive and strategic interface for the import of American AI knowledge and experience to the Chinese state.[44] Microsoft plans to double employees in some locations by 2025.[45]

Unlike its Windows 10 agreement, Microsoft's artificial intelligence exports in China are cutting-edge to compete with state-sponsored competitors.[46] These technologies are implemented in what Microsoft calls "specialized fields," including security, defense, and intelligence. One partner, China Electronics Technology Group Corporation (CETC), uses Microsoft's Cloud AI to engineer national military and civil ICT systems used in the oppression of Uyghur minorities.[47] Another, China Telecom, supports AI-empowered mass surveillance technologies and services in Xinjiang, which led to widespread cuts in mobile services for Uyghurs in 2015.[48] In 2019, it was discovered that Microsoft had worked with a Chinese military university to research AI used for surveillance and censorship, enabling the transfer of AI-empowered software, hardware, and other dual-use technology to Beijing in the process.[49]

In 2018, Microsoft signed a strategic partnership agreement to bring advanced AI and machine learning capabilities to the PRC's top drone manufacturer, Shenzhen DJI Innovation Technology Co. (DJI).[50] Microsoft Azure's AI and machine learning was integrated with DJI hardware to "provide real-time data transfer and turn vast quantities of aerial imagery and video data into actionable insights," ostensibly for commercial use.[51] In February 2022, the Washington Post uncovered multiple state- and defense-backed investments in DJI, despite the company's claims to the contrary.[52] In October 2022, the U.S. government sanctioned DJI for its obfuscated ties to the Chinese military.[53]

Case Study 2: Research and Development Trojan Horses

China has thirty national artificial intelligence research institutions.[54] Some, like the Ministry of National Defense Artificial Intelligence Research Centre and Unmanned Systems Research Centre, overtly develop AI applications for warfare. Others are ostensibly academic. According to its website, the Beijing Academy of Artificial Intelligence (BAAI) is a "non-profit, non-government, neutrally positioned" research institution envisioned by Zhang Hongjiang, former managing director of Microsoft Advanced Technology Center, to "benefit people and the planet."[55]

According to Chinese media reports, however, BAAI was created by the Ministry of Science and Technology and the Beijing Municipal Government under the CCP's Zhiyuan Action Plan.[56] The Action Plan, which also funds the Shanghai World AI Conference headlined by Elon Musk and Jack Ma in 2019, was introduced to absorb foreign expertise and innovation into the Chinese state and reduce brain drain of Chinese scientists abroad by creating attractive facsimiles of American-based research labs and conferences.[57]

The CCP's strategy is working. In a 2019 Twitter post, Meta Vice President and Chief AI scientist Yann LeCun supported BAAI by stating, "The Beijing Academy of Artificial Intelligence publishes AI ethics guidelines. Yes, the protection of individual privacy is mentioned."[58] He has since been an invited guest multiple times, and as of 2023, BAAI funders include Microsoft, Linux, and OpenAI.[59]

As a result of American financial support and expertise, Microsoft President Brad Smith noted that BAAI was only months behind Microsoft and Google in April.[60] Speaking at BAAI's annual conference in June, OpenAI CEO Sam Altman declared that "China has some of the best AI talent in the world."[61] Noting its abundance of funding, one journalist praised the BAAI for "avoiding commercial propaganda or gimmicky forums aimed at advertisers…despite the presence of renowned companies in the AI industry."[62]

Amazon Web Services

Amazon Web Services (AWS) is the primary artificial intelligence and cloud computing provider of the U.S. Department of Defense, receiving over $20 billion in contracts in 2022.[63] It simultaneously maintains several high-impact contracts with Chinese government partners. For example, Ningxia Western Cloud Data Technology Co., which is partially state-owned and partnered with U.S.-sanctioned Beijing Highlander, provides Amazon's services, including its Machine Images Deep Learning technology, to Zhongke Guangqi Space Information Technology Co. (CAS Space).[64] CAS Space provides remote sensing and satellite services for Chinese state and defense agencies and holds national records for satellite deployment, making it a lucrative business partner for an American AI firm.[65]

Providing courses and training in artificial intelligence and web service provision helps AWS carve a niche for its AI products in China. One of its academic partners is the training base for the Xinjiang Production and Construction Corps (XPCC), a paramilitary organization sanctioned by the U.S. government for its ties to human rights abuses in Xinjiang.[66] While ties to the CCP are frequently obfuscated to provide plausible deniability for sponsorship of abuses (fig. 4), XPCC's work includes "poverty alleviation" and "patriotic education"—terms used to refer to the forcible relocation, internment, and indoctrination of Uyghur and other ethnic minorities in China.

Another AWS partner, Nanjing Keji Data Technology Co, Ltd (KGDATA), provides cognitive intelligence application services to military end-users under its "AI+National Defense Military Industry Solution" program.[67] Its "full-cycle, graph-based intelligence application" was listed on the AWS Marketplace, and has "served dozens of government and military industries, major state-owned enterprises, and science and technology agencies" such as the PLA's National University of Defense Technology and SOE China Airspace and Science Technology Corporation.[68]

Meta Platforms, Inc.

Despite its products being banned in China since 2009, Meta has repeatedly attempted to court Chinese markets through significant investments in research, start-up funding, and partnerships with CCP entities. Despite not directly operating in China, Meta businesses and supply chains are embedded within the country, and Facebook's ad revenue is increasingly dependent on Chinese investors selling to the international market.[69]

Company founder and CEO Mark Zuckerberg has expressed criticism of the CCP's data policies and its ongoing intellectual property theft—yet Meta has been aggressively trying to break into the country since 2015, illustrating how the appeal of China's large domestic market offsets its security risks to American firms.[70] In 2018, Meta financed a $30 million dollar subsidiary in Hangzhou, which lasted six days until its approval was rescinded and its existence censored by the CCP.[71] Two years later, Zuckerberg stated that Meta and Beijing "could never come to an agreement on what it would take for us to operate there, and they never let us in" and that "it is well documented that the Chinese government steals technology from American companies."[72] Meta's consumer electronics hardware remains manufactured in China, despite reported attempts to diversify into Taiwan and Italy.[73]

Despite acquiring firms with U.S. military AI contracts, Meta retains deep connections with Chinese AI researchers working with the CCP.[74] Meta Vice President Yann LeCun has co-authored multiple papers on artificial intelligence with Professor Ma Yi from the Tsinghua-Berkely-Shenzhen Institute.[75] Ma, who also teaches at the University of California Berkeley, served as a senior advisor to the Bytedance Research Lab in Silicon Valley from 2017 to 2020. Bytedance Ltd. developed TikTok in China in 2016 and maintains strong ties to the Chinese Communist Party. Ma is also a distinguished scholar of the Thousand Talents Program, where he served from 2015 to 2017.[76] Overseen by CCP intelligence organizations, this program recruited professionals with access to overseas dual-use intelligence and pressured them to betray their nation in exchange for money or status in China.[77]

