Bureau of Industry and Security 2022 Agenda

FUTURE OF BIS

www.futureofbis.com

Recommendation #4:

Build an AI Workforce at BIS to Strengthen Controls and Stop Illicit Acquisition of American Artificial Intelligence Technologies.

"Whoever becomes the leader in this sphere will become the ruler of the world."
– Vladimir Putin

APRIL 2022

The Department of Commerce's Bureau of Industry and Security (BIS) is probably the most important U.S. government agency most Americans have never heard of. Charged with ensuring export control, treaty compliance, and strategic technology leadership, BIS plays a critical role in U.S.-China policy and without its due diligence, American-made, sensitive and strategic technologies could end up in the hands of the Chinese military and threaten America's national security.

With Alan Estevez as the Director and Thea Kendler serving as Assistant Secretary for Export Administration, BIS now has leaders with unparalleled national security experience at one of the most critical junctures in the agency's history. This series of policy recommendations will provide ideas for BIS and its leadership to pursue an aggressive agenda and use the agency's full range of tools to protect America's security and prosperity.

WHAT IS ARTIFICIAL INTELLIGENCE?

In contrast to natural intelligence displayed by human beings, artificial intelligence is intelligence displayed by machines.[1] More functionally, Michael Kanaan's book *T-Minus AI* describes AI as follows: "Through a combination of silicon, plastics, metals, electrical connections, and code, the goal of artificial intelligence is to simulate the intellectual capacities of the human brain."[2] The U.S. government's National Security and Counterintelligence Center has defined it as "the demonstration of cognition and creative problem solving by machines rather than humans or animals."[3]

We experience AI when our iPhone suggests the next word of the sentence we type or Netflix presents the next movie to watch. But, as the landmark U.S. National Security Commission on Artificial Intelligence (NSCAI) report released in 2021 states, "AI is also the quintessential "dual-use" technology. The ability of a machine to perceive, evaluate, and act more quickly and accurately than a human represents a competitive advantage in any field—civilian or military."[4] Militarily, AI has enormous application for intelligence, surveillance, reconnaissance, logistics, command and control capabilities, lethal autonomous weapons systems, and many other components of warfighting. The

1 See Stuart Russel and Peter Norvig, *Artificial Intelligence: A Modern Approach* (3rd ed.). Upper Saddle River, New Jersey: Prentice Hall, 2009.

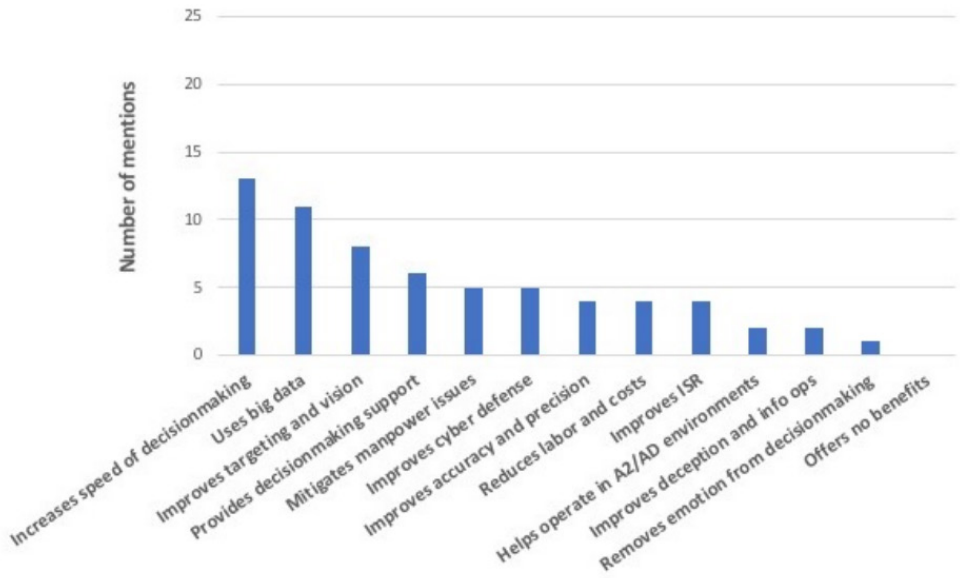
2 Michael Kanaan, *T-Minus AI : Humanity's Countdown to Artificial Intelligence and the New Pursuit of Global Power* Dallas, Texas: BenBella Books, 2020, Kindle Edition p. 59.

3 The National Counterintelligence and Security Center, "Protecting Critical And Emerging U.S. Technologies from Foreign Threats," Fact Sheet released October 2021, p. 4.

