AI, Great Power Competition & National Security

Eric Schmidt

Breakthroughs in AI are accelerating global commercial competition and transforming the international security environment. The reach and influence of foreign-based network platforms present risks to American society and require us to confront questions about their origin and purpose. Meanwhile, AI technologies are enhancing several existing national security threats, and will change the way states try to gain leverage against adversaries and exercise coercion and influence in other societies. The open nature of free and democratic societies, combined with their increasing reliance on poorly secured digital networks, makes them especially vulnerable. In the military realm, AI holds the prospect of augmenting cyber, conventional, and nuclear capabilities in ways that make security relationships among rivals more challenging to predict and maintain, and conflicts more difficult to limit. Even as they compete, rivals should explore limits on AI capabilities. The AI ecosystems of the principal global competitors, the United States and China, remain intertwined, and a calibration of the bilateral technology relationship requires both selective decoupling and continued collaboration in areas of mutual interest. These changes require a comprehensive national strategy for the next decade that preserves global leadership advantages for America's economy and security.

The second decade of the twenty-first century featured two major developments that, together, are shaping the third decade we have now entered. The geopolitical landscape is marked by intensifying competition between the United States and its major power rivals, China and Russia. At the same time, the scientific landscape is characterized by significant advances in artificial intelligence, which promise tremendous economic and strategic advantages for those who capitalize on them.

The confluence of these trends has set up an intense commercial competition among the world's leading technology companies, most of which are based either in the United States or in China. AI is transforming almost every sector of national economies and is accelerating globalized competitions among digital platforms and services. As a consequence, the stakes for future prosperity and long-term national competitiveness are immense.

https://doi.org/10.1162/DAED_a_01916

The security environment is also undergoing significant transformations. This is true across a broad spectrum of national and international security problems, extending from lower- to higher-level intensities of conflict. At the low end, AI is exacerbating cyber and disinformation threats and is changing the way states exercise targeted coercion against opponents. In the middle of the spectrum, warfare between conventional armed forces will feature more rapid actions and delegated decision-making that could make conflict harder to control. At the high end, AI-enabled military and intelligence capabilities may disrupt the fundamental premises of nuclear deterrence in ways that undermine strategic stability.

All of this requires a comprehensive national strategy for the next decade that preserves global leadership advantages for both America's economy and security. The United States must protect against hacking, coercion, and other efforts by adversaries to use our society's openness against us. The most dangerous aspects of the U.S.-Chinese and U.S.-Russian military rivalries must be managed to avoid disastrous conflicts. And the innovation economy that has put American technology and ingenuity at the forefront of scientific advances for decades must be bolstered to stay ahead of America's principal competitor, China.

Understanding how AI drives the new global commercial landscape begins with *network platforms*, which I describe in a recently published book, *The Age of AI*, coauthored with Henry Kissinger and computer scientist Daniel Huttenlocher, as digital services that provide value to their users by aggregating them in large numbers, often at a transnational and global scale.[1] Today, the major network platforms increasingly rely on AI for growth. A network platform's value and attractiveness grow as additional users adopt it. The potential social, economic, political, and geopolitical influence of each major network platform is substantially augmented by the degree of these positive network effects.

Two features of global network platforms are especially significant to geopolitics. First is their tendency toward consolidation. As more users are drawn to certain platforms, their network advantages reduce competition, leaving us with fewer providers of a given service, each with a large base of users. In other words, the dynamics of positive network effects tend to support only a handful of major players who are operating at the forefront for their product or service. The small number of leading platforms thereby gain and exercise significant influence on a global scale.

The second feature is that many nations are, and are likely to remain, reliant on network platforms that are both designed and hosted in other countries. As a result, they are dependent, at least in part, on other countries' regulators for continued access, key inputs, and international updates. In the United States and elsewhere, this has created concerns about the implications of conducting broad aspects of national economic and social life on network platforms that were built

in other, potentially rival, countries. These platforms may foster a close level of connection and influence, particularly with the use of AI to learn from and steer a country's citizens.

Taken together, these two features point to a growing geopolitical and national security concern for the United States. The globally dominant network platforms of the future could be based in rival countries and could exert significant influence over American society and even critical infrastructure. If a network platform is useful and successful, it comes to support broader commercial and industrial functions and, in this capacity, may become nationally indispensable. At least theoretically, the threatened withdrawal of such a network platform serves as a potential instrument of leverage. This hypothetical ability to "weaponize" network platforms by withholding service in a crisis is an increasingly significant factor in national security planning.

The reach and influence of global network platforms require us to ask essential questions about their origin and purpose: By whose design, and with what regulatory parameters, is the AI operating? What impact might these processes have on social norms and institutions? Who has access to the information generated through the platform?