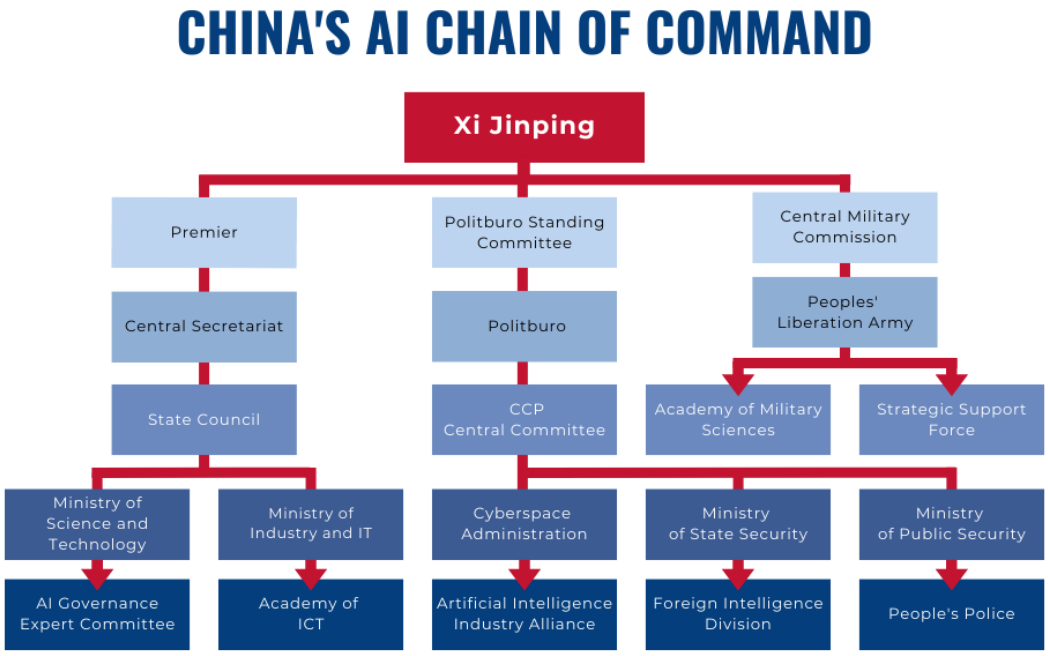


Figure 4. Most industry alliances and universities in China are directly governed by CCP offices.

Case Study 3: The Economic Espionage Cover-Up

Technical and industrial bottlenecks prevent China from attaining global leadership in multiple critical sectors. Chinese leaders are cognizant of the need to reverse brain drain and facilitate indigenous technology development but were historically reticent to cede control of these activities to non-state enterprises. As a result, the CCP tasked its Ministry of State Security with conducting hundreds of economic espionage operations targeting American and European technology firms to transfer proprietary documents, patents, and physical prototypes directly into the state's security apparatus.

The Ministry's heavy investment in espionage operations culminated in its United Front Work Department Thousand Talents Program (TTP) in 2008.[78] The program attracted technical experts from Five-Eyes countries with experience in ICT and other strategic sectors to China, ostensibly for awards, research grants, or academic collaborations. In reality, the Thousand Talents Program incentivized participants to steal trade secrets, break export control laws, and violate conflict-of-interest policies in exchange for wealth, status, or other rewards in China.[79] The Federal Bureau of Investigation published these findings in 2018 and as a result, the U.S. Senate Permanent Subcommittee on Investigations and Committee on Homeland Security and Governmental Affairs designated these programs a threat to U.S. national security one year later.[80]

After this controversy, the CCP removed American TTP members from official websites and rebranded the program as the "High-end Foreign Experts Recruitment Plan."[81] The rebranding signaled a shift to more obfuscated means of technology transfer that, combined with continued economic espionage against the U.S., has paid substantial dividends for the state. Ongoing partnerships with American and European ICT companies provide more opportunities than ever for licit and illicit activities to support CCP objectives.

Oracle Corporation

Oracle, the cloud provider for TikTok's U.S. operations, has built extensive artificial intelligence infrastructure throughout China and is deeply embedded in its public institutions.[82] Until it was sanctioned in 2019, Oracle maintained multiple collaborative agreements with major PRC enterprises such as Huawei and Tencent, through which it provided data services and facilitated artificial intelligence transfer to PRC government and state security entities.[83] Oracle remains a top U.S. Department of Defense contractor, securing up to $9 billion in grants last year.[84]

As reported by *The Intercept* in 2021, Oracle provides artificial intelligence software that allows Chinese police to conduct facial recognition and "criminal prediction," or the use of artificial intelligence technologies to predict whether someone is likely to commit a crime.[85] Government entities in Xinjiang, including the paramilitary XPCC, still use this and other Oracle artificial intelligence tools to conduct mass surveillance and incarceration.[86] In response to the report, Oracle executives stated that Oracle is not responsible for the misuse of its software and services.[87]

On its Chinese website, Oracle claims to maintain 24 offices throughout the PRC. Simultaneously, an announcement on its American website claims that its customers include "all five branches of the U.S. military" as well as NASA, the Department of Commerce, and the Central Intelligence Agency.[88] Despite the high risk of the CCP obtaining data belonging to the U.S. military apparatus through its data transfer regulations governing Oracle, cloud computing technology was left out of the Biden administration's November 2022 ban on artificial intelligence exports to China, leaving American defense technology and intelligence vulnerable to CCP penetration.[89] In August 2023, the Biden administration's Executive Order on AI Investments authorized the Secretary of the Treasury to regulate U.S. investments in Chinese artificial intelligence, including cloud computing technology, which may close this loophole.[90]

The Risks of China's Intelligent Security

In 2023, the Chinese Communist Party utilizes foreign artificial intelligence for surveillance, mass incarceration, forced labor, and "re-education" initiatives aimed at minority groups, political dissidents, and the general populace. American and multinational corporations create artificial intelligence applications used by Chinese state security and military entities, granting the CCP access to nearly identical software and hardware employed in United States government and military infrastructure. If left unchecked, these innovations in the hands of China and other adversary states will facilitate an erosion of democratic values, undercut global innovation, and destabilize international security.

To meet these goals and establish command and control over the global intelligence landscape, the CCP:[91]

1. Siphons foreign investment and expertise to bolster domestic research and development.
2. Integrates commercial AI innovations into its civil-military infrastructure through Civil-Military Fusion.
3. Exports Chinese AI technologies to states and leaders that share China's ideology and goals.