4 National Security Commission on Artificial Intelligence Final Report, p. 7. Released March 2021.

goal of incorporating AI technologies into military functions is to achieve or increase competitive advantages in areas such as reaction time, decision-making accuracy, or even target identification. The chart below shows the potential benefits of the military use of AI:[5]

Figure 2.2. Potential Benefits of Military Applications of Artificial Intelligence Identified in Structured Interviews



While the world's militaries undertake their own research and development activities to integrate AI technologies into their military capabilities, many private companies have sprung up worldwide to build AI-powered products that can likewise be deployed for defense purposes. The California-based company Anduril, to name one, has already brought AI-powered surveillance systems, targeting systems, and drone technologies to market, and has found willing buyers by national governments, including the U.S. and the United Kingdom.[6] Says Anduril CEO Brian Schimpf, "Artificial intelligence should be the linchpin of our efforts to re-armor ourselves for a new kind of fight."[7]

AI'S POTENTIAL TO TRANSFORM SOCIETY

Technologists and military and government leaders alike have touted AI's ability to transform society. The power of machines to solve problems and make decisions without human input will fundamentally alter how human beings spend their time and energies. The NSCAI Final Report released in 2021 repurposed Thomas Edison's words on the potential of electricity to reshape human existence to describe AI: "It is a field of fields…it holds the secrets which will reorganize

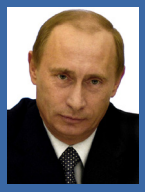
5 Forrest E. Morgan, Benjamin Boudreaux, et al., "Military Applications of Artificial Intelligence," Report published by the Rand Corporation, October 10, 2018, p. 16.

6 Jacob Ward and Chiara Sottile, "Inside Anduril, the startup that is building AI-powered military technology," *NBC News*, October 3rd, 2018.

7 Brian Schimpf, "Anduril Boss: In an era of strategic competition, we need artificially intelligent systems," *Defense News*, December 6, 2021.

the life of the world."[8] Recognizing that artificial intelligence is among the key technologies for America's economic prosperity and national security, the Trump Administration created the American AI initiative in 2019, which doubled AI research investment and established the first-ever AI research institutes, among other achievements. The Biden Administration built on this work in June of 2021 with the National Artificial Intelligence Research Resource Task Force – an advisory committee of technical experts who will help shape national policy on AI. The Department of Commerce also established its own high-level committee, the National Artificial Intelligence Advisory Council, to advise the federal government on AI, but to date there does not appear to be progress in populating it with members.

It is widely thought that the militaries which best harness AI technologies will achieve battlefield superiority over competitors. Chris Brose, an Anduril executive and former Staff Director on the U.S. Senate Armed Services Committee, has written in his seminal book *The Kill Chain*: "The entire basis by which the US military understands events, makes decisions, and takes actions—how it closes the kill chain—will not withstand the future of warfare. It is too linear and inflexible, too manual and slow, too brittle and unresponsive to dynamic threats, and too incapable of scaling to confront multiple dilemmas at once."[9] The NSCAI Report speculates, "In the coming decades, the United States will win against technically sophisticated adversaries only if it accelerates adoption of AI-enabled sensors and systems for command and control, weapons, and logistics."[10] More directly, in a comment with undertones that grow darker by the day, Russian President Vladimir Putin has said, "Whoever becomes the leader in this sphere will become the ruler of the world."[11]



"Whoever becomes the leader in this sphere will become the ruler of the world."

Russian President Vladimir Putin

CHINA'S DEVELOPMENT AND USE OF AI: A GROWING LEAD?

Fully comprehending the potential of AI to produce enormous competitive advantages, adversaries of the United States have begun a de facto arms race in this technological domain. No country threatens American supremacy in AI more than People's Republic of China (PRC), whose drive at AI leadership is part of a broader overall goal to achieve supremacy over the United States and other Western nations in all critical technologies. As the National Bureau of Asian Research's recent report "China's Digital Ambitions: A Global Strategy to Supplant the Liberal Order" notes, "China is strategically and deliberately capitalizing on the digital revolution as an opportunity to define and assert control over international resources, markets, and governance."[12]

Where AI specifically is concerned, the PRC's own communications state its goals quite clearly. The country's own Artificial Intelligence Development Plan claims "AI is a strategic technology that will lead in the future; the world's major developed countries are taking the development of AI as a

8 National Security Commission on Artificial Intelligence Final Report, p. 7. Released March 2021.

9 Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare*. New York: Hachette Books, 2020.

