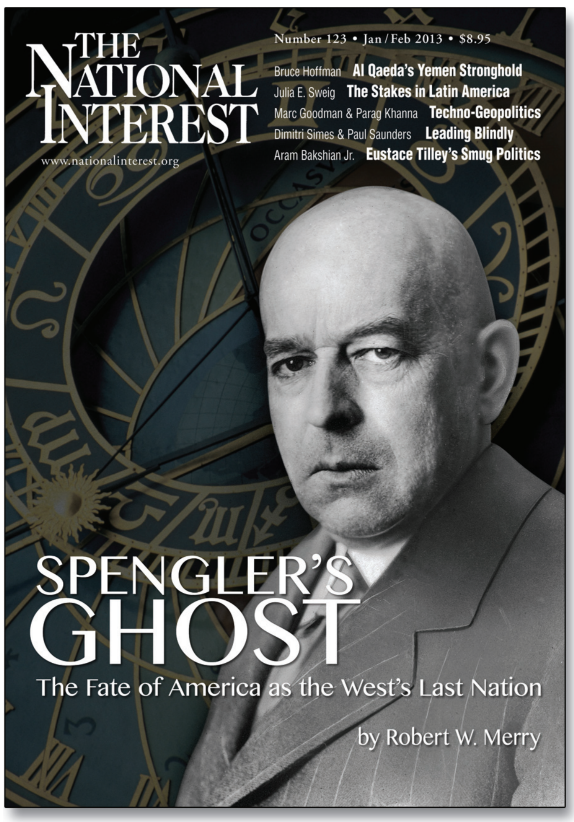
THE NATIONAL INTEREST

Number 123 • Jan / Feb 2013



EDITOR *Robert W. Merry*

The National Interest • 1025 Connecticut Avenue, N.W. • Suite 1200 • Washington, D.C. 20036
Phone (202) 467-4884 • Fax (202) 467-0006 • editor@nationalinterest.org

The contents of *The National Interest* are copyrighted. ©2013 The National Interest, Inc.
All rights reserved. Reproduction and distribution of this material is permitted only
with the express written consent of *The National Interest*.

The Power of Moore's Law in a World of Geotechnology

By Marc Goodman and Parag Khanna

While cyberspace and social media have grabbed global headlines in recent years, other major technology clusters will have an even more seismic impact on geopolitics in coming decades. They include biotechnology, robotics and artificial intelligence. Indeed, these technologies are coming of age and experiencing exponential innovation as well as growth—and not just in the United States. New contenders, including Asian state-run laboratories, corporate investors, DIY/maker groups, terrorists and organized criminals are all competing to harness and leverage technology in pursuit of their interests. In this rapidly changing environment, America risks having its international dominance undermined by these emerging technologies and players, much as Arab despots have been overthrown by protesters empowered in part by social media.

To understand and frame the ever-shifting nature of international relations, analysts have traditionally relied upon both geopolitics and geoeconomics. The discipline of geopolitics dates to nineteenth-century European scholars and diplomats whose primary concerns were territorial control and the capability to project dominance overseas. Examining the fundamental elements of geopolitical advantage (demographics, natural resources, forces under arms, warships, conventional and nuclear weapons, etc.) remained the dominant approach to analyzing comparative power through much of the twentieth century.

After the Cold War, geoeconomics became a counterweight to geopolitics. In 1990, strategist Edward Luttwak said geoeconomics applied the "logic of conflict" to the "grammar of commerce." In this view, GDP size and growth, trade balances, currency reserves and foreign investment are critical in assessing the global balance of power. Although China is not yet a military rival to the United States, it is the largest holder of American debt and represents almost 15 percent of world GDP, making it a geoeconomic superpower. Similarly, the combination of petroleum resources and large currency reserves has put the small Arab monarchies of the Gulf Cooperation Council on the geoeconomic map.