Autonomous Aerial Combat

American AI chips and software integrated within Chinese Unmanned Aerial Vehicles (UAV) grant the CCP an edge in both intelligence and warfare. AI-empowered CPI systems sold internationally improve radar performance by up to 46% and can instantaneously collect and share data with foreign ICT installations.[92] Seven Chinese firms have tested autonomous vehicles in California using these capabilities, exposing American civilians to surveillance risk.[93]

In combat, AI-empowered UAVs perform reconnaissance, jamming, obfuscation, and attacks at a fraction of the cost and risk of manned vehicles. Traditionally, military personnel program drone targets and flight paths; smart drones, however, make autonomous targeting decisions and rapidly adapt to factors such as weather conditions, air pressure, and aerial defenses.[94] While carrying heavy firepower can be challenging due to tradeoffs in weight and endurance, loitering UAVs can use lightweight or self-destructive munitions.[95] These drones, originally developed in Israel with American defense funding, continue to be supplied to China despite ongoing sanctions.[96]

U.S. Navy remote flight operations. Photo by Juan Sua.

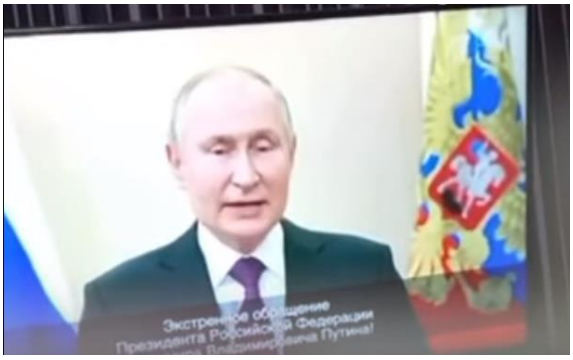
Smart drones do not need to be cutting-edge or military-grade to enact devastating attacks. Modern Chinese models reflect similar specifications as the 2009 Wing Loong I, which is still in use across Egypt, Libya, and Yemen.[97] While technologically inferior to their American counterparts, the Wing Loong II and III offer substantial cost savings and increased payload capacity.[98] These improvements have likely been bolstered by ongoing espionage activities that their SOE developer, China Aerospace Science and Technology Corp, has been implicated in since 2011.[99]

Adopting cutting-edge AI is often a simple matter of purchasing or replicating American products. Drones developed by Microsoft partner CETC and operated by the People's Liberation Army operate in coordinated groups known as "swarms" utilizing an AI chip based on an imported American model.[100] Jammers are ineffective against some of these UAVs, and recently installed U.S. aerial defense systems may not be fast enough to take them down.[101]

Exemplified in widespread use of DJI UAVs on both sides of the Ukraine war, even hobbyist Chinese drones can facilitate surveillance and reconnaissance and be modified to carry munitions and explosives.[102] In July, the Office of the Director of National Intelligence declared that China had shipped more than $12 million in drones and drone parts to Russia since its invasion of Ukraine, with independent auditors estimating these sales to be $32 million.[103] The resulting controversy prompted the CCP's first export controls on civilian drones on both sides of the Ukraine war, despite these drones contributing to ongoing destruction and loss of life in Yemen, Iraq, and Myanmar.[104]

Disinformation Brigades

Information warfare enables the Chinese Communist Party to exert greater control of its population and fight perceived "separatist movements" in Tibet, Taiwan, and Xinjiang. The Central Propaganda Department and United Front Work Department engineer whole-of-government influence campaigns to covertly promote CCP leaders and ideologies and undercut competing global narratives.[105] In a practice called astroturfing, thousands of false and impersonated individuals, organizations, and entities mimic grass-roots campaigns that influence both Chinese citizens and Americans.[106] In 2017, it was estimated that out of the 80.4 billion social media posts in Chinese online communities in 2013, 448 million were likely from state agents masquerading as domestic and foreign citizens.[107]



A deepfake of Russian President Vladamir Putin.

Foreign AI enables the CCP to enhance and broaden these campaigns. Programs trained on videos of celebrities, officials, and citizens can obscure state actors behind realistic virtual masks for as little as $30.[108] These tools have already been used by the CCP to create "deepfakes" of Americans criticizing the U.S. and lauding the Chinese state.[109] In the future, AI will be able to autonomously create highly divisive propaganda and misinformation campaigns that exploit search engine algorithms for maximum reach and impact.[110] As state-sponsored entities are exempted from China's AI regulations, no oversight mechanism governs these activities.[111]

Strategic Warfare Planning

Artificial intelligence algorithms will eventually provide a decisive advantage in both short-term battlefield tactics and long-term warfare strategy. The human brain processes an estimated 11 million bits of information every second and considers about 40 simultaneous parameters when making decisions.[112] ChatGPT-3 processes 500 billion bits and considers 175 billion parameters to generate its outputs.[113] While processing speed and input volume do not directly correlate with reasoning ability, AI's potential to exceed human cognition makes it a critical military investment.

Like other complex technologies, strategic algorithms increase potential points of failure on the battlefield. The success of AI integration within China's warfare planning capacity is unknown, as the People's Liberation Army has never engaged in a contemporary combined arms operation.[114] However, AI products trained on U.S. military data may anticipate challenges that Chinese strategists would otherwise overlook. Nearly all of the PLA's military AI chips are designed by U.S. defense contractors, granting China indirect access to U.S. military expertise and intelligence.[115]

Domestic and International Surveillance

China's "sharp eyes" surveillance regime is the most sophisticated in the world.[116] Facial recognition cameras have been installed in Xinjiang mosques since 2018.[117] In 2021, the Henan government expanded these activities to track journalists, international students, and women traveling illegally.[118] In 2022, over 50 similar contracts had been filed by different provinces.[119] Facial scans are stored in a database with details such as hair type, facial expressions, social status, gender, religion, and ethnicity.[120]

Surveillance cameras in Hong Kong. Photo by Steve Webel.

Chinese AI-empowered technologies also covertly infringe upon U.S. sovereignty. Over the past five years, China has injected eavesdropping equipment within American cellphone towers, cultural installations, and naval ports.[121] Surveillance operations have also been discovered in Cuba, Hawaii, Guam, and New York.[122] As a result of American advances in semiconductor and battery technology, miniaturized surveillance cameras will soon be undetectable without sophisticated equipment, enabling broad surveillance of U.S. citizens.