Looking across the world, a multidisciplinary contest for economic advantage, digital security, technological primacy, and ethical and social objectives is unfolding.

The United States has begun to view network platforms as an aspect of international strategy, restricting the domestic activities of some foreign platforms and restricting the export of some software and technology that could strengthen foreign competitors. At the same time, critics in and out of government have identified major domestic network platforms as targets for antitrust actions. This simultaneous drive for strategic preeminence and domestic multiplicity may push U.S. development in opposing directions.

Meanwhile, China has similarly supported the development of formidable network platforms that are global in scale and poised to expand their reach. Beijing has also taken steps to shape international technology standards and bar the export of sensitive, domestically developed technologies. Chinese network platforms predominate in China and nearby regions, and some are leading global markets.

The landscape will also be shaped by actors beyond the United States and China. Europe, unlike China and the United States, has yet to create homegrown global network platforms or cultivate the technology industry that has supported the development of network platforms elsewhere. To be sure, Europe has a significant place in the global AI landscape with some leading companies and universities, sizable markets, and a formidable regulatory apparatus. Yet Europe continues to face disadvantages for the initial scaling of new network platforms due to the

many languages and separate national regulatory systems in Europe's combined market.

The European Union has focused recent regulatory attention on obliging changes in American and (to some extent) Chinese network platforms' conduct as a condition of their operation in the European market. Europe faces the choice of whether to act as an ally to one side or another in each technological sphere or to act as a balancer between sides. Here, the preferences of the traditional, core EU states and the newer Central and Eastern European entrants may differ, reflecting varying geopolitical and economic experiences. Thus far, historic global powers like France and Germany have prized independence and freedom to maneuver in their technology policy, whereas more peripheral European states with recent and direct experience of foreign threats (such as the post-Soviet states) have shown greater readiness to identify with a U.S.-led technology sphere.

While still an emerging force in this arena, India has substantial intellectual capital, a relatively innovation-friendly business and academic environment, and a vast reserve of technology and engineering talent that could support the creation of leading network platforms. India's population and economy are of a scale that could potentially sustain independent network platforms, without recourse to other markets. Likewise, Indian-designed network platforms have the potential to become popular in other markets as well. As India assesses its regional relationships and relative reliance on imported technology, it may elect either to chart a more independent path or to assume a principal role within an international bloc of technologically compatible nations.

The Global AI Index, the most comprehensive effort to date to rank countries in terms of AI advancement, offers several insights into how the global competitors stack up.[2] The creators of the index assessed countries based on 143 indicators across areas such as the talent of AI researchers and practitioners, infrastructure, R&D, government strategy, and commercial activity. This is, of course, a snapshot in time. What emerges, though, is the centrality of AI talent indicators to assess both current strength and future trends. Consider, for example:

- The United States leads China by the widest margin in the talent category (scoring five times higher). It also holds significant leads in research and in commercial AI. These factors seem naturally related: the best talent is producing the best research and driving the best commercial products. All of this points to the importance of keeping America's global edge in attracting and retaining top AI talent.
- Several Western allies also score higher than China in AI talent, including the United Kingdom, Canada, Germany, the Netherlands, and France. This raises questions about the extent to which European states will be able to capitalize

on this excellent talent base after Brexit and in the midst of the EU's evolving regulatory approach to AI.

- Although India's overall score is much lower than China's, its talent score is substantially higher. India ranks second in the world in AI talent, behind only the United States. This suggests tremendous potential for India to emerge as a global AI heavyweight over time, if India can improve its position in other areas such as national infrastructure, government strategy, and commercial application.

In overall scores, the United States and China are in a league of their own at number one and two, respectively. But the next tier (about ten countries whose overall scores fall in the same ballpark) is made up entirely of U.S. allies and partners. This points to the critical need to develop and strengthen AI partnerships with those nations.

Depending on how the commercial competition unfolds – even with, or perhaps as an effect of, such global partnerships – an industry founded on the premise of global community and communication may, in time, be enlisted in a process of regionalization. Such a process could unite blocs of users in separate realities, influenced by distinctive AI that has evolved in different directions and is shaped by spheres of regional technology standards. While these trends play out, some of these AI-driven platforms will be at the center of novel national security challenges.

Artificial intelligence technologies are enhancing several existing national security threats and will change the way states try to gain leverage against adversaries and exercise coercion and influence in other societies. The open nature of free and democratic societies, combined with their increasing reliance on poorly secured digital networks, makes them especially vulnerable to these threats.

