Issue Brief

Decoupling in Strategic Technologies

From Satellites to Artificial Intelligence

Authors
Tim Hwang
Emily S. Weinstein

CSET CENTER *for* SECURITY *and* EMERGING TECHNOLOGY

July 2022

Introduction

Geopolitical tensions between the United States and China have sparked an ongoing dialogue in Washington about the phenomenon of "decoupling," the use of public policy tools to separate the multifaceted economic ties that connect the two powers. This process has already begun, with a range of steps taken in recent years on both sides of the Pacific to reshape the bilateral economic relationship.

Decoupling encompasses a wide range of tactics and policy objectives.[1] Some have advocated for decoupling as a means of protecting the economic health of certain U.S. industries. Others have argued for decoupling as a tool to reduce the dependence of the United States on China for strategically important products and supplies. Still others see decoupling as a means of limiting the channels through which China might compromise U.S. national security, as in the ongoing debates around 5G and network infrastructure.

This issue brief studies the efficacy of one specific aspect of this broader decoupling phenomenon. Specifically, it examines the use of export controls and related trade policies to prevent a rival from acquiring the equipment and know-how to catch up to the United States in cutting-edge, strategically important technologies. This objective has already motivated some of the most widely discussed events of the "decoupling era" in U.S.-China relations. The Committee on Foreign Investment in the United States, for example, has been active in blocking Chinese firms from accessing specific types of leading-edge semiconductor designs.[2]

To study the efficacy of these tactics, this issue brief examines past efforts by the United States to decouple supply chains in satellite technology. For decades, an array of export controls and other regulations have worked to prevent rivals from accessing key technologies for satellites designed and manufactured in the United States. The satellite domain affords the opportunity to examine the effectiveness of decoupling policies in the context of a suite of emerging technologies considered strategically important. These lessons have contemporary relevance as U.S. policymakers consider establishing similar regimes in the current generation of strategic emerging technologies like artificial intelligence (AI).

This paper addresses two critical questions. First, to what extent does history support the hypothesis that decoupling is an effective tool in blocking access and slowing the progress of a rival in an emerging technology? Second, to the extent that it can be a tool in achieving this aim, what factors make decoupling policies more or less successful?

This analysis uncovers a number of valuable insights. For one, it is clear that decoupling is a viable strategy: export controls can indeed play a powerful role in reshaping supply chains and limiting rival access to emerging technology. At the same time, the satellite example tempers our expectations about what decoupling can achieve. It is clear that decoupling regimes are imperfect and frequently act as a hindrance, rather than an absolute bar, to a rival's technological progress. Moreover, the transition of a hard-to-access, cutting-edge technology to a widespread, commodified one over time means that the effectiveness of decoupling tactics declines dramatically over time. The satellite domain suggests that strategically important technologies can and will be acquired by a motivated rival, and decoupling can help to determine when that might happen.

The experience of decoupling in supply chains around satellites also suggests that the success of decoupling turns in large part on specific characteristics of the technology in question. Specifically, technologies that feature geographically concentrated supply chains appear more amenable to decoupling tactics. This feature facilitated the temporary success of decoupling policies in the satellite domain. To the extent that supply chains are diffuse, with many interchangeable providers spread widely across multiple countries, decoupling may be a relatively weak means to limit rival progress in a given technology.

Decoupling is a narrow tool of national competition in emerging technologies. It has limited impact, in the sense that it appears difficult to use decoupling to permanently bar a rival from catching up in a given technology. It also has limited scope in that the specific supply chain geographies of certain technologies lend themselves to more effective decoupling regimes than others. But, to the extent that imposing even a temporary delay in the progress of a rival is valuable, and where the technology in question is amenable to effective decoupling, the tactic offers an attractive option.

This paper is organized in two parts. First, we examine the case study of satellite technology, evaluating the effectiveness of decoupling as a strategy in that domain and the factors that shaped success and failure. Second, we apply those lessons to the contemporary case of artificial intelligence, finding that while aspects of AI competition do support the need to find ways of imposing even temporary delay in rival progress, the tactic of decoupling is fundamentally limited in achieving this end.

Part I: Decoupling in Space

The U.S.-China relationship in space technology, specifically satellites and their respective components, provide an excellent historical case study from which to examine the effectiveness of "decoupling" as a tactic for preserving a nation's advantage in a strategic technology for two reasons.

First, satellites represent a technological domain that has been definitively "decoupled," providing an opportunity to examine the impact of such policies. Beginning from a period of scientific and economic cooperation around space technology in the 1990s, the present state of play is characterized by one researcher as featuring "almost no direct links between the United States and China with regard to space technology research, development, and operations thanks to various export controls and limits on bilateral engagement with China counterparts."[3]

Second, decoupling can serve a variety of different ends in national competition. Satellite technologies are particularly useful for this analysis since the specific intent of pursuing a decoupling strategy—focused around nonproliferation objectives—eventually had broader implications for the competitiveness of the United States and U.S. firms in space technologies. In this sense, the means (decoupling), the desired ends (preventing China from developing advanced conventional weapons), and the eventual long-term, albeit unintended effects provide important lessons for contemporary discussions around decoupling tactics.

This section reviews the historical arc of the embargo on satellite technology, extracting a series of lessons in whether and how decoupling regimes can be effective. This provides a useful framework for analyzing whether decoupling regimes might play a similar role in AI.

A Brief History of U.S.-China Relations in Space Technology

China harbors long-standing ambitions to establish a comprehensive space program.[4] In the early years of China's space program, the majority of its advancements in the area came via expertise from the Soviet Union. However, as the Sino-Soviet relationship began to sour in the late 1950s, the Chinese found themselves forced to rely on their indigenous abilities for the next two decades.

During this period, China made significant strides in its intercontinental ballistic missile (ICBM) program, due in part to the expertise of U.S.-trained scientist Qian Xuesen after he was driven out of the United States over fears of espionage.[5] As the result of these efforts, China launched its first satellite in April 1970.[6] Successor systems known as Long March 2A and 2C were first successfully deployed in 1975 and 1982, respectively. These rockets became the standard platform used by Chinese military and space programs through the end of the twentieth century.[7] However, outside of its progress on ICBMs, China's space activities were relatively limited during the 1960s and 1970s, primarily due to small government budgets and the loss of a generation of science and technology talent during the Cultural Revolution.[8]

In the early 1970s, U.S. policymakers moved towards a reconciliation with China out of a desire to counter Soviet influence in the Cold War. After the establishment of diplomatic relations in 1979, initial space cooperation began when Chinese Premier Deng Xiaoping visited NASA's Johnson Space Center in January of that year.[9] In the late 1980s, the two sides signed three separate agreements that would allow for the launch of three U.S.-built satellites on Chinese rockets. These agreements allowed for the export of the then-advanced U.S.-built AUSSAT and Asiasat-1 satellites to China.[10]

Despite tensions between the United States and China resulting from the Tiananmen Square massacre in 1989, both the George H. W. Bush and Bill Clinton administrations continued to push U.S.-China space cooperation forward. Between 1989 and 1998, Presidents Bush and Clinton issued 13 Presidential waivers for 20 satellite projects based on "national interest," allowing U.S.-origin satellites or components that were otherwise subject to export controls to be exported to China.[11] In 1993, the Clinton administration announced that it would review commercial satellite export control regulation to speed up and complete a shift from the State Department's more restricted Munitions List to the Department of Commerce's Commerce Control List. According to Sciences Po's Hugo Meijer, this "desire to shift authority to the Commerce Department . . . reflected the evolution of satellites from a military to a civilian technology."[12]

Turning Point: The Loral and Hughes Cases

Incidents involving two U.S. companies in 1998—Hughes Electronics Corporation and Loral Space & Communications—represented a turning point in U.S.-China space cooperation, pushing the two countries toward decoupling and setting the stage for the current bifurcation in bilateral space relations.