Cyber Attacks

The data China collects through mass surveillance is used to conduct malicious operations. In 2015, Chinese hackers stole 22 million security clearance files and 5.6 million fingerprints from the U.S. Office of Personnel Management.[123] In May 2023, CCP-sponsored hackers planted malicious scripts within ICT infrastructure in Guam.[124] China has not executed a destructive cyber attack on U.S. soil, but the Director of National Intelligence's 2023 Threat Assessment found that it is capable of doing so, with critical infrastructure like pipelines and rail systems particularly at risk.[125]

According to *Wired*, Chinese military-grade AI is being repurposed to conduct cyber-crimes against American citizens.[126] Deep learning algorithms trained on security clearance data can identify those with access to classified intelligence and target individuals who may be susceptible to spear-phishing campaigns. If successful, these activities could inject situationally-aware and adaptive AI malware into U.S. network systems and critical infrastructure.[127]

Strategic Recommendations

As all U.S.-China partnerships are vulnerable to militarization, targeted controls are insufficient to mitigate the risk of technology transfer. Conversely, widespread controls across multiple sectors may invite retaliation and cut off critical supply chains. To maintain leadership in AI without granting America's adversaries access to proprietary intelligence, the U.S. government should lock down military AI, invest in strong defenses, and promote ethical AI development.

Control Proliferation of Military Artificial Intelligence

Legislative loopholes allow American AI developers to bolster China's defenses, transferring U.S. government-funded military technology and expertise in the process. Some are simultaneously tasked with protecting classified intelligence, making them double targets. To cut the technology transfer pipeline, Congress must investigate the enmeshment of American cloud storage and AI contractors within China's AI ecosystem. As artificial intelligence is digitally stored, leaving it vulnerable to duplication and theft, AI with warfare capabilities should be federally classified. Finally, firms should be required by law to watermark and encrypt their dual-use AI software to deter unauthorized access.

The U.S. government must consider China's expansive intelligence ecosystem when making contractual agreements. To prevent military and dual-use AI from reaching foreign adversaries, American defense contractors cannot be permitted to operate within China's critical technology ecosystem. As the CCP grants itself the right to poach all foreign data in the name of "national security," clauses in DoD contracts should prevent defense contractors from engaging in AI collaborations with CCP-sponsored partners regardless of intent or place of origin.

Multinational companies and arms exporters can help devise new mechanisms to prevent misuse of AI technologies. However, as the tradeoffs for firms differ from those of the U.S. government, policymakers should give greater weight to recommendations from impartial experts and researchers. As demonstrated by the responses of large tech companies when faced with increasingly restrictive market conditions in China, the economic potential of large foreign markets often overpowers these firms' commitment to U.S. national security.

Invest in AI-Empowered Technological Defenses

Many AI-empowered military technologies in use today are offensive in nature. Innovations designed to penetrate, plan, and act autonomously tend to outpace technologies designed to prevent and defend against attack. As the private sector continues to develop new offensive and dual-use AI capabilities, the Department of Defense must make proportional, private investments in defensive AI that can counter weapons China may access through international markets. Three domains can leverage the global innovation landscape while ensuring protection from outside threats:

1. **Spatial computing:** Spatial awareness is critical to protect the U.S. from foreign threats. AI programs

integrated within satellites and other ICT installations can scan both the physical and digital landscape to attribute intrusions and rapidly alert authorities, making it difficult for adversaries to obscure their activities.

2. **Smart infrastructure:** Resilient ICT infrastructure absorbs social, digital, and physical shocks in the event of disruptions such as cyberattacks, infrastructure hacks, and phishing attempts. Education and training should be provided to at-risk groups on how to prevent penetrations and defend against attacks.
3. **Counter-adversarial defenses:** Smart software identifies and repairs network vulnerabilities and gaps before adversaries can exploit them.[128] Defensive AI capabilities, such as air defense systems, should be developed alongside their offensive counterparts to ensure sustained protection from AI-empowered weapons.

Promote Ethical and Inclusive AI Development

As China's operatives often target small states where the U.S. has installations, the U.S. and its regional partners must navigate the technological landscape together to forge strong defenses. The Department of State should extend cyber defense, counterintelligence, and technical translation assistance to smaller U.S. partners and non-aligned states to bridge information gaps and enable informed decision-making on the risks of working with the CCP. Allies should be trained to identify eavesdropping and other covert penetrations within their defense systems and infrastructure.

Wittingly or unwittingly, Chinese-foreign partnerships enable CCP access to American technologies and intelligence. In addition to bolstering China's military capacity, these partnerships jeopardize international security when Chinese firms sell military equipment on to operators in Russia, Iran, North Korea, and Syria.[129] The DoD should work with Five-Eyes and NATO countries to promote responsible global proliferation of artificial intelligence and prevent China from circumventing sanctions through other foreign partnerships. Articulating a global commitment to AI ethics in military applications and engaging with like-minded states supports responsible use of new defense systems and presents non-aligned states an alternative to China's exploitative partnerships. International agreements on strong standards for AI safety, testing, and auditing can mitigate misperceptions and prevent unintended escalation.

Conclusion

In Jack Levy's 1984 *Offensive/Defensive Balance of Military Technology*, he states that "dominant weapons in the pre-nuclear era were used primarily for the defeat of adversary armed forces, whereas the most advanced weapons in the nuclear era are used primarily for coercion and bargaining."[130] China's shift to AI-empowered warfare threatens to usher in an era where the most advanced weapons are not used to defeat armed forces, nor for coercion or bargaining, but to attain strategic victory without the need for conventional weapons at all.

CCP access to U.S. military expertise, innovations, and intelligence threatens more than our economic prosperity. If American companies and allies continue to supply military-grade AI to China, Xi's "intelligentized warfare" could facilitate a global shift to more clandestine and manipulative means to obtain political ends. The geopolitical consequences of an authoritarian regime with revisionist objectives extending its authority across the Indo-Pacific and beyond are difficult to overstate. In the short term, China could meet its objectives in Taiwan, Xinjiang, and Tibet. In the long term, a transition to fifth-generation warfare would have broad implications on global influence and authority structures, undercut democratic principles and human rights, and alter the creation of international norms and values.

Artificial intelligence will continue to surpass full understanding, but it should not surpass American defenses. The first step is to investigate and sever the ties that bind the Chinese state to American innovation vanguards. Next, Congress should enforce rigorous ethical standards in AI functionality and proliferation. Finally, the Department of Defense must close gaps between offensive and defensive AI capabilities so that the CCP is unable to employ American offensive technologies against the United States and its allies. Tomorrow's weapons of war are being created in the U.S. today, and it is up to our democracies to ensure these weapons are used responsibly.