In its 2021 final report, the National Security Commission on Artificial Intelligence, an independent government panel that I chaired, found that the machine learning algorithms that transformed how business was done in the early years of this century are now transforming intelligence and statecraft.[3] Technology and advertising companies learned the value of AI for harvesting and analyzing consumer data. Similar capabilities wielded by governments can now be used for espionage, targeted coercion, tailored disinformation, sophisticated cyber intrusions, and potentially biological warfare.

AI opens new horizons of capabilities in the information space, both in monitoring and in disinformation and disruption. In theory, at least, AI could be used to determine the most effective ways of delivering synthetic content to people, tailoring it to their biases and expectations. Both "offense" and "defense" – both

the spread of disinformation and efforts to combat it – will become increasingly automated and entrusted to AI.

These capabilities could be used across the spectrum of conflict: as tools of pressure during peacetime, as a prelude to military actions, or in concert with a military campaign.

One implication of these changes is that data security has become a more central problem of national security. AI makes it harder to protect personal information – finances, patterns of daily life, relationships, and health among other things – that adversaries could use to develop individually tailored models for influence. This is the major counterintelligence challenge for the AI era.

Another, related security concern is that the cyber domain is becoming increasingly complex and automated. Once AI-enabled malware is lodged onto a computer system, it will be able to mutate into multiple forms to avoid detection and countermeasures. Such mutating polymorphic malware already accounts for the vast majority of malicious executable files circulating in cyberspace.

The U.S. government's tools to manage these threats are clearly inadequate. Substantial changes are required in the way we think about data security and in our policies and laws to strengthen it. We need to identify categories and combinations of our most sensitive personal and commercial data, and develop a broad approach with clear policies, criteria, or authorities to confront this multifaceted problem. Likewise, major reforms are needed in cybersecurity, including widespread integration of AI-enabled cyber defenses to match and neutralize offensive AI-cyber techniques.

The AI era risks complicating the riddles of modern strategy beyond human intention, or perhaps even human comprehension. AI holds the prospect of augmenting cyber, conventional, and nuclear capabilities in ways that make security relationships among rivals more challenging to predict and maintain, and conflicts more difficult to limit.

AI's capacity for autonomy and logic generates a layer of incalculability. Most traditional military strategies and tactics are based on the assumption of a human adversary whose conduct and decision-making calculus fit within a recognizable framework or have been defined by experience and conventional wisdom. Yet an AI system piloting an aircraft or scanning for targets follows its own logic, which may be inscrutable to an adversary and unsusceptible to traditional signals or feints and which will, in most cases, proceed faster than the speed of human thought.

Moreover, because AIs are dynamic and emergent, even those powers creating or wielding an AI-designed or AI-operated weapon may not know exactly how powerful it is, or what it will do in a given situation. When actors deploy AI weapons against one another, neither side may have a precise understanding of what their interaction will generate or what may be its collateral effects.

The integration of AI into military and intelligence systems heightens the risk of instability and conflict between the United States and its rivals across a spectrum of scenarios, from activities beneath the threshold of war, to conventional warfare between armed forces, to nuclear escalation.

At the lower end, for example, it is not hard to imagine how AI-enabled capabilities could provide China with more effective tools to patrol the South China Sea and consolidate its strategic position there. Nor is it hard to imagine Russian cyber and disinformation activities in Ukraine or elsewhere in Europe becoming more effective, persistent, and influential with AI.[4]

Once they are released into the wild, AI-enabled cyber weapons may be able to adapt and learn and may go well beyond their intended targets. The very capabilities of the weapon might change as the AI reacts to its surroundings. The multibillion-dollar global damage caused by Russia's 2017 NotPetya attack concretely demonstrates the power of even basic automated malware, the risk tolerance of capable state actors, and the consequences of such capabilities proliferating.

AI-enabled cyber weapons may allow adversaries to launch digital assaults with exceptional speed, dramatically accelerating the human capacity to exploit digital vulnerabilities. As such, a state may effectively have no time to evaluate the signs of an incoming attack. Instead, they may need to respond immediately or risk disablement. If they have the means, they may elect to "respond" nearly simultaneously, before the event can occur, constructing an AI-enabled system to scan for attacks and empowering it to counterattack. This could lead to new forms of automated preemption or anticipatory self-defense and strain the legal and policy frameworks that guide government decision-making.

In conventional warfare, greater reliance on automated capabilities, combined with the intense decision-making time pressures that attend operations conducted at machine speeds, could lead to rapid and even unintended escalation. This is all the more worrisome if militaries rush to field new systems that are unreliable in practice and poorly understood by operators. Unintended escalation could occur for many reasons – including when systems fail to perform as intended because of interactions between opposing systems on the battlefield, or as the result of machines or humans misperceiving signals or actions. As AI-enabled systems increase the pace of warfare across the board, the time and space available for de-escalatory measures will shrink.