In April 1998, it was first reported that the U.S. Department of Justice had initiated a criminal investigation into Hughes and Loral for possible violations of export control laws.[13] This came in the aftermath of several launch failures of U.S.-built satellites on

Chinese rockets that resulted in insurance investigations. These investigations revealed that Hughes and Loral were found to have shared sensitive technical information on guidance systems with Chinese engineers—information that was deemed to have likely been used to improve the accuracy and reliability of Chinese missiles, according to scholar Shirley Kan.[14]

U.S. policymakers criticized the Clinton administration for allegedly putting economic interests ahead of national security in its attempts to liberalize the export control regime. In response, the House Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China was established in June 1998, and their resulting investigation, known as the Cox Report, highlighted the degree to which Loral and Hughes had helped advance Chinese military capabilities in space technology.[15]

Ultimately, the core national security concern raised by these findings was that this assistance accelerated the pace of technological advancement in the space domain by China. As the committee concluded, the support of Hughes and Loral "led to improvements in the PRC's rockets and that the improvements would not have been considered or implemented so soon without the U.S. assistance."[16] In response to these findings, the committee recommended that the executive branch "aggressively implement satellite export control provisions from the . . . National Defense Authorization," and that the "State Department should have sole satellite licensing authority."[17]

These conclusions were controversial, with multiple experts critiquing the findings of fact and policy recommendations made by the committee.[18] Despite these criticisms, the 1999 National Defense Authorization Act (NDAA) directed that "all satellites and related items that are on the Commerce Control List of dual-use items . . . shall be transferred to the United States Munitions List,"[19] thereby defining in legal terms commercial satellites and related components as defense articles under the Department of State's Munitions List.

These policies "ended U.S.-China space cooperation."[20] Since the passage of the 1999 NDAA, China and the United States have maintained little to no interaction in space exports, research, or collaboration. Subsequent policies since 2000 have furthered U.S.-China decoupling in space. Notably, a 2011 amendment to the Commerce-Justice-Science Funding Bill, often referred to as the Wolf Amendment, sought to limit U.S. government agencies, including NASA, from working with Chinese commercial or government counterparts.[21]

Lessons from Decoupling in Satellite Technology

The legacy of U.S.-China relations in space technologies offer a valuable case study of an "already decoupled" domain that provides lessons to policymakers and researchers assessing the potential impact of implementing similar policies in a range of strategically important emerging technologies.

Two key lessons emerge. First, decoupling should be seen as a means of imposing a delay, rather than categorically halting the ability for a rival to reach parity in a particular technological domain. In the context of satellite technologies, stringent export control regimes do appear to have imposed hurdles in Chinese progress. However, in recent years, China has caught up and even exceeded U.S. capabilities in some respects in spite of these restrictions on technology transfer.

Second, decoupling is not a catch-all tool: the specific characteristics of a technology can make it more or less amenable to control by these tactics. In the satellite domain, the success of the decoupling regime in temporarily slowing Chinese progress around space technologies was due in part to specific aspects of the supply chain. Satellite technology historically featured a high level of geographic concentration, with a small number of U.S. companies controlling much of the global market share. This allowed export control regimes to more efficiently limit Chinese access to key components.

Lesson 1: Decoupling as a Delaying Stratagem

Decoupling from China in space via tools like export controls has limited technology transfer and appears to have inhibited satellite launch activity in China during the years immediately following the 1999 NDAA.[22] However, Chinese capabilities in space technologies have advanced over time even in spite of these restrictions.

There are a few reasons for this. For one, key components and expertise have become available elsewhere outside the United States. Meijer argues that the U.S.'s decision to unilaterally apply International Traffic in Arms Regulations (ITAR) export controls has been counterproductive, as it attempted to control technologies that were not as tightly regulated by other foreign governments and widely available from other sources.[23] Secondly, espionage remains one means of acquiring key technologies and evading export controls.[24] Even as recently as 2021, a senior NASA scientist pleaded guilty to charges that he had failed to disclose participation in China's Thousand Talents Program, a government-sponsored recruitment program aimed at recruiting overseas individuals with access to strategic technology or intellectual property.[25]

Moreover, the decoupling regime may have played a role in simultaneously inhibiting U.S. technological progress and competitiveness, making it easier for Chinese capabilities to catch up.[26] ITAR satellite export controls have harmed the U.S. space industrial base and favored international competitors, resulting in the decline of U.S. satellite market shares and revenues.[27] In 2014, the Department of Commerce's Bureau of Industry and Security estimated that between $988 million and $2 billion of foreign sales had been lost to U.S. industry between 2009 and 2012 due to export controls.[28]

Some experts have also argued that the talent decoupling that has arisen from the Wolf Amendment has further disadvantaged the United States by driving a deeper wedge between the United States and its allies, as well as by disrupting potential collaborations that could lead to innovation. In 2018, China's Ambassador to the United Nations, Shi Zhongjun, announced a memorandum of understanding with the UN Office for Outer Space Affairs to invite applications from other UN member states to conduct experiments on-board China's Space Station (CSS).[29] Due to Wolf Amendment restrictions, U.S. researchers are unable to participate in this collaboration, keeping them out of the loop on collaborative research and development efforts that may be happening aboard the CSS.

Ultimately, a 2020 report from the U.S.-China Economic and Security Review Commission argues that China has now emerged as a leading player in space despite U.S. efforts, due in part to a domestic push to indigenize space R&D capabilities without the assistance of U.S.-origin technologies. The report went on to conclude that the progress China has made in space technologies now has the potential to deny the United States and allies access to similar systems, and that China is now in a position to achieve disruptive breakthroughs in various space technologies, including satellites and counterspace capabilities.[30]

This assessment has been reaffirmed by those in the U.S. Department of Defense. Former Commander of U.S. Strategic Command, General Kevin Chilton, stated in 2009 that he was "highly concerned that our own civil and commercial space enterprise, which is essential to the military space industrial base, may be unnecessarily constrained by export control legislation and regulation."[31] The 2019 Industrial Capabilities Report to Congress by the Department of Defense's Office of Industrial Policy notes that DOD's reliance on the commercial space sector imposes sources of vulnerability, as it creates a "need to sustain fragile domestic sources."[32]

The case study of space technologies highlights that decoupling is at best a tool of delay. Chinese progress has not been halted by the restrictive decoupling regime in satellite technologies implemented in the wake of the Loral and Hughes cases. Instead, progress has been merely delayed, as the emergence of alternative sources for talent and technology, espionage, and ebbing U.S. competitiveness have chipped away at the effectiveness of the decoupling regime in blocking Chinese advancement.

Lesson 2: Geographic Concentration Influences Decoupling Effectiveness

The space technology case tempers optimism about the use of decoupling as a tool for preventing a rival from accessing emerging, strategically important technologies. It is also a useful case study since it suggests that the effectiveness of a decoupling regime can depend greatly on the specific characteristics of the technology in question. One major factor that stands out in the satellite technology example is the important role that a geographically concentrated supply chain plays in decoupling effectiveness.