10 NSCAI Final Report, p. 61.

11 Tom Simonite, "For Superpowers, Artificial Intelligence Fuels New Global Arms Race," *Wired*, September 8, 2017.

12 Emily de La Bruyère, Doug Stroub, and Jonathan Marek, eds., "China's Digital Ambitions: A Global Strategy to Supplant the Liberal Order." National Bureau of Asian Research #97, March 2022, p. 3.

major strategy to enhance national competitiveness and protect national security."[13] PRC President Xi Jinping has stated that China must "ensure that our country marches in the front ranks where it comes to theoretical research in this important area of AI, and occupies the high ground in critical and AI core technologies."[14] And Major General Ding Xiangrong, Deputy Director of the General Office of the PRC's 's Central Military Commission, defined military goals as to "narrow the gap between the Chinese military and global advanced powers" by taking advantage of the "ongoing military revolution . . . centered on information technology and intelligent technology."[15]

The NSCAI report affirms the PRC's intentions: "China's plans, resources, and progress should concern all Americans. It is an AI peer in many areas and an AI leader in some applications. We take seriously China's ambition to surpass the United States as the world's AI leader within a decade."[16] The reality is that the PRC may already be surpassing the U.S. in AI prowess. A Tsinghua University (China) study found that China is #1 in both total AI research papers and highly cited AI papers worldwide, #1 in AI patents, #1 in AI venture capital investment, #2 in the number of AI companies, and #2 in the largest AI talent pool.[17] Joshua P. Meltzer, Cameron Kerry, and Alex Engler of the Brookings Institution have assessed, "By many accounts, China is either leading or number two in AI research, leading AI application in at least some industries such as facial recognition."[18] More alarmingly, the Pentagon's Chief Software Officer quit in frustration in 2021 over the slow pace of technological change within the U.S. military, believing such sluggishness has already caused the U.S. to cede AI leadership to the PRC. "We have no competing fighting chance against China in 15 to 20 years," said Nicholas Chaillan. "Right now, it's already a done deal; it is already over in my opinion."[19]

AI TECHNOLOGIES AND THE PRC'S REPRESSION OF UYGHUR MUSLIMS

Of course, nations have the right to pursue technological advantages for their own national benefit. What is troubling about the PRC's efforts at AI dominance is that its government has already established a long track record of using AI technologies for repressive ends. Most infamously, the Chinese government uses AI-powered surveillance tools, such as facial-recognition technology, to track and dehumanize Uyghur Muslims in Xinjiang, part of a broader campaign of repression against ethnic minorities.[20]

Of course, nations have the right to pursue technological advantages for their own national benefit. What is troubling about the PRC's efforts at AI dominance is that its government has already established a long track record of using AI technologies for repressive ends. Most infamously, the Chinese government uses AI-powered surveillance tools, such as facial-recognition technology, to track and dehumanize Uyghur Muslims in Xinjiang, part of a broader campaign of repression against ethnic minorities.

13 "State Council Notice on the Issuance of the New Generation Artificial Intelligence Development Plan," released July 20, 2017. Translated by Graham Webster, Rogier Creemers, Paul Triolo, and Elsa Kania. Published by the New America Foundation, August 2, 2017.

14 Elsa Kania and Rogier Creemers, "Xi Jinping Calls for 'Healthy Development' of AI (Translation)," New America Foundation. November 5, 2018.

15 Gregory C. Allen, "Understanding China's AI Strategy," Report published by the Center for New American Security, February 6, 2019, p. 5.

16 NSCAI Final Report, p. 2.

17 Allen, "Understanding China's AI Strategy," p. 9.

18 Joshua P. Meltzer, Cameron Kerry, and Alex Engler, "The importance and opportunities of transatlantic cooperation on AI," Brookings Institution Paper Published June 2016, p. 3.

19 Katrina Manson, "U.S. Has Already Lost AI Fight to China, Says Ex-Pentagon Software Chief," *The Financial Times*, October 10, 2021.

20 Paul Mozur, "One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority," *The New York Times*, April 14, 2019.

Since at least 2017 the PRC has conducted a campaign of brutal repression against Uygur Muslims living in the Xinjiang province of western China. Up to one million Muslims have been detained in what can be called internment camps and been subject to other abuses such as forced abortions and sterilizations,[21] the demolition of mosques,[22] and the forced quartering of Chinese Communist Party officials in their homes. [23] After a review of the overall situation, the U.S. State Department determined in 2021 that the abuses amount to a "genocide."[24]

To track and control local populations, the Chinese government has imposed a surveillance apparatus on ethnic minorities within Xinjiang that can described without hyperbole as Orwellian.