Endnotes

[a] All photos not otherwise attributed are provided by the U.S. Department of Defense. The appearance of U.S. Department of Defense visual information does not imply or constitute DoD endorsement.
[1] *Oversight of AI: Rules for Artificial Intelligence, Before the U.S. Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law*, 118th Cong. (2023) (statement of Sen. Dick Durban, D-IL).
[2] *Artificial Intelligence: Advancing Innovation Towards the National Interest*, *Before the U.S. House of Representatives Committee on Science, Space and Technology*, 118th Cong. (2023) (statement of Rep. Zoe Lofgren, D-CA).
[3] Matt Berg and Rebecca Kern, "Ted Cruz: Congress 'Doesn't know what the hell it's doing' with AI regulation," *Politico,* May 16, 2023.
[4] Nicholas Crafts, "Artificial intelligence as a general-purpose technology," *Oxford Review of Economic Policy* 37, no. 3 (Autumn 2021): 521–536; Matt O'Shaughnessy, "One of the Biggest Problems in Regulating AI Is Agreeing on a Definition," Carnegie Endowment for International Peace, October 6, 2022.
[5] Miao Cui and David Y. Zhang, "Artificial intelligence and computational pathology," *Laboratory Investigation* 101, no. 4 (2021): 412–422.
[6] Xi Jinping, "国家中长期经济社会发展战略若干重大问题 [Several Major Issues in the National Medium and Long-Term Economic and Social Development Strategy]," *Xinhuanet*, October 31, 2020; Xi Jinping, "Speech by President Xi Jinping at a Ceremony Marking the 95th Anniversary of the Founding of the Communist Party of China," CSIS, July 1, 2016; Xi Jinping, "构建中国特色现代军事力量体系 [Build a modern military power system with Chinese Characteristics]," People's Daily Online, August 31, 2014.
[7] Information Office of the State Council of the People's Republic of China, "China's National Defense in 2008" (PDF), *Federation of American Scientists*, January 2009.
[8] The State Council of the People's Republic of China, "New Generation Artificial Intelligence Development Plan," Translated by Graham Webster et al., Stanford DigiChina, August 1, 2017; The State Council of the People's Republic of China, "Outline of the 14th Five-Year Plan (2021-2025) for National Economic and Social Development and Vision 2035 of the People's Republic of China," The People's Government of Fujian Province Website, August 9, 2021.
[9] Bill Gertz, "China in race to overtake the U.S. in AI warfare," Asia Times, May 30, 2018.
[10] Ryan Fedasiuk, Jennifer Melot, and Ben Murphy, "Harnessed Lightning," *CSET Georgetown*, October 2021.
[11] *Man and Machine: Artificial Intelligence on the Battlefield, Before the U.S. House of Representatives Subcommittee on Cyber, Information Technologies, and Innovation,* 118th Cong. (2023) (statement of Alexandr Wang, Founder and Chief Executive Officer, Scale AI).
[12] William Lacy Clay et al., "Follow the Money: AI Winners in President Biden's FY 2024 Budget Request," *Pillsbury*, April 28, 2023.
[13] "China AI Development and Business Opportunities," Cambridge Wireless News, July 3, 2023.
[14] Ruihan Huang and Joshua Henderson, "The Return of the Technocrats in Chinese Politics," *Macro Polo*, May 3, 2022.
[15] China State Council, "New Gen AI Plan"; Networking and Information Technology Research and Development Subcommittee, "The National Artificial Intelligence Research and Development Strategic Plan" (PDF), *National Science and Technology Council*, October 2016.
[16] European Union, "The Artificial Intelligence Act," *Future of Life Institute,* April 21, 2021; National Institute of Standards and Technology, "Artificial Intelligence Risk Management Framework" (PDF), U.S. Department of Commerce, January 2023.
[17] Ambassador Mark Green, "China is the Top Trading Partner to More Than 120 Countries," *Wilson Center,* January 17, 2023.
[18] Bergur Thormundsson, "AI market spending worldwide 2020, by segment," *Statista,* June 14, 2023.
[19] Jamie Gaida et al., "ASPI's Critical Technology Tracker," *Australian Strategic Policy Institute*, March 1, 2023.
[20] Francisco Urdinez, "Economic Displacement: China's Growing Influence in Latin America," *Wilson Center,* June 16, 2023; Ministry of Foreign Affairs of the People's Republic of China, "Fact Sheet: Cooperation Between China and Pacific Island Countries," May 24, 2022.
[21] Jamie Gaida, "ASPI's Critical Technology Tracker."; Meia Nouwens and Helena Legarda, "China's pursuit of advanced dual-use technologies," *International Institute for Strategic Studies*, December 18, 2018; "Biden orders restrictions on U.S. investments in Chinese technology," NPR, August 9, 2023; Ryan Junck et al., "China's New Data Security and Personal Information Protection Laws: What They Mean for Multinational Companies," *Skadden,* November 3, 2021.
[22] Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" *Information Technology and Innovation Foundation*, May 1, 2017; Aqib Aslam et al., "Globalization Helps Spread Knowledge and Technology Across Borders," *International Monetary Fund*, April 9, 2018.
[23] Ana Swanson, "China Continues to Fall Short of Promises to Protect Intellectual Property," *The New York Times,* April 27, 2022.
[24] Julian Baird Gewirtz, "China's Long March to Technological Supremacy," *Foreign Affairs,* August 27, 2019; Xi Jinping, "President Xi Jinping's Speech."
[25] Xiao Tan and Yao Song, "China's 'Whole Nation' Effort to Advance the Tech Industry," *The Diplomat,* April 21, 2022; Jordan Robertson and Michael Riley, "Engineer Who Fled Charges of Stealing Chip Secrets Now Thrives in China (Repeat)," *Bloomberg,* June 6, 2022; Glenn Fleishman, "Justice Department Charges Chinese-Controlled Firm With Semiconductor Trade Secret Theft From Micron Technologies," *Fortune,* November 1, 2018.
[26] Nicholas Eftimiades, "The Impact of Chinese Espionage on the United States," *The Diplomat,* December 4, 2018.
[27] Every company operating in China must provide its stored data to government officials upon request, including data stored in the PRC that was gathered abroad. See Ryan Junck, "China's New Data Laws."
[28]Sean Gallagher, "Red Flag Windows: Microsoft modifies Windows O.S. for Chinese government," *ARS Technica,* 2017. MK Wang et al., "Data sovereignty and China regulations," Microsoft.com, May 30, 2023.
[29] Ryan Gallagher, "Google's Secret China Project "Effectively Ended" After Internal Confrontation," *The Intercept,* December 17, 2018.