Technologies that have a small number of manufacturers concentrated in a handful of countries lend themselves more naturally to effective export control regimes, since there are fewer alternative routes through which a rival might gain access to key technologies. Unilateral U.S. export controls initially slowed Chinese progress in satellite technology during an era in which U.S. firms simultaneously controlled much of the global market share. However, as “ITAR-free” alternatives to U.S. providers became viable during the 2000s, so too did these controls see reduced effectiveness.[33]

Satellites which contained no components covered by the U.S. exports control regime (so-called “ITAR-free” satellites) emerged in the early 2000s. These satellites could be acquired and traded more easily than those with components subject to ITAR and offered customers faster delivery of products. In particular, European institutions like Thales Alenia Space, with support from the European Space Agency, hoped these products would reduce their dependence on U.S. components and provide access to the growing Chinese market. These products grew in popularity and quality. By 2008, one analysis concluded that European providers had achieved “relative parity in commercial system capabilities” based on a comparison of key features such as satellite size, transponder count, and power output.[34]

The rise of an alternative source of satellite technology reduced the ability for the U.S. to limit rival access. A 2007 report prepared by the European Commission emphasized that ITAR-free products and services have allowed European manufacturers to gain significant market shares, while the U.S. business suffered from a substantial disadvantage.[35] Thales Alenia Space, for instance, saw its market share jump from around 10 percent prior to the implementation of U.S. export controls, to around 20 percent by 2004.[36] This growth has been driven, in part, by Chinese acquisition of these satellites.[37] Since the Cox Report and the 1999 NDAA, as a result of ITAR export controls, the U.S. share of the global commercial satellite market has declined significantly from 73 percent in 1995 to 25 percent in 2005.[38] It has since risen to 44 percent in 2018, although it has yet to reach its pre-Cox Report levels.[39]

Geographic concentration also reduces the coordination costs of forging effective decoupling regimes internationally. Technology transfer regimes are only as strong as their weakest link; failure to coordinate strategic economic policies offers opportunities for adversaries to exploit and renders the regimes impotent. During the Cold War, stringent U.S. regulations on technologies surrounding submarines were ultimately undermined by technology transfer between the Soviet Union and restive U.S. allies with access to cutting-edge milling and computer equipment.[40] For decades, policymakers, defense analysts, academics, and industry executives have affirmed the vital need for international cooperation in restricting access to emerging technologies.[41] This posed a major problem for export controls during the Cold War, and applies to modern attempts to use decoupling tactics, as well.[42]

Part II: Lessons for Artificial Intelligence

AI has emerged as a focal point of national competition in advanced technology between the United States and China.[43] This has included major initiatives to accelerate the pace of research, recruit lead talent, and set global standards around the technology.[44]

While the set of high priority, strategically critical technologies is continually evolving, many of the core policy tools for influencing them remain the same. It is perhaps no surprise then that the tactics of decoupling have been proposed as a means for slowing Chinese progress in the technology.[45] This includes a range of investment restrictions, export controls, and tariffs.[46] As with debates around satellite technologies in decades past, the severing of supply chains through export control appears to provide an attractive option for preserving the U.S. advantage.

Does decoupling provide a strong policy option for the United States to preserve its technological advantages in AI? The lessons drawn from the example of satellite technology provide a useful framework for analysis, requiring us to examine two underlying questions. First, given that decoupling is likely to be a temporary strategy of delay, would imposing such a delay be valuable to U.S. interests? Second, if imposing such a delay is indeed attractive, does AI as a technology possess the attributes that make it effectively "decouplable"?

Our analysis concludes that while imposing delays on China's progress on AI may be attractive in the abstract, the specific characteristics of machine learning (ML)—the subfield of AI responsible for most of the recent advances in the technology—make decoupling a highly ineffectual tactic for achieving this end. We address each of these questions in turn.

Strategic Delay in Artificial Intelligence

Before reaching the question of whether or not decoupling is feasible, it is critical to confront the question of whether or not delaying rival progress in a strategic technology is desirable. The answer to this inquiry is not always "yes." There are many ways that delaying tactics can backfire against the aggressor: as illustrated in the satellite context, decoupling can alienate allies, inhibit domestic industry, and prompt the creation of industry alternatives that isolate a technology leader over time. Moreover, efforts at delay pose their own opportunity costs. Expending money and effort on "running faster" may ultimately be a more productive approach to competition in strategic technologies than attempting to slow a rival down.

To that end, it is necessary to examine whether or not the strategic dimensions of competition in AI suggest that imposing delay in technological progress is of unique importance. There are three key reasons to believe that it is.

First, as an emerging technology, ML features significant implicit knowledge that is acquired by engineers and researchers through their work with veteran participants in the field. These core clusters of researchers are likely to create "knowledge spillovers" that lead to a disproportionate level of innovation concentrating in a handful of regions and organizations.[47] In this initial nascent period, it may be particularly important to delay access of a rival nation to a core technology since it limits the ability to foster competing research clusters. This may result in compounding advantages over time as a rival remains dependent on talent and innovations coming from a competitor country even as the technology matures.

Second, industrial competition over AI awards first-mover firms. This is due to the tight relationship that exists between data and high-performance ML systems. Firms that are able to launch early and establish market share around a ML service are able to continuously acquire data that in turn accelerates the improvement of those systems. This can make it challenging for laggard firms, from whom limited market share translates into a scarcity of data assets to create competitive products. This dynamic has manifested in a range of ML product areas, including search and translation.[48] Insofar as national leadership in a technology is a function of the leadership of firms based within a country, this factor may favor imposing delays to allow domestic leading firms to establish their first-mover dominance over a technology.

Finally, while the United States leads in AI in many respects, its integration into key areas such as military applications remain confounded by a range of organizational issues that slow adoption and deployment.[49] This "deployment gap" may mean that adversaries that might begin with less sophisticated versions of a strategic technology may nonetheless achieve superiority by integrating and deploying it faster than the United States. Blocking access to a rival, even temporarily, is critical in this context since it provides the necessary time for the United States to deploy first and leverage the full advantages of the technology.

Is Artificial Intelligence Decouplable?

Insofar as the competitive dynamics around AI make even a temporary delay on rival advancement attractive, the second question is whether decoupling is the most effective method for achieving that end. As the examination of satellite technology suggests, geographic concentration is a key determinant in whether or not decoupling is effective.

ML does not appear to be an attractive candidate for decoupling when viewed through this lens. Developing ML technologies depend critically on access to three inputs: (1) data, which provides the raw material for training AI systems, (2) algorithms, which facilitate the process of extracting useful patterns from data, and (3) computational power, the hardware necessary to perform the training process.[50] Presently, lack of access to any one of the elements of this "AI triad" can significantly hinder attempts to develop and deploy these systems.

To that end, any decoupling regime seeking to limit rival progress in the technology would need to target data, algorithms, computational power, or some combination of the three. However, each of these key inputs feature characteristics that raise doubts about the ability of decoupling regimes to be effective. Data and algorithms are too geographically distributed to be easily amenable to an export control approach. Computing power, while geographically concentrated, is for a number of reasons only a narrow lever for influencing rival progress in the technology.

As a whole, this analysis suggests that a decoupling approach would be a largely ineffectual route to inhibit rival advancement in AI writ large, even as it suggests some options in hindering progress of specific applications of the technology.