In 2019, the *New York Times* documented PRC use of AI technologies to repress China's Uyghur Muslim minority. The *Times* conducted in-person interviews with those familiar with the technology and examined databases used by authorities, concluding that the PRC had at one point used its surveillance tools to conduct approximately 500,000 face scans in one month. The *Times* consequently reported that "The facial recognition technology, which is integrated into China's rapidly expanding networks of surveillance cameras, looks exclusively for Uighurs based on their appearance and keeps records of their comings and goings for search and review. **The practice makes the PRC a pioneer in applying next-generation technology to watch its people, potentially ushering in a new era of automated racism."**[25]

Later that year, Bethany Allen-Ebrahimian of the International Consortium for Investigative Journalism published what the ICIJ dubbed "China's operating manuals for mass internment and arrest by algorithm," a batch of highly classified PRC documents verified by Western experts like James Mulvenon as authentic.[26] Aside from precise instructions for Party officials on how internment camps are to be run, the documents also include details on the Party's data-collection platform targeting Uyghurs, which "collects and interprets data without regard to privacy, and flags ordinary people for investigation based on seemingly innocuous criteria, such as daily prayer, travel abroad, or frequently using the back door of their home."[27]

In 2021, an engineer who had helped install AI-powered emotion detection cameras in police stations in Xinjiang province told the BBC that "The Chinese government use Uyghurs as test subjects for various experiments just like rats are used in laboratories. We placed the emotion detection camera 3m from the subject. It is similar to a lie detector but far more advanced technology."[28]

The U.S. government also has abundant intelligence on such abuses, which undoubtedly formed the basis a U.S. Department of Commerce Bureau of Industry and Security decision to place Chinese surveillance gear companies such as Hikvision, Dahua, and Megvii on the Entity List. The rule noted that the designations were being made against "entities [which] have been implicated in human rights violations and abuses in the implementation of China's campaign of repression, mass arbitrary detention, and high-technology surveillance against Uighurs, Kazakhs, and other members of Muslim minority groups."[29] The Department of Commerce added an additional 14 Chinese entities to

---

21 "China cuts Uighur births with IUDs, abortion, sterilization," The Associated Press, June 29, 2020.

22 Chris Buckley and Austin Ramzy, "China Is Erasing Mosques and Precious Shrines in Xinjiang," *The New York Times*, September 25th, 2020.

23 Steven Jiang, "Chinese Uyghurs forced to welcome Communist Party into their homes," *CNN*, May 14, 2018.

24 Michael R. Pompeo, "Genocide in Xinjiang," *The Wall Street Journal*, January 19, 2021.

25 Mozur, "One Month, 500,000 Face Scans"

26 Bethany Allen-Ebrahimian, "Exposed: China's Operating Manuals for Mass Internment and Arrest by Algorithm," International Consortium of Investigative Journalists website, November 24, 2019.

27 Ibid

28 Jane Wakefield, "AI emotion-detection software tested on Uyghurs," *BBC*, May 26, 2021.

29 *The Federal Register*, "Addition of Certain Entities to the Entity List," October 9, 2019.

the Entity List in 2021 specifically for their complicity in these abuses.[30]

China Tech Threat has written on the threat posed by PRC-owned Lenovo. Following a highly controversial and ill-advised acquisition of the IBM's laptop division, Lenovo has grown into the world's largest laptop maker. Many of its products are embedded with unethical AI, and the company is also complicit in the abuses in Xinjiang. The Chinese surveillance equipment company Megvii's flagship product, Face++, is a facial recognition platform which has been used to track and surveil Uyghurs. Lenovo was a lead investor in Face++, which, in turn, is now used in Lenovo laptops and other devices with facial recognition.[31]

CHINA LEVERAGES AI FOR SPYING AND SUPREMACY

The Chinese government and Chinese companies proliferate surveillance gear abroad as a way of helping other countries, especially those with authoritarian tendencies, establish their own high-tech police states. In Myanmar, home to a brutal regime, more than 300 Huawei-made cameras equipped with facial recognition technology dot the capital of Naypitaw.[32] And in Zimbabwe, the PRC startup CloudWalk, has landed an agreement with the government to build a national facial recognition program, with the data being sent back to CloudWalk to help the company improve its AI capabilities.[33] The widespread adoption of PRC surveillance equipment gives China another avenue of partnership with other nations. This has the effect of both expanding the global PRC surveillance dragnet and solidifying symbiotic relationships with cash-strapped and tech-hungry countries. To quote Anduril founder Palmer Luckey: "In the same way that the Soviets gave away boxes of AK-47s to other countries to get in bed with them, China is giving countries in Africa and Asia access to artificial intelligence technology that allows them to build totalitarian police states. And they do this because it makes these countries completely dependent on China."[34] Ishan Sharma at the DayOne Project emphasizes the need for alternatives to PRC gear: "If we are to expect digitizing countries to responsibly deploy advanced technologies, then the US and allies must create a visible alternative to China's turnkey authoritarian technology solutions."[35]