Geopolitics and geoeconomics complement each other, but even together they do not give a full picture of the catalysts for change in world affairs. A third area of inquiry is necessary to complete the triangle: geotechnology. The geotechnology lens offers an understanding of the potent innovations that can tilt geoeconomic advantage through rapid commercialization and can have a major geopolitical impact through strategic deployment and potential militarization. Whether we're talking about

Marc Goodman is the chair for Policy, Law & Ethics at Singularity University and founder of the Future Crimes Institute. **Parag Khanna** is a senior research fellow at the New America Foundation and director of the Hybrid Reality Institute.

the stirrup and crossbow; steamships and railways; or nuclear fusion and the Internet, every era is a time of geotechnological change. What is different today is the rate of change, which is ever accelerating.

The perspective afforded by geotechnology informs our understanding of global dynamics in two important ways. First, it positions technology alongside economic power, military alliances and diplomatic statesmanship as a driver of history. It was the ability of Europe's royal families to harness weaponry and the printing press that gave the state the upper hand over other political forces in the seventeenth century and created the modern Westphalian system. Second, whereas geopolitics largely ignores nonstate actors and geoeconomics acknowledges them only as marginal players, geotechnology fully recognizes current systemic changes that are driving us into a post-Westphalian world. It recognizes that actors leveraging and controlling new technologies, even with limited capital and crowdsourced manpower, can amass formidable influence as well as a capacity to challenge nation-states. While WikiLeaks and Anonymous; Al Qaeda and Hezbollah; and Google and Facebook may be rooted in certain territories more than others, they are increasingly autonomous in their transterritorial reach and capabilities.

Gordon Moore, the former chairman of Intel, famously predicted in 1965 that the number of transistors per square inch on an integrated circuit would double every year into the future. This principle, later revised to a doubling every two years and commonly referred to as "Moore's Law," now applies more broadly to the power and capabilities of all circuit-based technologies. Thus, everything from biotechnology to robotics is driven by Moore's Law, and this has implications for both geopolitics and geoeconomics. These technologies are exponential in their growth curves—not linear. Taking thirty steps linearly, one might walk across the living room. But taking thirty steps exponentially—doubling the distance with each successive step—would be the equivalent of traveling the distance to the moon. The iPhone that hundreds of millions of users carry in their pocket has more processing power than what was available to NASA during the Apollo 11 moon landing a mere forty years ago. Such is the world we now live in.

Most academic studies examining the impact of new technologies on international affairs have focused on the Internet. Though the average Internet user today may be busily updating his Facebook status or playing Angry Birds, it is important to recall that today's Internet emanates from the Advanced Research Projects Agency Network, a U.S. Department of Defense invention created to ensure redundancy in military communications in the event of a nuclear attack. Simply stated, the Internet is a military creation with significant corollary

geopolitical ramifications. Cyberspace and its underlying computer networks have been as transformative as the printing press. The fact that information can travel at the speed of light over a fiber network from Bangkok to Berlin has had a tremendous impact on society, economics and international affairs. But the Internet itself is only version 1.0 of twenty-first-century geotechnology, a stepping-stone to a world of even greater scientific advancements with unpredictable geopolitical consequences.

Today's Internet will soon be eclipsed by an array of rapidly evolving technologies, all flowing, per Moore's Law, in an exponential fashion. While most of these innovations will be connected to today's global information grid, they will leave the two-dimensional space of our computer screens behind and reach well into three-dimensional aspects of our lives.

Robotics is one such rapidly emerging field with geopolitical and geoeconomic consequences. Unmanned aerial vehicles now perform tasks such as imagery collection, interception of communications and the launching of missiles. Remote pilots sitting halfway around the world can kill perceived enemies with the click of a mouse. The next frontier is the miniaturization of flying robots, with quadcopters and microbots the size of insects achieving autonomous flight and swarming patterns for vastly expanded surveillance and intelligence gathering. On the geoeconomic front, President Obama has declared the goal of doubling America's exports, partially through the National Robotics Initiative, which would augment American workers' productivity in order to better compete with Asian manufacturers. At the same time, Foxconn, the Chinese company that manufactures millions of household electronic goods (with four hundred thousand workers making Apple products alone), plans to integrate a million robots into its assembly lines in coming years. The geotechnological competition in robotics not only will affect the global trade balance profoundly but will also demonstrate how our economic fear of mass unemployment will be driven less by outsourcing than by robo-sourcing.