[30] Josh Ye, "Alibaba's cloud unit brings Meta's AI model Llama to its clients," *Reuters,* July 26, 2023; The State Council of the People's Republic of China, "Measures for the Management of Generative Artificial Intelligence Services– April 2023," Translated by Seaton Huang et al., *Stanford DigiChina*, April 12, 2023.
[31] U.S. Embassy Beijing Economic Section, "2021 Investment Climate Statements: China," 2021; "China's 161 trillion yuan state asset watchdog says more M&As to come," Bloomberg News, April 11, 2018; Wendy Wu, "How the Communist Party controls China's state-owned industrial titans," *South China Morning Post,* June 17, 2017. "China's central SOEs deliver strong performance," *Xinhuanet,* March 9, 2017.
[32] "FACT SHEET: Executive Order Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China," The White House, June 3, 2021.
[33] "21Vianet Group, Inc. Form 20-F," United States Securities and Exchange Commission, April 14, 2018, 65.
[34] "21Vianet Group, Inc," 2018, 43.
[35] "2021 Investment Climate Statements: China," U.S. Bureau of Economic and Business Affairs, 2021.
[36] "21Vianet Group, Inc. Form 20-F," United States Securities and Exchange Commission, April 26, 2022.
[37] Graham Webster, "Targeting U.S. Chip Firm Micron, China's Cybersecurity Reviews Continue to Evolve," DigiChina, April 7, 2023.
[38] "21Vianet Group, Inc. Form 20-F," United States Securities and Exchange Commission, 50.
[39] "Department of Defense Prime Awards to Microsoft, 2022," USASpending.gov, accessed September 12, 2023.
[40] Rick Wagner, "Microsoft continues commitment to US Department of Defense with JWCC selection," *Microsoft*, December 8, 2022.
[41] Loren Thompson, "Microsoft's Big Footprint In China Is Out Of Step With U.S. Security Concerns," *Forbes,* June 12, 2023.
[42] Loren Thompson, "Microsoft's Big Footprint In China Is Out Of Step With U.S. Security Concerns," *Forbes,* June 12, 2023.
[43] Frank Hersey, "Microsoft unveils more ways to work with the Chinese government and raise Chinese children," *TechNode,* May 25, 2018; "Microsoft and OpenAI Extend Partnership," Microsoft Corporate Blogs, January 2023, archived; "Azure global infrastructure: Products available by region," Microsoft.com, accessed April 26, 2023, archived; "Azure OpenAI Demo Center: Empowered by Microsoft China GPS," *Azure Static Apps*, accessed April 25 2023, archived; Microsoft Open Source, "Microsoft GPSCSA China OpenAI in a Day," *Github*, March 19, 2023.
[44] Kate Kaye, "Microsoft helped build AI in China. Chinese AI helped build Microsoft," *Protocol,* November 2, 2022.
[45] Zhu Shenshen, "Microsoft to offer more AI features in cloud service in China," *Shine*, March 3, 2023.
[46] Frank Hersey, "Microsoft unveils more ways."; Loren Thompson, "Microsoft's Big Footprint."
[47] "Microsoft and CETC announce partnership to serve Chinese users in specialized fields," Microsoft News Center, September 23, 2015.
[48] "CMI Cloud Connect," Microsoft Azure Marketplace, accessed July 18, 2023; Paul Mozur, "China Cuts Mobile Service of Xinjiang Residents Evading Internet Filters," New York Times, November 23, 2015.
[49] Madhumita Murgia and Yuan Yang, "Microsoft worked with Chinese military university on artificial intelligence," Financial Times, April 10, 2019.
[50] "DJI and Microsoft partner to bring advanced drone technology to the enterprise," Microsoft News Center, May 7, 2018.
[51] "DJI and Microsoft partner," Microsoft News Center.
[52] For detail on DJI's denial of allegations, see Cate Cadell, "Drone company DJI obscured ties to Chinese state funding, documents show," *Washington Post,* February 1, 2022; Space Force Director of Operations Maj. Gen. David Miller states that the U.S. must presume a Chinese satellite is a threat regardless of whether it is commercial or military. See: Patrick Turner, "China's Commercial Space Ventures Pose A Variety of Threats, DOD Officials Say," *Defense One,* July 4, 2023.
[53] "U.S. puts Chinese drone giant DJI on military ties blacklist," AlJazeera News, October 7, 2022; for additional evidence, see Rui C. Barbosa, "China continues to build up of Yaogan-30 constellation," Nasa Spaceflight, December 26, 2017.
[54] William Hannas, Huey-Meei Chang, Daniel Chou, and Brian Fleeger, "China's Advanced AI Research," Center for Security and Emerging Technology, July 2022.
[55] "新闻 [BAAI Frontpage]," *Beijing Academy of Artificial Intelligence*, accessed August 21, 2023. BAAI's usage of 'neutrality' in this context [复合的团队背景与非营利研究机构的中立定] suggests a lack of party and commercial affiliation as an alternative to the standard phrase of support for Chinese government entities and initiatives usually found on the pages of state-affiliated enterprises.
[56] "伍建民院长带队调研北京智源人工智能研究院 [Dean Wu Jianmin led a team to investigate Beijing Academy of Artificial Intelligence],"BJAST News, April 15, 2022.
[57] Thomas Lehmann, "AI Politics Is Local," *New America*, January 23, 2020; Jeffrey Ding, "ChinAI #73: Dispatch from the Beijing Academy of AI Conference (BAAI) 2019," ChinAI Newsletter, November 10, 2019; "AI Policy And China: Realities of State-Led Development," *Stanford Program on Geopolitics, Technology, and Governance*, October 29, 2019.
[58] Yann LeCun (@ylecun), "The Beijing Academy of Artificial Intelligence publishes AI ethics guidelines," Twitter, June 3, 2019.
[59] "June 30, 2022 Meeting of the LF AI & Data Technical Advisory Council" (PDF), *LF AI Data Foundation*, 30 June 2022.
[60] Geoffrey Cain, "Microsoft Issues Warning About Chinese AI That Microsoft Helped Create," The Dispatch, May 11, 2023.
[61] Will Knight, "Good News! China and the US Are Talking About AI Dangers," Wired, June 15, 2023.
[62] Neil Shen, "BAAI: the idealists driving China's large-scale model industry," *PingWest*, June 16, 2023.
[63] Skyler Bernards, "Top Government Contracts Won by Amazon Web Services," ExecutiveGov, August 11, 2023.
[64] Defense contractor Beijing Highlander appears on the U.S. Department of Commerce Bureau of Industry and Security's Supplement No. 4 to Part 744 – Entity List for license requirements that apply to entities acting or at significant risk of acting contrary to the national security interests of the United States. See "Supplement No. 4 to Part 744 – Entity List" (PDF), U.S. Department of Commerce Bureau

of Industry and Security, accessed June 16, 2023; According to the *Wall Street Journal*, Beijing Highlander "touts its role in China's defense industry on its Chinese-language website and in company filings, including a claim in its 2017 annual report that its products are featured on "all models" of Chinese warships, according to C4ADS." See Kate O'Keeffe, "China taps its private sector to boost its military, raising alarms," *Wall Street Journal*, September 5, 2019. For information on NWCD, see "NWCD is the Operator and Provider of AWS China Ningxia Region Cloud Services," Amazonaws.com, accessed May 25, 2023, archived; "AWS Regional Services," Amazon Web Services, accessed March 28, 2023.