Quite terrifyingly, the proliferation of PRC surveillance equipment has deeply penetrated the United States and other Western countries. Hikvision, perhaps the best-known Chinese surveillance equipment company, had already captured 12% of the North American surveillance camera market by 2017, including 750,000 devices in the U.S., and even has even managed to place products in U.S. military bases and diplomatic facilities.[36] What makes deployments of Chinese surveillance equipment around the world so concerning is that all companies based in China are obligated to follow the country's 2017 Cybersecurity Law – an edict which mandates cooperation with state-initiated data sharing requests.[37] That could lead to data captured by China-made AI-powered

30 U.S. Department of Commerce, "Commerce Department Adds 34 Entities to the Entity List to Target Enablers of China's Human Rights Abuses and Military Modernization, and Unauthorized Iranian and Russian Procurement," Press Release. July 9, 2021.

31 "Lenovo Capital and Incubator Group Created to Advance Core Technology Investments," Lenovo Press Release, May 6, 2016.

32 Nyan Hlaing Lin and Min Min, "Hundreds of Huawei CCTV cameras with facial recognition go live in Naypyitaw" *Myanmar Now*, December 15, 2020.

33 Peter Layton, "Belt and Road means big data and facial recognition, too," *The Interpreter,* June 19, 2020.

34 Ward and Sottile, "Inside Anduril"

35 Ishan Sharma, "A Strategy to Blend Domestic and Foreign Policy on Responsible Digital Surveillance Reform," Report by the Day One Project, released February 2021.

36 Jonathan Hillman, "China Is Watching You," *The Atlantic,* October 18, 2021.

37 Jack Wagner, "China's Cybersecurity Law: What You Need to Know," *The Diplomat,* June 1, 2017.

surveillance technologies, already present in eighty or more countries,[38] weaponized against Party adversaries, including Americans, in many different forms. As former State Department Deputy Assistant Secretary for East Asia-Pacific Affairs David Feith testified to the U.S. House Foreign Affairs Committee, "Beijing recognizes that the competition for global influence in the 21st century will require protecting and harnessing this data to achieve commercial, technological, military and intelligence advantages. And that's what it is doing."[39]

But Americans need not subject themselves to PRC surveillance cameras to expose themselves to risk. Approximately 80 million Americans use the the world's most popular app, TikTok, which is powered by an algorithm that selects automatically the videos users watch. TikTok attracted significant attention from the U.S. government during the Trump Administration because of concerns that its PRC-based parent company, ByteDance, would be forced to hand over vast troves of American user data per PRC practice and rules like its National Intelligence and Cybersecurity Law.[40] These actions against TikTok were unresolved by the end of the administration. While the Biden Administration has used the platform to engage with a key voter demographic, mitigating the threat of TikTok remains legally complicated. The Administration did, according to a spokeswoman for the National Security Council, have an ongoing review of TikTok underway as of February 2022. [41]

In the meantime, young Americans who overwhelmingly comprise TikTok's U.S. user base are leaving their personal data exposed to the PRC. The likely effect is that the Chinese government is vacuuming up user data which it can use to assign every user a social credit score. As described by *Cybersecurity for Dummies* author Joe Steinberg at a March 2022 China Tech Threat discussion, using TikTok will likely even give the PRC an opening to compromise any young adult who will grow up to become President of the United States: "They're going to know every possible detail to blackmail them." [42]

CHINA'S ARMY IS COMMITTED TO CREATING SUPERIOR AI WEAPONRY

Of greatest concern to American national security, insofar as AI is concerned, is the Chinese military's commitment to integrating AI platforms and capabilities into its military apparatus. According to a Center for Security and Emerging Technology (CSET) report titled "Harnessed Lightning: How the Chinese Military is Adopting Artificial Intelligence," released in October 2021, the PLA spends more than $1.6 billion each year on AI-related systems and equipment.[43] CSET went on to note that, based on an analysis of 343 PLA contracts with AI firms, the PLA seems most focused on procuring AI for intelligence analysis, predictive maintenance, information warfare, and navigation and target recognition in autonomous vehicles.[44] The potential for China to leapfrog the U.S. military in AI capabilities without ever having achieved comparable strength in more traditional

38 Sheena Chestnut Greitens, "Dealing with Demand for China's Global Surveillance Exports", *Brookings Institution Global China Report,* April 2020

39 David Feith, "The Strategic Importance of a U.S. Digital Trade Agreement in the Indo-Pacific," Testimony before the U.S. House Foreign Affairs Committee Subcommittee on Asia, the Pacific, Central Asia, and Nonproliferation, January 19, 2022.