There are also reasons to believe AI will erode nuclear stability, although some of these concerns are largely theoretical for now. For example, if AI-enabled intelligence and targeting systems are better able to locate nuclear forces that are currently hard to see and strike (because they are under the sea or moving around on land), this would put at greater risk a state's second-strike capability and thereby undermine mutual vulnerability, which is considered to be a source of stable nu-

clear deterrence. Other concerns relate to potential integration of AI into nuclear command and control.

In the military sphere, realism should compel rivals, even as they compete, to explore limits on the development and use of certain destructive, destabilizing, or unpredictable AI capabilities. This could include a sober effort at some form of AI arms control or, if that is too ambitious, the development of confidence-building measures between rival states to reduce risks to international stability.[5]

If weapons can change in ways that prove different in scope or kind from what their creators anticipated or threatened, calculations of deterrence or escalation have the potential to turn illusory. Moreover, from a technical standpoint, the lines between engaging AI in reconnaissance, targeting, and lethal autonomous action may be relatively easily crossed, making a search for mutual restraint and verification systems difficult but imperative.

To be meaningful, restraints must be reciprocal. But the management of mutual restraints on military AI systems will be even more difficult than it has been for nuclear weapons, which has been the endeavor of more than a half century of diplomacy among rivals and remains incomplete and fragmentary. The challenge of assessing the nuclear balance is relatively straightforward. Warheads themselves can be counted and their yields known. Conversely, the capabilities of AI are not fixed, they are dynamic. Unlike nuclear weapons, AI systems are hard to track: once trained, they can be copied easily and run on relatively small machines. And detecting their presence or verifying their absence is difficult or impossible with present technology. This is an important area for further technical research and policy development.

To begin approaching these questions through diplomacy, initial U.S. dialogue with China or Russia should focus on making sure that both sides know, at least in general terms, what the other is doing. Such a discussion of AI weapons among major powers must be endeavored, if only to develop a common vocabulary of strategic concepts and some sense of each other's red lines.

Because the incorporation of AI systems in nuclear strategy is still nascent, now is the window of time for nuclear states to discuss protocols and understandings that could minimize the disruption to nuclear stability. One helpful measure would be to clearly and publicly affirm existing U.S. policy that only humans can authorize the employment of nuclear weapons – and then seek similar commitments from other states.

At the same time, the United States and other major powers should make efforts to limit the proliferation of AI-enabled weapons. Once introduced, these capabilities could spread quickly. Although creating a sophisticated AI requires substantial computing power, proliferating the AI or running inference generally

does not. AI will be ubiquitously acquired, mastered, and employed; the imposition of restraints on weaponizing AI, or even achieving a collective definition of restraint, will be exceedingly difficult.

Security risks to the United States will become more acute if China's researchers, companies, and military and intelligence agencies overtake their American counterparts in AI proficiency and breakthroughs. At the same time, an open international research environment encourages mutually beneficial scientific advances in both countries. Adjusting the degrees to which U.S.-China technology relations should be open or closed will remain an evolving challenge.

Only the United States and China have the resources, commercial might, talent pool, and innovation ecosystem to lead the world in AI. In some areas of AI research and application, China is a peer, and in certain applications, China is already more technically advanced. Within the next decade, China could surpass the United States as the world's preeminent AI power.

If China's firms win the competition for global network platforms, it will not only disadvantage U.S. companies, it will also create the digital foundation for a geopolitical challenge to the United States and its allies. Platform domination abroad allows China to harvest the data of its users and permits China to extend aspects of its domestic system of control. Wherever China controls the digital infrastructure, it will gain greater leverage to conform the world to its goals.

Meanwhile, the research ecosystems in China and the United States are deeply connected through shared research projects, talent circulation, and commercial linkages that include supply chains, markets, and joint research ventures. It would be counterproductive to sever the technology ties to China that foster basic research and benefit U.S. companies. But the United States must safeguard the integrity of open research, prevent the theft of American intellectual property, and employ targeted tools like export controls and investment screening to protect technology industries that are critical to national security.

An appropriate calibration of the U.S.-China technology relationship would include: 1) some purposeful decoupling of specific linkages that introduce unacceptable vulnerabilities, such as in areas with clear security and military applications; 2) continuing cooperative research that brings significant joint benefit; 3) continuing commercial interchange between technology sectors; 4) greater collaboration in shared scientific challenge areas; and 5) increased federal government investment in research and development, which will help position the United States to win network platform competitions.[6]

Decoupling, through this lens, is not just about disconnecting from China. It is about revitalizing America's own productivity in critical areas. At the same time, the United States must also build up the capacity of its allies and partners. Done

right, purposeful decoupling could spur a commercial renaissance in particular classes of technologies across Western nations.