Ubiquitous computing is another emerging area of strategic importance. Over the past decade, the number of Internet-connected devices has skyrocketed, surpassing the planet's human population in 2008. This revolution is known as the "Internet of Things." Based on the exponential nature of Moore's Law and the number of devices we expect to be connected to the Internet, we are in the process of reengineering the basic Internet Protocol, upgrading it from version four to version six. Internet Protocol version six will massively expand the addressable space online from a mere 2^{32} to 2^{128} things, a transition expected to be complete within the next three to five years.

To put these exponential numbers into perspective, we're about to transition from an Internet the size of a golf ball to an Internet the size of the sun. The coming generation of the Internet will include tens of billions of sensors connected to the network via a variety of emerging technologies such as radio frequency identification tags and near-field communication. These sensors and networks will ensure that everyday physical objects such as automobiles, trees, chairs, street lights, elevators, pacemakers and fire alarms will all have an Internet protocol address. Moreover, expansive networks of these objects will communicate with each other online, allowing humanity for the first time to reach everything from anywhere.

Physical objects will thus be transformed into information technologies, allowing things to be tracked instantaneously and

Whether we're talking about the stirrup and crossbow; steamships and railways; or nuclear fusion and the Internet, every era is a time of geotechnological change. What is different today is the rate of change.

---

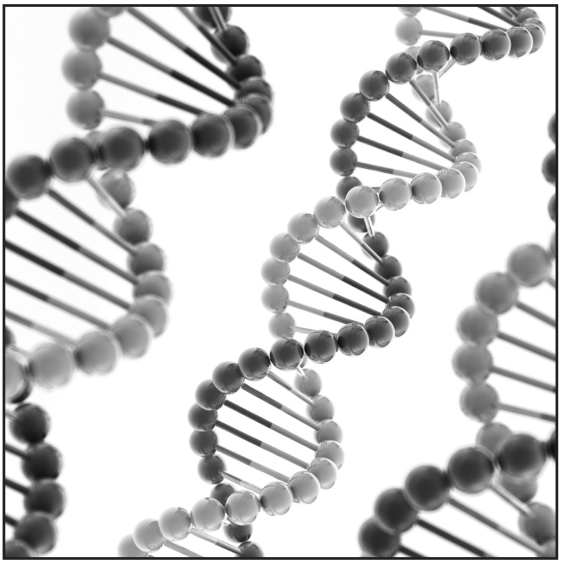
their history in physical space and time known. Metcalfe's Law dictates that the value of a network increases exponentially with the number of nodes or computers attached. Thus, our transition from an Internet of 2^{32} things to an Internet of 2^{128} things will create unimaginable future value. Nations and nonstate actors capable of leveraging these data streams to their fullest potential will have unparalleled intelligence and strategic advantage.

However, as the number of objects connected to the Internet increases, a nation's "threat surface" will expand exponentially as well, meaning far more security vulnerabilities. The U.S. Chamber of Commerce, for example, discovered that its computer network had been breached by an intruder based in China who accessed its strategic plans. An investigation revealed that the breach was enabled via an Internet-connected smart thermostat recently installed in a Chamber building. Moreover, networked printers used by the organization's executives began spontaneously and inexplicably printing pages with Chinese characters. As Chinese premier Wen Jiabao noted in a speech in August 2009, "Internet + Internet of Things = Wisdom of the Earth."

Artificial intelligence (AI) also has progressed beyond search-engine results and customized movie and book recommendations. Automatic pilot systems on aircraft (including military planes) and stock trading in global financial markets are guided and controlled by the scripted algorithms that are the building blocks of artificial intelligence. Human beings increasingly find that they cannot keep pace with the vast volumes of data to be processed. So they are turning to artificial intelligence to act in their stead.