40 U.S. Department of Homeland Security, "Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China."

41 Cat Zakrzewski and Drew Harwell, "Biden administration weighting new rules to limit TikTok, foreign apps," *The Washington Post,* February 2, 2022.

42 China Tech Threat, "CTT Quick Cut: The Tech Threat Disconnect: Federal-State Security Gaps Open Doors to PRC Intrusion." Online discussion held March 10, 2022.

43 Ryan Fedasiuk, Jennifer Melot, and Ben Murphy, "Harnessed Lighting: How the Chinese Military is Adopting Artificial Intelligence," Center for Security and Emerging Technology Report, October 2021, p. iv.

44 Ibid.

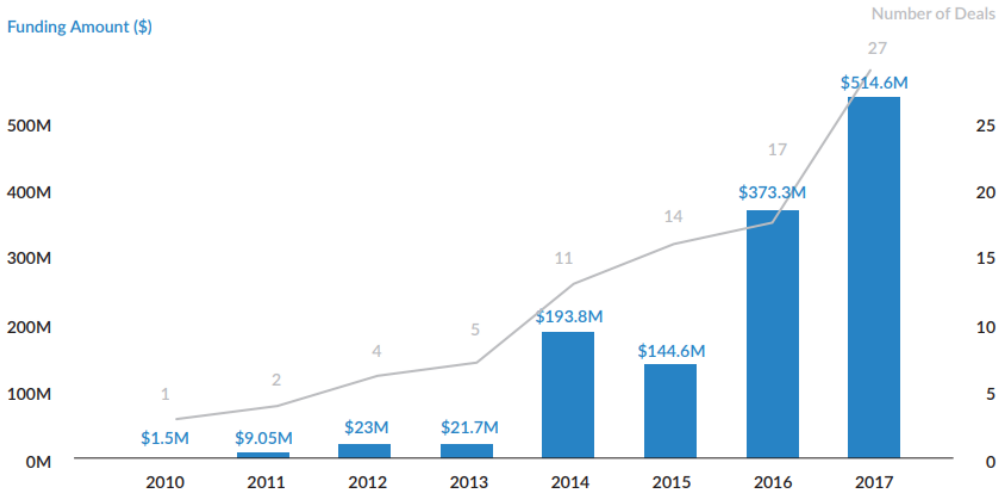
capabilities is very real. A report from the Center for New American Security in 2019 commented: "China sees military AI R&D as a cheaper and easier path to threatening America's sources of military power than developing Chinese equivalents of American systems."[45]

PLA experimentation with such technologies is already translating into functional or near-functional weaponry. According to research done by Elsa Kania of the Brookings Institution, "While there is currently no direct evidence that the PLA has formally fielded a weapons system fully consistent with the definition of 'AI weapon,' a number of systems are analogous or comparable in their functionality."[46] Per Kania, older PLA tanks have been retrofitted with certain autonomous and remote-control capabilities, and PLA is also building automatic targeting capabilities into its cruise missiles.[47] Joseph Trevithick has reported that Chinese pilots have faced off against AI-powered combat systems in simulations and lost.[48] CSET has also found that "laboratories affiliated with the Chinese military are actively pursuing AI-based target recognition and fire control research."[49]

PROBLEM #1 – INVESTORS FRONTING FOR THE PRC INVEST IN AMERICAN AI STARTUPS, THEREBY GAINING ACCESS TO SENSITIVE TECHNOLOGIES

Preventing China from obtaining an insurmountable AI lead over the U.S. begins with recognizing how American companies themselves may be feeding the beast. The chart below, reproduced from a Defense Innovation Unit Experimental paper, shows the dramatic increase in Chinese investments in American AI companies from 2010-2017:[50]

Chart 3: Chinese Investment in U.S. Artificial Intelligence Companies, 2010 - 2017
$1.3 Billion in Deal Value; 81 deals



45 Allen, "Understanding China's AI Strategy," p. 9.

46 Elsa Kania, "AI Weapons in China's Military Innovation," Brookings Institute report released April 2020, p. 4.

47 Ibid.

48 Joseph Trevithick, "Chinese Pilots Are Also Dueling With AI Opponents in Simulated Dogfights and Losing: Report" *The Drive*, June 18, 2021.