Breakthrough progress by China on several fronts has intensified the U.S.-China technology competition. The United States must continue to invest in American innovation to keep from falling behind. There has been a continuity of purpose across administrations to mount a major national effort in AI. Keeping the momentum requires the federal government to take a more assertive role than Americans have been accustomed to in recent decades.

Most technology advances in the United States will be driven by the private sector and universities. Although publicly funded research has been important for innovation, the private sector has proved to be America's great strength. Companies move faster and more globally than any government could. But large technology firms cannot be expected to compete with the resources of China or make the large, nationwide investments the United States needs to stay ahead in the competition. A hybrid approach that more tightly aligns government and private sector efforts is needed to win.

One example of such an approach is the National AI Research Resource (NAIRR), a recommendation of the AI Commission. Requested by Congress through the National AI Initiative Act of 2020, this initiative aims to democratize access to compute environments, data, and testing facilities, providing researchers beyond the leading industry players and elite universities with the ability to pursue cutting-edge AI work. The initiative promises to spur nationwide technology advances with benefits for overall national competitiveness.

Another area for constructive government action is in microelectronics. After decades of leading the microelectronics industry, the United States is now almost entirely reliant on foreign sources for production of the cutting-edge semiconductors that power the AI algorithms critical to everything from our defense systems to our smartphones. The dependency on semiconductor imports, particularly from Taiwan, creates a strategic vulnerability from adverse foreign government action, natural disaster, or other events that could disrupt supply chains for electronics. At the same time, China has made an enormous financial commitment to forging a world-leading semiconductor industry by 2030, with the goal of minimizing or eliminating China's own dependency on imported microelectronics. The United States must be committed to a strategy to stay at least two generations ahead of China in state-of-the-art microelectronics. Doing so requires continued funding and incentives to maintain multiple sources of cutting-edge microelectronics fabrication in the United States.

In the coming years, economic and security competitions will proceed in parallel, with China aiming to achieve global preeminence in AI by 2030 and security agencies among all competitors adopting AI for a wide range of applications.

Trends in global network platforms will not just define the landscape of commercial AI, but will also shape the security environment in novel ways. International stability will hinge in large measure on whether rival states can manage the uncertainties of AI in the cyber, conventional, and nuclear realms. And the United States will need to carefully navigate its interdependencies with China while also continuing domestic reforms to bolster innovation. How the United States manages these interrelated challenges will go a long way toward determining its competitive position by the end of the decade.

ABOUT THE AUTHOR

Eric Schmidt, a Fellow of the American Academy since 2007, is the former Chief Executive Officer of Google and former Executive Chairman and Technical Advisor of Alphabet, Inc. He is also a Founder of the Schmidt Foundation, the Schmidt Ocean Institute, and Schmidt Futures. He is the Chair of the Special Competitive Studies Project and was the Chairman of the National Security Commission on Artificial Intelligence from 2019 to 2021. He is the author of *The Age of AI: And Our Human Future* (with Henry Kissinger and Daniel Huttenlocher, 2021), *Trillion Dollar Coach: The Leadership Playbook of Silicon Valley's Bill Campbell* (with Jonathan Rosenberg and Alan Eagle, 2019), and *How Google Works* (with Jonathan Rosenberg, 2014). In 2020, he launched the podcast Reimagine.

ENDNOTES

[1] This discussion on network platforms and global commercial competition in AI draws in part from Henry A. Kissinger, Eric Schmidt, and Daniel Huttenlocher, *The Age of AI: And Our Human Future* (Boston: Little, Brown and Company, 2021).

[2] The Global AI Index, Tortoise Media, https://www.tortoisemedia.com/intelligence/global-ai/ (accessed January, 2022).

[3] National Security Commission on Artificial Intelligence, *Final Report* (Washington, D.C.: National Security Commission on Artificial Intelligence, 2021), https://www.nscai.gov/2021-final-report/.

[4] This essay was written before Russia's invasion of Ukraine in February 2022.

[5] This discussion of measures to mitigate international stability risks draws in part from Kissinger et al., *The Age of AI*.

[6] For an elaboration of the argument for calibrating U.S.-China technology relations, and further explanation of these five features, see Eric Schmidt, "Building a New Technological Relationship and Rivalry," in *COVID-19 and Global Order*, ed. Hal Brands and Francis Gavin (Baltimore: Johns Hopkins University Press, 2020).