Machine learning and automated systems also are on an exponential growth track, with notable implications for economic and national security. Consider the May 2010 "flash crash," in which the Dow Jones industrial average plunged about one thousand points, then recovered within minutes. It was the biggest one-day point decline on an intraday basis in history—and was caused by a predetermined AI-based trading algorithm. With companies such as Narrative Science using AI to produce market-price predictions and sell them to investors, algorithms now are making decisions based on computational predictions, potentially sowing the seeds for a much greater flash crash. With billions of dollars to be made by executing trades nanoseconds ahead of the competition, increasing numbers of financial transactions will be turned over to AI bots, which will have an untold impact on global economic markets.

As computer processing power increases exponentially, the number of expert systems with key links to our daily activities will proliferate. This poses a threat to national security from state or nonstate actors capable of exploiting the logic behind these fast-acting, automated decision engines. For example, Google's self-driving cars use AI to sense objects near the vehicle and in turn mimic the decisions made by human drivers. Once a city or a nation



platforms, intellectual property, and the future of exports for China and America. 3-D manufacturing uses software programs and computer-aided design to print not just in colored ink but also metal, plastic and even concrete, using three-dimensional layering techniques to "print" objects or prototypes from car parts to toys. Goods that have been imported for decades could soon be manufactured locally at massive scale, leading to dramatic upheavals in global trading patterns. Often this technology is heralded for potentially reviving American manufacturing—but a massive decline in Chinese exports would certainly also mean a sudden downward shift in Chinese investment in U.S. treasuries, sending interest rates dramatically up. When geotechnology, geoeconomics and geopolitics come together, an apparent victory in one area may have unintended consequences in another.

switches to fully autonomous vehicles, the underlying technology could be exploited to attack a nation's critical transportation infrastructure.

The U.S. Defense Department is financing studies of autonomous armed robots that could find and destroy targets on their own, with AI-decision support systems deciding whether or not to fire their weapons. As these systems proliferate, legions of robotic weapons may use AI to decide whether and how to engage with one another, with little if any time for human intervention. As Moore's Law advances, computer-enabled artificial intelligence will outpace the speed and processing power of our mammalian brains. Those nation-states and nonstate actors capable of harnessing the power of AI more effectively than their rivals will possess an undeniable strategic advantage on real and virtual battlefields.

The arena of advanced manufacturing is also receiving more attention for its economic and security implications. A recent paper by the Atlantic Council focuses on the rise of 3-D printing devices and their potential impact on supply chains, assembly

One remarkable aspect of 3-D printers and other forms of advanced manufacturing is that the devices are moving toward total self-replication. Today most 3-D printers can print more than 50 percent of the parts required to make another 3-D printer—a percentage that is increasing rapidly. Once 3-D devices can not only produce weapons but also replicate themselves, the security and economic ramifications will escalate.

In the realm of nanotechnology, impossibly small nanosized machines will be created at the atomic and molecular scale, driving significant advances in material sciences, medicine and warfare. Molecular manufacturing would enable molecular assemblers, which are nanosized machines, to reorder matter itself at the atomic scale—also allowing for their self-replication. For example, toxic nanoparticles could be absorbed into the body of human beings and animals through the skin, lungs, ears and eyes, and given their size could likely evade the natural defenses of mammalian immune systems. Many governments around the world (especially the United States, China and Japan) have created nanotechnology research centers to study the national-security implications of such technology. As K. Eric Drexler, a noted nanotechnology expert, observed, "Molecular manufacturing will bring a revolution in military affairs greater than the transition from hand-made spears to mass-produced guns. It is unwise to be on the wrong side of such a technology gap."