Data: Too Ubiquitous for Decoupling

Data distinguishes AI from the algorithms of bygone eras. An AI system learns how to complete a task based on patterns it discerns from data, rather than relying on prewritten "if/then" rules. An explosion in data collection and availability partly facilitated the new AI research boom of the 2010s.[51]

Data is specific in utility, ubiquitous in collection, disaggregated in storage, and typically commercial in application. It is generated by thousands of industrial control systems, millions of GPS relays, billions of smartphones and personal computers, and apps for everything.[52] These features, among others, are what led CSET Fellow Carrick Flynn to conclude in 2019 that "[e]xpanded export controls on general purpose AI software, untrained algorithms, and most datasets are unnecessary and likely counterproductive to U.S. leadership in AI."[53] Put succinctly, data is so foundational to 21st century life, it cannot be effectively controlled.

This fact makes the creation of a decoupling regime categorically limiting the flow of data of all kinds across borders a daunting prospect. However, data is not a fungible resource. Feeding a neural network millions of X-ray images can help it diagnose lung cancer, but will certainly not enable the system to drive a car autonomously.[54]

This means that there may be some promise in targeted limitations of certain kinds of data critical for strategically important applications of AI, for instance particularly sensitive datasets collected and used by militaries. Scientists at China's leading defense companies, for example, frequently lament that they do not have sufficient access to datasets required to build and run AI for military applications—like X-band radar images of targets taken from missile seekers.[55] This kind of data is not commercially available and not easily substituted, and access to it is a significant barrier in developing AI systems that are robust and reliable enough to be deployed on the battlefield. But the United States has already adopted security measures to protect this kind of information, and much of it was not being shared with the Chinese military at the onset.[56]

The bottom line is that the international dissemination of data writ large is not easily amenable to control by public policy. Global data supply chains are too large, unwieldy, and interconnected—and U.S. firms stand too much to lose—for the United States to restrict the sale of or access to broad categories of commercial data. Narrower policies focusing on protecting specific datasets, such as niche, militarily-specific images or citizen genetic information, may be a means of blocking rival progress in certain key AI application areas. However, prospects for broad "data decoupling" are slim.

Algorithms: Not Much Better

Algorithms are what most people think of when they hear "artificial intelligence." They are the reasoning models that allow AI systems to mimic intelligence—lines of code that "govern how machine learning systems process information and make decisions."[57]

There are several kinds of algorithms used in ML systems, but all are difficult to regulate or control, for many of the same reasons as data. They are strings of code built on computing architectures, capable of being emailed, saved on an external hard drive, or simply uploaded to online repositories such as GitHub, which recorded almost 2 million contributions from 56 million developers in 2020.[58] This is to say nothing of the growing, remote AI software licensing industry.[59] Among democracies, it is unlikely that regulatory and law enforcement agencies could monitor the online transaction of information such that they could reasonably know when and where AI algorithms change hands. Doing so would require restricting access to open-source repositories like GitHub, closing off vectors of open-source research collaboration, and hamstringing the U.S. AI industry.

Given the AI sector's reliance on international research collaboration, imposing meaningful export controls would be nothing short of a mortal blow to AI research and development.[60] But even in a tightly controlled digital panopticon, distinguishing between ML models capable of recognizing military targets—vice those capable of identifying school buses and stop signs—would be an unreasonably tall order. AI is not a dual-use component; it is a field of general-purpose technology. The same language transformer being used to identify famous paintings and generate websites is capable of unleashing a wave of disinformation.[61]

While the distributed nature of ML models makes a broad decoupling regime targeting this input unlikely, more targeted approaches seeking to control algorithms in certain domains may be possible. One present-day illustration can be seen in the fact that the risk of abuse inherent in some AI systems is leading some developers to delay publishing or restrict access to the most cutting-edge models.[62]

The research lab OpenAI, for example, restricted access to its generative language model GPT-2 more than six months after announcing its existence to the public.[63] In a blog post entitled "Better Language Models and Their Implications," the lab warned that its language model could generate misleading news articles or impersonate others online, and urged researchers and governments to consider the societal risks of advanced transformers.[64] For its massive, 175-billion-parameter successor, GPT-3, OpenAI did not open the source code at all, but created an API off of which developers could build applications.[65] Today the lab vets and grants interested researchers access to the API to work only within approved research areas.[66]

Yet even here there are doubts that a narrower, more targeted decoupling regime would be able to effectively limit rival progress even on specific application areas of AI. For one, the wide distribution of research results within the field and availability of open-source software means that it can be straightforward for a rival to access near-substitutes for a strategically critical algorithm.

GPT-3 offers a good illustration of this. While OpenAI was indeed able to limit access to its uniquely advanced language model for a period of time, similarly advanced substitutes were available in open-source channels a little more than a year later.[67]

Decoupling regimes targeting algorithms would likely confront similar challenges in limiting rival access.

Second, algorithms are ultimately pieces of software, meaning that they are easy to distribute and nearly costless to copy and store. This may make decoupling regimes targeting algorithms uniquely vulnerable to being undermined through espionage. Rather than requiring the exfiltration of a physical component, a rival simply needs to obtain access to a computer system containing the algorithm to cripple an algorithm-focused decoupling effort.

Algorithms for ML are unpromising targets for a decoupling regime for many of the same reasons as data: they feature a diffuse and widely distributed supply chain. Narrower decoupling regimes targeting specific kinds of algorithms are also unpromising since substitutes are likely to be easily accessible to a rival and vulnerable to espionage.

Compute: A Possible Option?

Of the three major inputs to the "AI triad," computing power stands alone as an obvious target for a decoupling regime given the geographic concentration of its supply chain. These are processors designed expressly to handle the computationally demanding needs of AI systems. As prior CSET research indicates, only cutting-edge AI chips, typically with a transistor density of 10 nanometers or below, are suitable to train and run cutting-edge neural networks.[68] Older computer chips take too much time—sometimes months—and generate millions of dollars in electric bills.[69] Chips are discrete, physical products, produced in batches with serial numbers from a handful of known factories on earth. Those factories are principally located inside the continental United States and among some of its chief partners: Japan, South Korea, and Taiwan.[70]

What's more, while the United States and its allies are ahead in AI chip production, China is behind. In their report *AI Chips and Why They Matter*, Saif M. Kahn and Alexander Mann explain that even though Chinese firms are becoming more competitive in designing AI chips, even well-known design firms such as HiSilicon "outsource manufacturing to non-Chinese fabs, which have greater capacity and exhibit greater manufacturing quality"—particularly those in the United States, Taiwan, and South Korea.[71] In 2020, foreign imports filled 84 percent of the Chinese market for semiconductor devices.[72] Other analysts have concluded that "Beijing has 'no prospect' of reaching its goal of 70 percent self-sufficiency by 2025."[73]

China's chip dependency on the United States and its strategic partners has created a situation that is particularly conducive to export controls. For twenty years, U.S. government policy has intended to keep Chinese semiconductor manufacturing capability approximately two chip "generations" behind that of U.S. firms, although the gap has been narrowing.[74] Military end-users in China are, in theory, unable to purchase high-end AI chips from the U.S.-based firms that make them, and the U.S. government has worked to persuade allies to adopt similar export control regimes.