[65] Andrew Jones, "Chinese commercial rocket firm launches 26 satellites, sets national record," SpaceNews, June 7, 2023.

[66] The training base is called the "Bingtuan Xingxin Vocational and Technical College" and is listed as a partner on AWS Partners Page. U.S. Department of the Treasury, "Treasury Sanctions Chinese Entity and Officials Pursuant to Global Magnitsky Human Rights Executive Order," July 31, 2020.

[67] "合作伙伴 [Our Partners]," KGT Data, accessed August 1, 2023; "柯基数据加入创邻科技 "Graph+X" 图智能生态合作体系 [Corgi Data joins Chuanglin Technology's "Graph+X" graph intelligent ecological cooperation system]," Sohu News, December 17, 2022; "案例研究: 柯基数据 [Case Study: Corgi Data]," Amazon AWS China, accessed July 24, 2023; "智明达：成都智明达2021年年度报告全文 [Zhimingda: Chengdu Zhimingda 2021 Annual Report Full Text]," Zhimingda, April 4, 2022.

[68] "AWS Marketplace," Amazon Web Services, accessed June 13, 2023.

[69] Jonathan Vanian, "Chinese retailers helped lift Meta's first-quarter sales in a tough online advertising market," CNBC, April 26, 2023.

[70] Aaron Mok, "Mark Zuckerberg reportedly wants to follow in Elon Musk and Tim Cook's footsteps, and sell products in China — but his past criticisms of China could haunt him," *Business Insider,* July 3, 2023; Paul Mozur and Lin Qiqing, "How Facebook's Tiny China Sales Floor Helps Generate Big Ad Money," *The New York Times,* February 7, 2019.

[71] Paul Mozur and Sheera Frenkel, "Facebook Gains Status in China, at Least for a Moment," *The New York Times*, July 24, 2018.

[72] "Mark Zuckerberg Stands for Voice and Free Expression," Meta.com, October 17, 2019; Rishi Iyengar, "America's top tech CEOs can't agree on whether China steals from them," CNN, July 30, 2020.

[73] Elizabeth Dwoskin and Christian Shepherd, "Made-in-China Labels Become a Problem for Meta's Anti-China Stance," *Washington Post*, December 31, 2022.

[74] Madhumita Murgia, "Facebook to build metaverse with start-up that had US military contracts," Financial Times, December 24, 2021.

[75] The papers are "Minimalistic Unsupervised Learning with the Sparse Manifold Transform," "Unsupervised Learning of Structured Representations via Closed-Loop Transcription," and "EMP-SSL: Towards Self-Supervised Learning in One Training Epoch." See "Profile of Yann LeCun," Google Scholar, accessed June 1, 2023.

[76] "Professor Yi Ma," Berkely EECS, accessed June 9, 2023.

[77] Alex Joske, "The Party speaks for you: Foreign interference and the Chinese Communist Party's united front system" (PDF), *Australian Strategic Policy Institute*, June 2020; Alex Joske, "Hunting the phoenix: The Chinese Communist Party's global search for technology and talent," *Australian Strategic Policy Institute*, August 2020.

[78] Yojana Sharma, "China's Effort To Recruit Top Academic Talent Faces Hurdles," The Chronicle of Higher Education, May 28, 2013.

[79] "The China Threat: Chinese Talent Plans Encourage Trade Secret Theft, Economic Espionage," *Federal Bureau of Investigation*, accessed August 21, 2023.

[80] *Securing the U.S. Research Enterprise from China's Talent Recruitment Plans*, B*efore the Senate Homeland Security and Governmental Affairs Committee, Permanent Subcommittee on Investigations* (2019) (Statement of John Brown, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation).

[81] Ellen Barry and Gina Kolata, "China's Lavish Funds Lured U.S. Scientists. What Did It Get in Return?" *The New York Times*, February 6, 2020.

[82] Albert Calamug, "Delivering on our U.S. data governance," TikTok.com, June 17, 2022.

[83] Anusuya Lahiri, "China's Payback: Huawei Develops IT Software, Reducing Dependence On Oracle," Yahoo Finance, April 20, 2023.

[84] Maureen Farrell, "Pentagon Divides Big Cloud-Computing Deal Among 4 Firms," The New York Times, December 7, 2022.

[85] Mara Hvistendahl, "How Oracle Sells Repression in China," *The Intercept,* February 18, 2021.

[86] "NVIDIA Chooses Oracle Cloud Infrastructure for AI Services," Oracle.com, March 21, 2023.

[87] Mara Hvistendahl, "Oracle Executive's Contentious Interview with The Reporter He Sought Dirt On," *The Intercept*, April 30, 2021.

[88] "Oracle Expands Government Cloud with National Security Regions for U.S. Intelligence Community," Oracle, September 16, 2020; Frank Konkel, "CIA Awards Secret Multibillion-Dollar Cloud Contract," *NextGov,* November 20, 2020.

[89] Thomas Maxwell, "The U.S. could restrict Chinese companies from using cloud service providers like Amazon and Microsoft," *Insider,* July 4, 2023.

[90] "President Biden Signs Executive Order on Addressing United States Investments In Certain National Security Technologies And Products In Countries Of Concern," The White House, August 9, 2023.

[91] China State Council, "New Gen AI Plan."

[92] Nam Hoai Chu et al., "AI-empowered Joint Communication and Radar Systems with Adaptive Waveform for Autonomous Vehicles," *ResearchGate,* February 2022.

[93] "Chinese autonomous vehicle tech raises concerns, US transportation chief says," Reuters, July 20, 2023.

[94] "HARPY: Autonomous Weapon for All Weather," IAI, November 12, 2016; "Loitering Munitions," UVision

[95] *Report to Congress on the Future of Unmanned Aircraft,* Congressional Research Service, July 18, 2022.

[96] Arie Egozi, "US warned Israel over Chinese push to get defense tech: Sources," Breaking Defense, January 27, 2022.