Though it may not seem obvious, biology is transforming itself into an information technology. Subtle genetic changes that took millennia to evolve can now be engineered in a laboratory. DNA is the original computer operating system, and cells are the machines that execute the code. Rather than using ones and zeros, biology employs base pairs of adenine, cytosine, guanine and thymine to code the software of life. In the twentieth century, we discovered how to read DNA; the twenty-first century will be about writing the code ourselves, opening up phenomenal new opportunities to create new and synthetic forms of life that will have a major impact on our economy, food availability, energy needs and global security.

But the revolution in biology is unfolding at a pace three to five times faster than that of Moore's Law. The first time a human genome was decoded and sequenced, in 2000, the cost was $300 million. By 2007 the cost had dropped to $1 million, and in 2011 it was just $5,000. The implications of the superexponential developments in biology are staggering, with every living thing on the planet likely to be sequenced and the technology of synthetic biology to be completely democratized. As the price of research and equipment drops precipitously, technologies previously available only to the most powerful of nations are becoming rapidly accessible to even nonstate actors. Indeed, the 2008 report of the Commission on the Prevention of WMD Proliferation and Terrorism, chaired by former senators Bob Graham and Jim Talent, warned that a biological attack within the United States was deemed probable before 2013 and specifically highlighted the dangers of synthetic biology:

> As DNA synthesis technology continues to advance at a rapid pace, it will soon become feasible to synthesize nearly any virus whose DNA sequence has been decoded . . . as well as artificial microbes that do not exist in nature. This growing ability to engineer life at the molecular level carries with it the risk of facilitating the development of new and more deadly biological weapons.

Governments around the world have recognized the transformational power of biology, and thirty-six nations have invested in synthetic-biology research. Nowhere are these efforts more advanced or portentous than at China's Beijing Genomics Institute (BGI). Founded in 1999, BGI is the world's largest producer of genetic code, sequencing the equivalent of over fifteen thousand human genomes a year and harboring more sequencing capacity than all the labs in the United States combined. Given its aging population and lopsided dependency ratio resulting from its one-child policy, might China undertake society-wide enhancements? Those with the greatest capacity to encode and decode the software of life will have significant economic, political and military advantages.

Clearly, advances in both synthetic biology and genomics will have a profound impact on society and national security.

While the risk of biowarfare or chemically based terrorist attacks has been widely discussed since the Aum Shinrikyo cult's 1995 sarin-gas attack on the Tokyo subway, much less attention has been paid to the potential for bioenhancement technologies to alter national demographics and the military balance of power. For example, the Pentagon has invested in "supersoldier" technologies such as advanced prosthetics and medical transplant capabilities, which make it possible to implant animal tissue into humans to speed injury recovery times. For its part, China's BGI could accelerate the ability of government laboratories to develop society-enhancing therapies and interventions that could improve life expectancy and worker productivity. With a regulatory environment favorable to both stem cell research and human trials, China and other Asian nations could develop breakthrough gene therapies far more rapidly than the West.

It is also important to consider the impact of one exponential technology on another. For example, developments in robotics will not occur in isolation but will be enhanced by AI, potentially enabling swarms of robots to carry out attacks in unison. Bioengineering and nanomanufacturing could combine to create superfast and cheap nanocomputers, as well as superproductive renewable-energy resources such as synthetic biofuels. Synthetic biology and 3-D manufacturing will come together to mass-produce organic matter such as in vitro meat: food for the world. The synergies among these exponential scientific developments will be a driving geotechnological force that could further accelerate geoeconomic competition and geopolitical change. The appearance of exponential technologies—and their intersection with each other—promises an age full of disruptions: the exponential of exponentials.

Competition to capture the upper hand in these leading technology sectors is heating up among both states and nonstate actors. China's 12th Five-Year Plan pledges over $1 trillion in funding for research and development and commercialization in key areas such as advanced manufacturing, alternative energy and biotechnology, while innovations in robotics, nanotechnology and clean energy are emerging from Europe and Japan. International mergers, acquisitions and joint ventures represent another approach to acquiring exponential technologies. China's rapid adoption of semiconductor technology through the presence of German engineering giant Siemens is well-known. One sovereign wealth fund of the UAE, Advanced Technology Investment Co., recently acquired ownership of the microchip-production firm Global Foundries. Geoeconomic maneuvers can accelerate geotechnology transfer rapidly.