These export controls on advanced semiconductor devices have met some success. Engineers at Chinese defense state-owned enterprises frequently complain that they lack the requisite advanced AI chips to develop and deploy AI.[75] Restrictions on military end-users have cut the revenue of China's premier technology companies, including Semiconductor Manufacturing International Co. and Huawei, its principal customer.[76]

The semiconductor supply chain is concentrated at multiple levels, making it even more promising as the target of a decoupling regime. Semiconductor factories—referred to as foundries—themselves rely on equipment that is itself concentrated. For instance, an extreme ultraviolet (EUV) photolithography machine is a semiconductor foundry's most sophisticated and expensive tool, enabling cost-effective mass production of the most cutting edge and powerful processors.[77] Of the five subject matter experts CSET interviewed regarding AI decoupling, all cited lithography as a chokepoint technology in AI development, and three specifically discussed the role of extreme ultraviolet lithography.[78] Just two companies in the world manufacture the photolithography equipment required to fabricate high-end chips: ASML in the Netherlands, and Nikon in Japan.[79] Only ASML produces high-end EUV equipment. Despite Beijing's redoubled efforts to catch up in semiconductor manufacturing equipment, Chinese firms remain reliant on foreign firms for several components in the semiconductor manufacturing equipment.[80]

The Fragility of Compute-Based Decoupling

Given the high degree of geographic concentration in the supply chain, computational power would initially appear to be promising candidate for a decoupling regime targeted at slowing rival progress in the technology. However, a deeper examination suggests that such a compute-focused decoupling regime would be fragile at best for achieving this end. While export controls focused on the semiconductor supply chain may effectively inhibit rival ability to make progress on some aspects of AI, there are three reasons to believe that these limitations will be narrow in scope and potentially short-lived.

First, superior access to computational power may ultimately offer only limited advantages in advancing the capabilities of AI systems. Expanding computing power has facilitated significant leaps in the capabilities of ML systems in recent years, but these gains may ultimately be confined to improving AI performance along certain dimensions.[81]

Researchers have observed that current ML systems may not be able to fully achieve the broader ambition of giving computers a wide range of cognitive abilities. The ability for computers to reason causally, for instance, may be one task that is impossible to achieve purely through the current data- and compute-intensive methods of performing ML.[82] This may limit the effectiveness of existing ML systems in key areas such as medicine, where the ability to identify a causal relationship between a treatment and an outcome may be critical.[83] Similarly, existing ML paradigms may be unable to successfully recognize the presence of "distributional shift," a common failure mode whereby an AI system is unable to adjust successfully to a new context.[84] This may limit the application of the technology in high-stakes scenarios where rigid behavior on the part of the AI system would create danger for operators.

Broadening the range of cognitive capabilities for machines may depend less on access to superior computing power and more on advancements in algorithm architecture and in the processing of data. Much work in the subfield of causal inference relies on improving system behavior without requiring significant leaps in computational power. To the extent that this is the case, limitations on rival access to computational power may only create narrow limitations on a rival's ability to acquire important capabilities in AI.

Second, cutting-edge chips are critical specifically in training, the process by which a ML system first acquires the ability to achieve a defined task. But it is unclear that limiting rival access to training new models will be the strongest determinant of national competitiveness in this emerging technology.

For one, a rival is likely to have access to a rich corpus of pretrained models in open-source repositories, the private marketplace, and through espionage. As explained above, ML models are ultimately software and are challenging to control through export controls and other tools of economic decoupling. Moreover, harnessing the benefit of AI may depend less on the ability to originate new models than the ability to effectively deploy existing models for practical use in the field. Solving these "last mile" deployment issues in—for instance, enabling AI systems to work on low-energy devices—does not rely on access to superior computing power but may be a significant determinant in the practical impact of these technology on national power.

Finally, advancements in algorithms may significantly blunt the impact of a decoupling regime focused on limited access to computational power. Researchers have had success in recent years in developing techniques that retain the effectiveness of ML systems while significantly decreasing the computational power necessary to train and operate them. These include subfields of research focusing on tasks such as dimensionality reduction, the simplification of data to improve model training and reduce computational load.[85] It also includes areas of study such as model pruning, which focus on allowing a compression of the size of a model to improve speed and lower power and compute consumption on resource-constrained devices.[86]

Conceptual breakthroughs in any of these subfields could significantly offset the advantages that superior computational power has in advancing the state of the art. Decoupling regimes premised on the need for computational power to train AI systems will be similarly vulnerable to developments in the field. Indeed, a restrictive decoupling regime limiting access to advanced chips is likely only to accelerate rival investments in making “low compute” ML systems practicable. The limits placed on rival progress through decoupling then, may be brittle to these shifts in the research field.

Conclusion: Means and Ends

The U.S. experience in decoupling satellite technologies highlights the importance of clarity on means and ends when analyzing the prospects of an export control or similar regime. Decoupling is a tactic that might plausibly be deployed to achieve a variety of different national ends, with the delay of rival progress on a strategically important technology being just one possible objective. Similarly, the objective of delaying rival progress is in turn achievable through a variety of different means, the severing of supply chains through decoupling being just one possible tactic.

The historical experience of satellite technologies highlights the need to approach decoupling with tempered expectations. To the end of blocking rival access to a technology, even stringent decoupling appears to be at best only able to delay, rather than categorically halt rival progress. The satellite example also limits our expectations about where decoupling will be effective as a means: these tactics appear more effective in the case where a geographic concentration of supply chains makes it more possible to control the flow of the technology through export controls and other measures.

These factors provide a guide to assessing the promise of strategic decoupling in contemporary emerging technologies. In the context of AI, imposing even temporary delays on rival progress in the technology may be highly valuable. However, the diffuse nature of its inputs in data and algorithms makes it unlikely that decoupling is an effective means of achieving this end. The one exception—computational power—provides a tenuous lever: while the supply chains present the necessary concentration, it is unclear that limiting access to this input is an effective means of denying a rival the ability to advance in the technology over the long run.

While the case for decoupling in AI is a weak one, it represents just one path for achieving a strategic delay in rival progress. Alternative tactics such as leveraging immigration policies to acquire top research talent, releasing technologies that undermine the high-value applications of AI for a rival, and the shaping of technical standards all can work towards slowing rival progress more effectively.[87] Competition in AI features numerous first-mover advantages that justify a continued search for alternative tactics of delay in the ongoing national competition around these strategically critical technologies.

Authors

Tim Hwang and Emily Weinstein are research fellows at CSET.

Acknowledgements

The authors acknowledge Catherine Aiken, Dale Brauner, Jeffrey Ding, Ryan Fedasiuk, Doug Fuller, Igor Mikolic-Torreira, John VerWey, and Kevin Wolf for their invaluable feedback and comments on earlier drafts of this report. Additionally, the authors would like to recognize Adam Kline, who provided extensive research and literature review in support of this project. Thanks also to Lynne Weil, Shelton Fitch, and Jess Shao for their assistance in reviewing, editing, and formatting this paper.

Document Identifier: doi: 10.51593/20200085

Appendix A: Interview Protocol and Expert Identification and Recruitment

The research team consulted existing literature, professional networks, and their own knowledge to compile a list of subject matter experts for this study. The team targeted individuals with expertise, demonstrated by publication or professional position, in one of the following areas: space, biotechnology, or AI/ML. The team invited 35 experts to participate in an interview and interviewed 23 experts between November and December 2020.

Eighteen interviews were conducted virtually, recorded and transcribed in full. Four interviews were conducted virtually but the interviewee requested not to be recorded and one interviewee provided responses electronically. Several experts were interested in the research, but did not have the time or authorization to participate in an interview.

Ultimately, these interviews guided further desk research into the historical record of export controls, and shaped research team understanding of how those lessons were applicable or not to contemporary discussions in the biotechnology and AI/ML space. To focus the analysis in this report, findings on AI/ML were incorporated into the final draft, with the findings on biotechnology being reserved for future work.

All interviews followed the semi-structured protocol below:

1. In your industry, how can public policy be used to control relevant supply chains, if at all?

2. We identified four criteria for defining what we call a "linchpin" technology - meaning a high-value technology that is amenable to decoupling in ways that advantage the United States. The four criteria are listed below. What technologies in your industry match these criteria and could be considered linchpin technologies?