[97] Michael Dahm, *Special Mission Aircraft and Unmanned Systems* (Baltimore: Johns Hopkins University Applied Physics Laboratory, Oct 2020), PDF; "Wing Loong Unmanned Aerial Vehicle (UAV)," *Airforce Technology*, February 2, 2021; "导弹直接命中移动皮卡 中国翼龙无人机再立下一大功 [Missile directly hits truck; Chinese UAV makes another great contribution]," toutiao.com, March 21, 2017; Abdulkader Assad, "Libyan Army shoots down Wing Loong drone provided by UAE for Haftar," Libyan Observer, August 3, 2019; Rawan Shaif and Jack Watling, "How the UAE's Chinese-Made Drone Is Changing the War in Yemen," *Foreign Policy*, March 27, 2018.
[98] Zaheena Rasheed, "How China became the world's leading exporter of combat drones," *AlJazeera,* January 24, 2023; "航展国产无人机抢先看：彩虹系列可用于战场侦察及反恐作战 [First look at domestic drones at the air show: Rainbow series can be used for battlefield reconnaissance and anti-terrorism operations]," People's Daily Online Military Channel, November 12, 2012.
[99] Duff Wilson and John Shiffman, "Special Report: Hunting for U.S. arms tech, China taps legion of amateurs," *Reuters*, December 18, 2023.
[100] David Hambling, "China Releases Video Of New Barrage Swarm Drone Launcher," Forbes, October 14, 2020.
[101] Parth Satam, "100% Autonomous Or Chinese Propaganda? US Expert Decodes Viral Video Showing China's Kamikaze Swarm Drones," *Eurasian Times*, December 29, 2022; Hambling, "China Releases Video."
[102] Greg Myre, "A Chinese drone for hobbyists plays a crucial role in the Russia-Ukraine War," NPR*,* March 28, 2023.
[103] Natasha Bertrand, "U.S. intel report details increasing importance of Chinese technology to Russia's war in Ukraine," CNN, July 27, 2023; "Amendment in the Nature of a Substitute to H.R. 8367 Offered by Mr. Schiff of California" (PDF), U.S. House Intelligence Committee, July 19, 2022; Jacob Fromer et al., "Special report: Russia buying civilian drones from China for war effort," Nikkei Asia, July 1, 2023.
[104] Simone McCarthy, "China curbs drone exports over 'national security concerns'," CNN, August 1, 2023.
[105] Renee Duresta et al., "Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives" (PDF), *Stanford Cyber Policy Center*, July 20, 2020.
[106] Flora Carmichael, "How a fake network pushes pro-China propaganda," BBC, August 5, 2021.
[107] 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* (2017): 484–501.
[108] @CRUX, "Putin 'Deep Fake' Speech Aired On Russian State T.V. After Hack," *YouTube*, June 6, 2023; Paul Sonne, "Fake Putin Speech Calling for Martial Law Aired in Russia," New York Times, June 5, 2023.
[109] Adam Satariano and Paul Mozur, "The People Onscreen Are Fake. The Disinformation Is Real," New York Times, February 7, 2023.
[110] *Oversight of AI: Rules for Artificial Intelligence, U.S. Senate Judiciary Committee.*
[111] "互联网信息服务深度合成管理规定 [Regulations on the Administration of Deep Synthesis of Internet Information Services]," Cyberspace Administration of China, December 11, 2022; "生成式人工智能服务管理暂行办法 [Interim Measures for the Management of Generative Artificial Intelligence Services]," Cyberspace Administration of China, July 13, 2023.
[112] Ikrame Masrhouni and Abdelaziz Bahoussa, "From the first studies of the unconscious mind to consumer neuroscience: A systematic literature review," *International Journal of Research in Business and Social Science* 12, no. 2 (March 2023).
[113] Michael Douglas, "Large Language Models" (PDF), *Harvard University*, July 2023.
[114] Timothy Heath, "China's Military Has No Combat Experience: Does It Matter?" *RAND,* November 27, 2018.
[115] Ryan Fedasiuk, Karson Elmgren, and Ellen Lu, "Managing the Chinese Military's Access to AI Chips," June 2022.
[116] Paul Mozur, Muyi Xiao, and John Liu, "'An Invisible Cage': How China is Policing the Future," *New York Times,* June 25, 2022.
[117] Charles Rollet, "Hikvision Wins PRC Government Forced Facial Recognition Project Across 967 Mosques," IVPM, July 16, 2018; Ana Swanson and Paul Mozur, "U.S. Blacklists 28 Chinese Entities Over Abuses in Xinjiang," New York Times, October 7, 2019.
[118] Beijing Newsroom and Lincoln Feast, "EXCLUSIVE Chinese province targets journalists, foreign students with planned new surveillance system," Reuters, November 29, 2021.
[119] Eduardo Baptista, "Insight: China uses AI software to improve its surveillance capabilities," *Reuters*, April 8, 2022.
[120] Johana Bhuiyan, "Police in China can track protests by enabling 'alarms' on Hikvision software," *The Guardian,* December 29, 2022.
[121] Zachary Cohen, "A look at China's history of spying in the U.S.," CNN, February 4, 2023.
[122] On Cuba, see Warren Strobel and Gordon Lubold, "Cuba to Host Secret Chinese Spy Base Focusing on U.S.," *Wall Street Journal,* June 8, 2023; On Hawaii, see Andrew Erikson and Emily de La Bruvere, "Crashing Its Own Party: China's Unusual Decision to Spy on Joint Naval Exercises," *Wall Street Journal,* July 19, 2014; On Guam, see Alexander Martin, "Chinese hackers behind Guam breach have been spying on U.S. military for years," *The Record,* May 25, 2023; On New York, see Larry Neumeister and Eric Tucker, "Secret Chinese police station in New York leads to arrests," Associated Press, April 17, 2023.
[123] David Sanger, "Hackers Took Fingerprints of 5.6 Million U.S. Workers, Government Says," New York Times, September 23, 2015.
[124] David Sanger, "Chinese Malware Hits Systems on Guam. Is Taiwan the Real Target?," New York Times, May 24, 2023.
[125] "China Cyber Threat Overview and Advisories," U.S. Cybersecurity and Infrastructure Security Agency, 2023.
[126] Gabriel Grill and Christian Sandvig, "Military AI's Next Frontier: Your Work Computer," *Wired,* June 22, 2023; Loukia Papadopoulos, "Military-grade AI may now be used to spy on American civilians," *Interesting Engineering,* June 25, 2023; Hannah Ritchie, "Microsoft: Chinese Hackers hit key U.S. bases on Guam," BBC, May 25, 2023.
[127] Melisha Dsouza, "IBM's DeepLocker: The Artificial Intelligence-Powered Sneaky New Breed of Malware," *PactHub*, August 13, 2018.
[128] Gopal Ratnam, "Defense agency holds contest for AI tools to boost cybersecurity," *Roll Call,* August 9, 2023.
[129] Moira Warburton, "Timeline: Key events in Huawei CFO Meng Wanzhou's extradition case," *Reuters,* December 3, 2020.
[130] Jack Levy, "The Offensive/Defensive Balance of Military Technology: A Theoretical and Historical Analysis" (PDF), *International Studies Quarterly* 28, No. 2 (June 1984), 219-238.