Public-private collaboration has brought together the long-term funding and scientific talent necessary for rapid technological progress. This diffusion of research-and-development activity into corporations and universities reflects the reality that a growing proportion of geotechnology activity is happening outside the control of even the most powerful states. Recall that Craig Venter's private firm, Celera Genomics, first decoded the human genome in 2000 after the U.S. government had faltered in its effort to do so.

In the future, we can expect not just partnerships but also genuine competition among state and nonstate actors to drive the development of and control over exponential technologies. Many companies, private laboratories, terrorist groups, organized criminal networks and other groups seek to harness and deploy these technologies. For example, IT giants such as Cisco and Microsoft have sold sensitive encryption technology to China and

As the number of objects connected to the Internet increases, a nation's "threat surface" will expand exponentially as well, meaning far more security vulnerabilities.

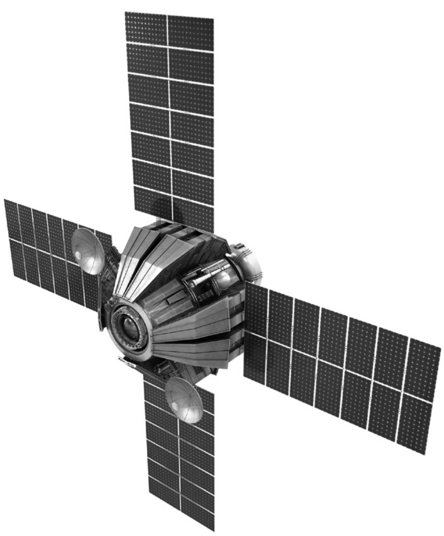
other governments over U.S. government objections and laws. Even where export controls are robust, technology often evades quarantine. Computer science, robotics, AI and synthetic biology all represent technologies that once were available only to the most powerful, well-resourced governments and their allied firms. Now they are much more widely distributed. Satellite imagery was a technology previously limited to powerful governments, but today GPS chips and Google Earth give each of us that capability on our mobile phones. While the majority of these developments have inured to the public's benefit, some have used them for ill. The terrorist organization Lashkar-e-Taiba, for example, used satellite imagery and GPS devices during its 2008 terrorist attack on Mumbai.

Robot and encryption technologies also give citizens the power to challenge the state. Much as Arab Spring activists used Facebook and Twitter to mobilize flash protests, the Sukey app enabled London rioters in the summer of 2011 to track the police, as did an "OccuCopter" during Warsaw's protests. In September 2011, the FBI accused Rezwan Ferdaus, a former Northeastern University student of Bangladeshi descent, of plotting to use remote-controlled, robotic aircraft loaded with plastic explosives to blow up the Pentagon and Capitol Building.

The international cyberhacking group known as Anonymous is a notable example of what author John Robb calls "guerrilla entrepreneurship." It not only can harness technology to suit its agenda but also can form alliances with other groups such as WikiLeaks to release the e-mails of target organizations, as it did in targeting the security consultancy Stratfor. Together, such guerrilla coalitions could assemble their capabilities to launch a zero-day attack, meaning a crippling simultaneous assault across multiple networks. Hezbollah and Hamas have deployed reconnaissance drones that have the potential to be weaponized. Even narcotics syndicates in Latin America have conducted joint research and development in robotics. The Revolutionary Armed Forces of Colombia reportedly developed robotic submarines capable of carrying five tons of cocaine to the shores of the United States. In July 2011, a robotic unmanned aerial vehicle known as the Wireless Aerial Surveillance Platform was unveiled at a hacking conference in Las Vegas. Weighing a mere fourteen pounds and sporting a six-foot wingspan, the autonomous flying vehicle is equipped with eleven separate antennae capable of intercepting mobile-phone conversations, text messages and Wi-Fi network traffic. In case the device encounters an encrypted, password-protected wireless network, it has a custom-built 340-million-word password dictionary for brute-force attacks against the network itself. This level of communications intercept was previously only available to the most sophisticated military services.