    Strategic Vulnerability: The loss of private leadership in the technology or the future inability to shape the supply chains of the technology would place the United States at a significant economic/military strategic disadvantage.

    Comparative Advantage: The U.S. possesses a comparative advantage in the technology relative to its rivals.

Import Dependence: Rivals currently depend on imports to produce or use the technology.

Controllable: There is the possibility for U.S. policy to influence the global supply chain.

3. In your industry, what are the relative strengths, or comparative advantages, of the United States relative to China? What about U.S. allies relative to China?

4. Do you think these advantages will endure over the long term or are they temporary? Why?

5. How much interaction does your industry have with Chinese companies and researchers? What is the nature of those interactions?

Endnotes

[1] For a review of the many motives driving decoupling policy, see Jon Bateman, *U.S.-China Technological 'Decoupling': A Strategy and Policy Framework* (Washington, D.C.: Carnegie Endowment for International Peace, 2022), https://carnegieendowment.org/2022/04/25/u.s.-china-technological-decoupling-strategy-and-policy-framework-pub-86897.

[2] Brandon L. Van Grack and James Brower, "CFIUS's Expanding Jurisdiction in the Magnachip Acquisition," *Lawfare*, October 11, 2021, https://www.lawfareblog.com/cfiuss-expanding-jurisdiction-magnachip-acquisition.

[3] Matthew Daniels, *The History and Future of US-China Competition and Cooperation in Space* (Baltimore, M.D.: The Johns Hopkins University Applied Physics Laboratory, 2020), https://www.jhuapl.edu/Content/documents/Daniels-Space.pdf.

[4] Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China, *Final Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China,* 105th Congress, 2nd Session, January 1999 (Washington, D.C.: U.S. Government Printing Office, 1999), https://www.govinfo.gov/content/pkg/GPO-CRPT-105hrpt851/pdf/GPO-CRPT-105hrpt851.pdf.

[5] Tianyu Fang, "The Man Who Took China to Space," *Foreign Policy*, March 28, 2019, https://foreignpolicy.com/2019/03/28/the-man-who-took-china-to-space/.

[6] Select Committee, *Final Report.*

[7] Select Committee, *Final Report.*

[8] Daniels, *The History and Future.*

[9] Zhihui Zhang and Bruce Seely, "A Historical Review of China-U.S. Cooperation in Space: Launching Commercial Satellites and Technology Transfer, 1978-2000," *Space Policy* 50 (November 2019), https://www.sciencedirect.com/science/article/abs/pii/S0265964618300079.

[10] Marcia S. Smith, "China's Space Program: A Brief Overview Including Commercial Launches of U.S.-Built Satellites" (Congressional Research Service, September 1998), https://www.everycrsreport.com/files/19980903_98-575_05fb2d841adab0b0fa7670eee5ba1679578923cb.pdf.

[11] Hugo Meijer, *Trading with the Enemy: The Making of US Export Control Policy Towards the People's Republic of China* (New York, NY: Oxford University Press, 2016): 220-221; "China: Possible Missile Technology Transfers Under U.S. Satellite Export Policy – Actions and Chronology" (Congressional

Research Service, October 2003), https://www.everycrsreport.com/files/20031006_98-485_da6014009a3511321a51c2ee3b73f061906f7bf5.pdf.

[12] Meijer, *Trading with the Enemy,* 213.

[13] "China: Possible Missile Technology."

[14] Meijer, *Trading with the Enemy*, 222-228.

[15] Select Committee, *Final Report.*

[16] Select Committee, *Final Report*, xv.

[17] Select Committee, *Final* Report, 170; Meijer, *Trading with the Enemy,* 227.

[18] Alastair Ian Johnston, W.K.H. Panofsky, Marco DiCapua, and Lewis R. Franklin, *The Cox Committee Report: An Assessment* (Stanford, C.A.: Center for International Security and Cooperation, 1999), https://cisac.fsi.stanford.edu/publications/cox_committee_report_the_an_assessment.

[19] Strom Thurmond National Defense Authorization Act for Fiscal Year 1999, Public Law 105-261 (October 17, 1998), https://www.congress.gov/105/plaws/publ261/PLAW-105publ261.pdf.

[20] Meijer, *Trading with the Enemy*, 228.

[21] Consolidated and Further Continuing Appropriations Act, 2012, Public Law 112-55 (November 18, 2011), https://www.congress.gov/112/plaws/publ55/PLAW-112publ55.pdf; Makena Young, "Bad Idea: The Wolf Amendment (Limiting Collaboration with China in Space)", *Defense360*, December 4, 2019, https://defense360.csis.org/bad-idea-the-wolf-amendment-limiting-collaboration-with-china-in-space/.

[22] Shirley A. Kan, "China: Possible Missile Technology Transfers Under U.S. Satellite Export Policy – Actions and Chronology" (Congressional Research Service, October 2003), 37, https://www.everycrsreport.com/files/20031006_98-485F_da6014009a3511321a51c2ee3b73f061906f7bf5.pdf.

[23] Meijer, *Trading with the Enemy.*

[24] For a summary of some recent incidents, see Justin Rohrlich and Tim Fernholz, "China is trying to steal military space tech. The US is running stings to stop it," *Quartz*, September 16, 2019, https://qz.com/1702414/inside-the-fight-to-keep-us-military-space-tech-out-of-china/.

[25] Department of Justice, "Senior NASA Scientist Pleads Guilty to Making False Statements Related to Chinese Thousand Talents Program Participation and Professorship," January 13, 2021, https://www.justice.gov/usao-sdny/pr/senior-nasa-scientist-pleads-guilty-making-false-statements-related-chinese-thousand.

[26] For a discussion of these trade-offs in the context of "strategic" technologies broadly, see Jeffrey Ding and Allan Dafoe, "The Logic of Strategic Assets: From Oil to AI," *Security Studies* 30:2 (2021), 182-212, https://www.tandfonline.com/doi/full/10.1080/09636412.2021.1915583.

[27] Meijer, *Trading with the Enemy,* 282.

[28] Office of Technology Evaluation, *U.S. Space Industry "Deep Dive" Assessment: Impact of U.S. Export Controls on the Space Industrial Base* (Washington, D.C.: U.S. Department of Commerce, February 2014), 28, https://www.bis.doc.gov/index.php/documents/technology-evaluation/898-space-export-control-report/file.

[29] United Nations Office for Outer Space Affairs, "United Nations and China Invite Applications to Conduct Experiments On-Board China's Space Station," May 28, 2018, https://www.unoosa.org/oosa/en/informationfor/media/2018-unis-os-496.html.

[30] Mark Stokes, Gabriel Alvarado, Emily Weinstein, and Ian Easton, *China's Space and Counterspace Capabilities and Activities* (Arlington, VA: Project 2049 Institute, 2020), https://www.uscc.gov/sites/default/files/2020-05/China_Space_and_Counterspace_Activities.pdf.

[31] Meijer, *Trading with the Enemy*, 289.

[32] Office of Industrial Policy, *2019 Industrial Capabilities Report to Congress* (Washington, D.C.: U.S. Department of Defense, June 23, 2020), https://www.businessdefense.gov/docs/resources/USA000954-20_RPT_Subj_FY19_ICR_07092020.pdf.