49 Fedasiuk et al.,"Harnessed Lighting," p. iv.

50 Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation," Defense Innovation Unit Experimental report, January 2018, p. 29.

Such investment is likely in part sowing the seeds of Chinese military superiority, even if the People's Liberation Army or other organs of the Chinese government are making the investments. The Congressional Research service noted in 2020, "In general, few boundaries exist between Chinese commercial companies, university research laboratories, the military, and the central government. As a result, the Chinese government has a direct means of guiding AI development priorities and accessing technology that was ostensibly developed for civilian purposes."[51]

Even with Chinese foreign investment coming into the U.S. subject to the Committee on Foreign Investment in the U.S. (CFIUS) review process, the relationships between putatively independent Chinese investors and the Chinese Communist Party can be opaque or even undetectable to U.S. authorities, thus allowing certain investments detrimental to American national security to slip through the cracks. CFIUS alone is not an adequate tool to stop the Chinese tech threat inside the U.S. Although Congress has expanded CFIUS' scope and review process – leading to many more red flags surrounding Chinese investment – the sheer number of private sector firms in U.S. makes perfect enforcement impossible. While CFIUS has stepped up its capabilities considerably to block PRC takeovers of companies with sensitive personal data like PatientsLikeMe, Grindr, and StayNTouch and entities with strategic importance like the Chicago Stock Exchange, more work remains to be done to bolster CFIUS' oversight capabilities and resources.

Even if American companies aren't developing AI technologies for dedicated military purposes, American civilian technologies can be leveraged by the PRC for military use.

Even if American companies aren't developing AI technologies for dedicated military purposes, American civilian technologies can be leveraged by the PRC for military use. The quintessential example of a dual use technology which China has already exploited is semiconductors. As just one example, Yangtze Memory Technologies Company (YMTC), the PRC-backed semiconductor firm with deep ties to the Chinese military, has avoided being placed on the Commerce Department's Entity List, despite using software and equipment sourced in America. Apple is reportedly poised to use YMTC chips in the iPhone, a move that helps the PRC fulfill its ambitions to dominate the global chip market and signal to other U.S. manufacturers the acceptability on Chinese state-backed entities.[52] Of course, where AI is concerned, writes Dylan Patel of the Substack *Semi-Literate,* "Sustained U.S. leadership in AI is contingent on sustained U.S. firm leadership in semiconductors."[53]

The U.S. government has no effective mechanism for stopping the transfer of technologies from so-called civilian companies to the PLA. Even if export controls are levied on companies supplying the PLA, the CCP's policy of military-civil fusion (MCF) stipulates that civilian companies and institutions provide the state any civilian technologies that could have a military application. As China Tech Threat has written, "there is no reliable and systematic way to ensure that the same technology is not used in PRC weaponry, a proliferation that violates U.S. and international law against so-called "dual use" technologies."[54] In an AI context, it wouldn't be surprising if, hypothetically, Nvidia chips currently used for AI platforms in Chinese electric vehicles were later found in Chinese military drones.[55]

---

51 The Congressional Research Service, "Artificial Intelligence and National Security," Report released November 10, 2020, p. 22.

52 China Tech Threat, "Apple Reportedly Considering Sourcing Chips for Next iPhone from China's "National Champion," March 29, 2022.

53 Dylan Patel, "The Other AI Hardware Problem," *Semi-Literate* Substack post, March 12, 2022.

54 Roslyn Layton, "The Art of Balancing Economic and National Security: Policy Review of Semiconductor Manufacturing Equipment Export Control," report released October 2020, p. 7.

55 Norihiko Shirouzu, Yilei Sun, "U.S. chipmaker Nvidia to provide AI platform for Chinese EV start-ups," *Reuters,* November 21, 2018.

Finally, beyond what the PRC can legally or surreptitiously procure via investment or its MCF policy, its well-known rampage of American technology theft continues apace. FBI Director Christopher Wray stated in 2020 that there has been a 1300% increase in China-related economic espionage probes in last decade.[56] Surely AI-focused technologies have been targeted as part of China's desired haul.