[33] "ITAR-free" is an implication of the International Traffic in Arms Regulations' extraterritorial jurisdictional reach. In essence, items subject to the ITAR, regardless of their size or significance, are always subject to the ITAR, even when incorporated into foreign-produced items destined for nonmilitary applications. Thus, if a foreign satellite company were to buy a U.S.-origin satellite component subject to the ITAR—which included all satellite components until 2014—then the foreign company would need the permission of the State Department to export their satellite from outside the United States. Thus, foreign producers worked to have "ITAR-free" satellites so that U.S. government licenses would not be required to export foreign-made items to third countries, whether China or any other country.

For more information, see: John Hoffner, "The Myth of 'ITAR-Free,'" Aerospace Security, Center for Strategic and International Studies, May 15, 2020, https://aerospace.csis.org/itar-satellite-regulation/.

[34] Michael J. Noble, "Export Controls and United States Space Power," *Astropolitics* 6:3, 260, https://www.tandfonline.com/doi/pdf/10.1080/14777620802469798.

[35] Meijer, *Trading with the Enemy,* 285-286.

[36] Ryan Zelnio, "The effects of export control on the space industry," *The Space Review*, January 16, 2006, https://www.thespacereview.com/article/533/1.

[37] George Abbey and Neal Francis Lane, "The First Barrier: The Impact of Export Controls on Space Commerce" in *United States Space Policy: Challenges and Opportunities Gone Astray* (Cambridge, M.A.: American Academy of Arts and Science, January 2009), https://www.amacad.org/publication/united-states-space-policy-challenges-and-opportunities-gone-astray/section/5.

[38] Meijer, *Trading with the Enemy,* 283.

[39] Satellite Industry Association, "Written Testimony for Patricia A. Cooper," November 20, 2013, https://sia.org/wp-content/uploads/2019/12/SIA-Commercial-Space-Testimony-2013-11-20-FINAL.pdf.

[40] Stephen D. Kelly, "Curbing Illegal Transfers of Foreign-Developed Critical High Technology from CoCom Nations to the Soviet Union," *Boston College International and Comparative Law Review* 12, no. 1 (1989), https://lawdigitalcommons.bc.edu/iclr/vol12/iss1/8/; Wende A. Wrubel, "The Toshiba-Kongsberg Incident," *American University International Law Review* 4, no. 1 (1989), https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1604&context=auilr. For a contemporary analysis, see Andrew Imbrie and Ryan Fedasiuk, *Untangling the Web: Why the U.S. Needs Allies to Defend against Chinese Technology Transfer* (Washington, D.C.: Brookings Institution, April 2020), https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_chinese_technology_transfer_imbrie_fedasiuk.pdf.

[41] J. Fred Bucy, "Technology Transfer and East-West Trade," *International Security* 5, no. 3 (Winter 1980-1981), 140; Pierre Chao, *Toward a U.S. Export Control and Technology Transfer System for the 21st Century* (Washington, D.C.: Center for Strategic and International Studies, 2008), 19, https://www.csis.org/analysis/toward-us-export-control-and-technology-transfer-system-21st-century; Alan P. Dobson, "From Instrumental to Expressive: The changing Goals of the US Cold War Strategic Embargo," *The Journal of Cold War Studies* 12, no. 1 (2010), 106; Ronald A. Finkler et al., *Technology Transfer in a Changing National Security Environment* (Washington, D.C.: Institute for Defense Analyses, December 1990), https://apps.dtic.mil/dtic/tr/fulltext/u2/a232458.pdf; Benjamin H. Flowe, "An Overview of Export Controls on Transfer of Technology to the U.S.S.R. in Light of Soviet Intervention in Afghanistan," *North Caroline Journal of International* Law 5, no 3 (1980), 572, https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1113&context=ncilj; Ellen L. Frost and Angela E. Stent, "NATO's Troubles with East-West Trade," *International Security* 8, no. 1 (1983), 180-181, 200, https://www.jstor.org/stable/2538491; U.S. Congress, House, Committee on Foreign Affairs, Hearing, *The Impact of U.S. Export Controls on National Security, Science and Technological Leadership*,

111th Congress, 2nd Session, January 15, 2010 (Washington, D.C.: U.S. Government Printing Office, 2010), 43, https://fas.org/irp/congress/2010_hr/export.pdf.

[42] Dobson, "From Instrumental to Expressive," 106.

[43] Michael C. Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," *Texas National Security Review* 1, no 3 (2018), https://repositories.lib.utexas.edu/handle/2152/65638.

[44] *The 2021 AI Index Report* (Stanford, CA: Stanford University Human-Centered Artificial Intelligence, 2021), https://aiindex.stanford.edu/ai-index-report-2021/; Neil Savage, "The race to the top among the world's leaders in artificial intelligence," *Nature*, December 9, 2020, https://www.nature.com/articles/d41586-020-03409-8.

[45] Amanda Macias and Kayla Tausche, "U.S. needs to work with Europe to slow China's innovation rate, Raimondo says," *CNBC*, September 28, 2021, https://www.cnbc.com/2021/09/28/us-needs-to-work-with-europe-to-slow-chinas-innovation-rate-raimondo-says.html.

[46] China Senior Analyst Group, "A New Great Game—China, the U.S. and Technology," *S&P Global*, October 1, 2018, https://www.spglobal.com/en/research-insights/featured/a-new-great-game-china-the-u-s-and-technology.

[47] David B. Audretsch and Maryann P. Feldman, "R&D Spillovers and the Geography of Innovation and Production," *The American Economic Review* 86, no. 3 (1996), 630-640, https://maryannfeldman.web.unc.edu/wp-content/uploads/sites/1774/2021/04/knowlege-spillovers-1996.pdf; Yasusada Murata, et al., "Localized Knowledge Spillovers and Patent Citations: A Distance-Based Approach," *The Review of Economics and Statistics* 96, no. 5 (2014), https://direct.mit.edu/rest/article-abstract/96/5/967/58198/Localized-Knowledge-Spillovers-and-Patent?redirectedFrom=fulltext.

[48] For example, see Gideon Lewis-Kraus, "The Great A.I. Awakening," *The New York Times*, December 15, 2016, https://www.nytimes.com/2016/12/14/magazine/the-great-ai-awakening.html.

[49] Danielle C. Tarraf, et al., *The Department of Defense's Posture for Artificial Intelligence: Assessment and Recommendations for Improvement* (Washington, D.C.: Rand Corporation, 2021), https://www.rand.org/pubs/research_briefs/RB10145.html.

[50] Jeff Desjardins, "How much data is generated each day?", *World Economic Forum Blog*, April 17, 2019, https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/.

[51] Desjardins, "How much data is generated each day?"

[52] Daniel Castro, et al., "Who is Winning the AI Race: China, the EU, or the United States?", *Center for Data Innovation Blog,* August 19, 2019, https://datainnovation.org/2019/08/who-is-winning-the-ai-race-china-the-eu-or-the-united-states/.

[53] Carrick Flynn, *Recommendations on Export Controls for Artificial Intelligence* (Washington, D.C.: Center for Security and Emerging Technology, 2020), https://cset.georgetown.edu/research/recommendations-on-export-controls-for-artificial-intelligence/.

[54] Husanjot Chahal et al, *Messier than Oil: Assessing Data Advantage in Military AI* (Washington, D.C.: Center for Security and Emerging Technology, 2020), https://cset.georgetown.edu/research/messier-than-oil-assessing-data-advantage-in-military-ai/.

[55] Ryan Fedasiuk, *Chinese Perspectives on AI and Future Military Capabilities* (Washington, D.C.: Center for Security and Emerging Technology, 2020), https://cset.georgetown.edu/research/chinese-perspectives-on-ai-and-future-military-capabilities/.

[56] Richard Tauwhare, "Export Controls and The Cloud: US rules clarified but the EU's remain obscure," *Institute of Export and International Trade,* February 13, 2020, https://www.exportcontrolprofession.co.uk/2020/02/13/export-controls-and-the-cloud-us-rules-clarified-but-the-eus-remain-obscure/.

[57] Ben Buchanan, *The AI Triad and What It Means for National Security Strategy* (Washington, D.C.: Center for Security and Emerging Technology, 2020), https://cset.georgetown.edu/wp-content/uploads/CSET-AI-Triad-Report.pdf.

[58] Sunith Shetty, "Why TensorFlow always tops machine learning and artificial intelligence tool surveys," *Packt*, August 23, 2018, https://hub.packtpub.com/tensorflow-always-tops-machine-learning-artificial-intelligence-tool-surveys/; Horace He, "The State of Machine Learning Frameworks in 2019," *The Gradient*, October 10, 2019, https://thegradient.pub/state-of-ml-frameworks-2019-pytorch-dominates-research-tensorflow-dominates-industry/; GitHub, *The 2021 State of the Octoverse,* https://octoverse.github.com/.

[59] Amazon Web Services, *AWS Machine Learning Infrastructure,* https://aws.amazon.com/machine-learning/infrastructure/.

[60] MacroPolo, *International Collaboration,* https://macropolo.org/digital-projects/the-global-ai-talent-tracker/international-collaboration/; Castro, "Who is winning the AI Race."

[61] Aman Anand, "Deep Learning Trends: top 20 best uses of GPT-3 by OpenAI," *Educative*, Spetember 28, 2020, https://www.educative.io/blog/top-uses-gpt-3-deep-learning; Renee DiResta, "The Supply of Disinformation Will Soon Be Infinite," *The Atlantic*, September 20, 2020, https://www.theatlantic.com/ideas/archive/2020/09/future-propaganda-will-be-computer-generated/616400/; Kris McGuffie and Alex Newhouse, "The Radicalization Risks of GPT-3 and

Advanced Neural Language Models." Preprint, submitted September 15, 2020, https://arxiv.org/abs/2009.06807.

[62] Karen Hao, "A college kid's fake, AI-generated blog fooled tens of thousands. This is how he made it," *MIT Technology Review*, August 14, 2020, https://www.technologyreview.com/2020/08/14/1006780/ai-gpt-3-fake-blog-reached-top-of-hacker-news/.

[63] Jack Clark et al., "GPT-2: 6-Month Follow Up," *OpenAI Blog,* August 20, 2019, https://openai.com/blog/gpt-2-6-month-follow-up/.

[64] Alec Radford et al., "Better Language Models and Their Implications," *OpenAI Blog*, February 15, 2019, https://openai.com/blog/better-language-models/.

[65] Greg Brockman et al., "OpenAI API," *OpenAI Blog*, June 11, 2020, https://openai.com/blog/openai-api/.

[66] OpenAI, Research Access Program Application, https://share.hsforms.com/1b-BEAq_qQpKcfFGKwwuhxA4sk30.

[67] Connor Leahy, "Why Release a Large Language Model?" *EleutherAI Blog*, June 2, 2021, https://blog.eleuther.ai/why-release-a-large-language-model/.

[68] Saif M. Khan, *AI Chips: Why They Are and Why They Matter* (Washington, D.C.: Center for Security and Emerging Technology, 2020), 6, https://cset.georgetown.edu/research/ai-chips-what-they-are-and-why-they-matter/.

[69] Khan, *AI Chips*.

[70] Saif M. Khan and Carrick Flynn, *Maintaining China's Dependence on Democracies for Advanced Computer Chips* (Washington, D.C.: The Brookings Institution, 2020), https://www.brookings.edu/research/maintaining-chinas-dependence-on-democracies-for-advanced-computer-chips/.

[71] Khan, *AI Chips.*

[72] IC Insights, "China Forecast to Fall Far Short of its 'Made in China 2025' Goals for Ics," *IC Insights*, January 6, 20201, https://www.icinsights.com/news/bulletins/China-Forecast-To-Fall-Far-Short-Of-Its-Made-In-China-2025-Goals-For-ICs/.

[73] Richard Danzig and Lorand Laskai, *Symbiosis and Strife: Where is the Sino-American Relationship Bound?* (Baltimore, MD: Johns Hopkins Applied Physical Laboratory, 2020), https://www.jhuapl.edu/Content/documents/Danzig-Laskai.pdf.

[74] United States General Accounting Office, "Export Controls: Rapid Advances in China's Semiconductor Industry Underscore Need for Fundamental U.S. Policy Review" (General Accounting Office, April 2002), https://www.gao.gov/assets/gao-02-620.pdf.

[75] Fedasiuk, *Chinese Perspectives on AI.*

[76] Cheng Ting-Fang et al., "China's top chipmaker SMIC cuts spending due to US export curbs," *Nikkei Asia*, November 12, 2020, https://asia.nikkei.com/Economy/Trade-war/China-s-top-chipmaker-SMIC-cuts-spending-due-to-US-export-curbs.

[77] Carrick Flynn, "The chip-making machine at the center of Chinese dual-use concerns," *Tech Stream*, June 30, 2020, https://www.brookings.edu/techstream/the-chip-making-machine-at-the-center-of-chinese-dual-use-concerns/.

[78] See Appendix A.

[79] Bryon Moyer, "Nikon vs. ASML," *Electronic Engineering Journal*, May 1, 2017, https://www.eejournal.com/article/nikon-vs-asml/.

[80] Will Hunt et al., *China's Progress in Semiconductor Manufacturing Equipment* (Washington, D.C.: Center for Security and Emerging Technology, 2021), https://cset.georgetown.edu/research/chinas-progress-in-semiconductor-manufacturing-equipment/.

[81] Dario Amodei and Danny Hernandez, "AI and Compute," *OpenAI Blog*, May 16, 2018, https://openai.com/blog/ai-and-compute/.

[82] Kevin Hartnett, "To Build Truly Intelligence Machines, Teach Them Cause and Effect," *Quanta*, May 15, 2018, https://www.quantamagazine.org/to-build-truly-intelligent-machines-teach-them-cause-and-effect-20180515/; Dana Mackenzie and Judea Pearl, *The Book of Why* (New York, NY: Basic Books, 2018).

[83] Jonathan Richens et al., "Improving the accuracy of medical diagnosis with causal machine learning," *Nature Communications* 11 (2020), https://www.nature.com/articles/s41467-020-17419-7.

[84] Dario Amodei, et al., "Concrete Problems in AI Safety." Preprint, submitted July 25, 2016, https://arxiv.org/abs/1606.06565.

[85] S. Velliangiri et al., "A Review of Dimensionality Reduction Techniques for Efficient Computation," *Procedia Computer Science* 165 (2019), https://www.sciencedirect.com/science/article/pii/S1877050920300879.

[86] Yi Cheng et al., "A Survey of Model Compression and Acceleration for Deep Neural Networks." Preprint, submitted June 14, 2020, https://arxiv.org/pdf/1710.09282.pdf; Davis Blalock et al., "What is

the State of Neural Network Pruning?" Preprint, submitted March 6, 2020, https://arxiv.org/pdf/2003.03033.pdf.

[87] For more analysis on the use of adversarial ML to undermine rival applications, see, Tim Hwang, *Shaping the Terrain of AI Competition* (Washington, D.C.: The Center for Security and Emerging Technology, 2020), https://cset.georgetown.edu/publication/shaping-the-terrain-of-ai-competition/.