PROBLEM #2 – AMERICAN-DEVELOPED COMPONENTS OF CRITICAL AI TECHNOLOGIES FIND THEIR WAY TO THE CHINESE MILITARY

It is likely that the PLA has already integrated American AI products into its own military AI research and development efforts. As CSET has reported "Of the 273 PLA AI equipment suppliers identified in this study, just 8 percent are named in U.S. export control and sanctions regimes."[57] 92% of known PLA AI suppliers, therefore, are free to purchase American AI technologies. The U.S. government has shown some capacity and will to prevent Chinese state-run military contractors and Chinese state champions from obtaining sensitive technologies – the most obvious example being limits on the export of advanced technological components used in Huawei products levied in 2020. But, as CSET also notes, "Most of the PLA's AI equipment suppliers are not state-owned defense enterprises, but private Chinese tech companies founded after 2010."[58] Thus, small Chinese companies with potentially significant technological outputs are likely transferring American technologies to the PLA, and the U.S. government is functionally powerless to stop it.

China is also proficient at skirting export controls by using intermediating companies which transfer AI tech to the PLA. CSET invokes the example of Beijing Zhongtian Yonghua Technology Development Co., Ltd., which purports only to be distributor of (civilian) technology, but in fact is a supplier for the PLA.[59] BIS has to date done too little to close such gaps of oversight. In October 2021, five U.S. senators wrote to Department of Commerce Secretary Gina Raimondo calling for BIS to "review and add all the PLA AI suppliers in the CSET report to the Entity List."[60] As of this writing, BIS has still not taken action.

56 Ursula Perano, "Wray: FBI has over 2,000 investigations that trace back to China," *Axios,* June 24, 2020.

57 Fedasiuk et al., "Harnessed Lightning," p. v.

58 Ibid. p. iv.

59 Ibid. p. 34.

60 Office of Senator Bill Hagerty, "Hagerty, Cotton, Colleagues Call On Secretary Raimondo To Blacklist Companies That Provide AI Technology To The Chinese Military," Press Release, November 16, 2021.

PROBLEM #3 – BIS HAS INSUFFICIENT STAFFING TO PROPERLY ENFORCE EXPORT CONTROLS

The inability of BIS to properly conduct oversight on the nexus of American AI technology companies and entities affiliated with the PLA could be rooted in inadequate numbers of personnel. With more than 7,000 for-profit AI companies operating in the U.S.,[61] it is unreasonable to think that BIS can identify the PRC's AI footprint in the U.S. with its current staff and budget. The agency has a scant 100 enforcement officers for all efforts globally.[62]

RECOMMENDATIONS

In 2018 Congress legislated BIS to regard artificial intelligence as a controlled technology. As of 2022, BIS has done little to enforce export controls on AI. Admittedly, categorizing AI is a difficult task because it is a collection of non-discrete technologies, many in theoretical stages, thus making it hard to isolate which components should be subject to export controls.

However, BIS can move forward to develop a distinct strategy to identify and control the top AI technologies with potential for use in military applications. For the first time, BIS has leadership sourced from the national security arena in its new Undersecretary, Alan Estevez. The Undersecretary should leverage Pentagon relationships and expertise to fast-track a BIS strategy for AI. This can include creating a cadre of personnel with military AI expertise, including individuals who can devote themselves part-time from the civilian sector, who can well understand which artificial intelligence technologies should be kept away from PRC-based entities.

Similarly, the NSCAI report proposes the creation of a "Digital Corps" workforce of AI-skilled professionals who are assigned to different agencies at different times to work on key problems and projects.[63] BIS need not wait for the federal government to complete the process of designing and implementing such a staffing model; it should take the initiative to stand up its own complementary unit of professionals.

Additionally, BIS has an important role to educate U.S. firms about the dual-use applications of AI and how it can be weaponized by adversaries. To quote the NSCAI report: "The Department of Commerce, through the BIS, should use targeted end-use controls and human rights due-diligence reporting requirements to prevent and deter U.S. firms from enabling problematic government end uses of AI and associated technologies."[64] This education should include but is not limited to BIS trainings, events, reports, and so on.

Beyond BIS, the U.S. government should establish a mechanism for screening outbound investment in China, a step which Secretary Raimondo supports.[65] This will have the effect of ensuring American capital is not unwittingly funding potential Chinese advantages in artificial intelligence.

---

61 Crunchbase, "United States Artificial Intelligence Companies," Accessed March 29, 2022.

62 Future of BIS, "Bureau of Industry and Security 2022 Agenda Recommendation #1: Strengthening Enforcement to Detect, Identify, and Deter Export Control Violation," report released December 2021, p. 2.

63 NSCAI Final Report, p. 123

64 Ibid. p. 534.

65 Gavin Bade, "Raimondo open to enhanced screening of U.S. investments in China," *Politico Pro,* March 22, 2022.