It is a mistake to limit our assessment of nonstate actors' impact to the cyberdomain, though that is where their ability to conduct offensive operations is most frictionless and anonymous. Eventually, efforts to leverage cutting-edge innovation may occur almost completely outside the jurisdiction of sovereign states. Technology billionaire Peter Thiel has provided funding for the Seasteading Institute, an effort to create an autonomous, unregulated floating platform in the Pacific Ocean to serve as a quasi-independent economic hub for technology companies.

Historically, geotechnology has been integral to the rise and fall of empires. The Soviet Union's lagging manufacturing output, inefficiency and poor infrastructure helped precipitate its decline, while China's capture of critical manufacturing and other sectors has helped fuel its rise. Many policy makers, including the chairman of the Joint Chiefs of Staff, General Martin E. Dempsey, have identified America's fiscal health and economic woes as a fundamental national-security concern. While many voices have called on Congress and Wall Street to do their part to get the nation's economic house in order, they do not emphasize enough the technological component of this challenge.



At present, the United States remains the dominant innovator in each of the aforementioned technology sectors, but competition is intensifying. The corporate superpowers defining today's technological landscape—Google, Facebook, Apple, Cisco, IBM and others—are American, but that may change as technological diffusion accelerates. The current phase of geotechnology competition has been characterized by China's persistent appropriation of American intellectual property. But China's heavy government investment and subsidization of its national scientific research-and-development agenda portends a move away from simple imitation toward actual innovation, with the potential for Chinese versions of Silicon Valley on the horizon.

Urgent steps need to be taken to maintain America's geotechnological advantage. In the same way that China and other nations are investing heavily in geotechnology as a means of ensuring geopolitical and geoeconomic advantage, so too must the United States if it wishes to retain its dominant role on the global stage. One imperative is a budgetary rebalancing away from outdated large-scale pork projects and toward technological research and development.

Economists Edward Mansfield and Robert Fogel have argued that the combination of major higher-education investments and mastery of complex technologies yields enormous economic and thus geopolitical gains. Accordingly, greater collaboration among government entities, the private sector and universities is crucial to fostering rapid innovation in areas such as alternative energy, robotics, nanomanufacturing and synthetic biology. High schools also need to promote long-term student engagement with these crucial technology clusters by revamping the national science, technology, engineering and mathematics curriculum. But America's educational system, which has not promoted science at home, has fostered a massive influx of scientific researchers from abroad, who are then forced to return to their own countries due to restrictive immigration policies. Armed with advanced technical degrees, these U.S.-trained graduates are sent home to compete with America.

In addition to spurring homegrown innovation, official measures can be taken to monitor the inevitable diffusion of sensitive technologies. The State Department's Office of the Science and Technology Adviser, Department of Defense and Department of the Treasury need to expand their collaboration in identifying dual-use technologies, closing loopholes that facilitate their export and sanctioning firms that violate these essential strictures. Of course, threats to America do not emanate solely from beyond its borders. As a result of Moore's Law, technology creation and access have been democratized, allowing dual-use technologies to slip into the wrong hands inside America itself.

America also needs a strategy to respond to any prospective attacks. With the growing diversity of actors capable of striking America's technological core at home and abroad, a "sovereignty first" policy (advocated by Anna Simons of the Naval Postgraduate School) assumes more state control than exists in much of the world. Targeting and retaliation strategies are needed to shape the electronic, legal, military and other potential responses to attacks from unpredictable and less readily traceable actors than states. This would allow for a cogent response plan to the new threat scenarios enabled by exponential technologies.

America's geotechnology advantage hinges on a deeper and more robust dialogue between its own coasts, a metaphor for our political and technological leadership. Unlike China, where eight of the nine top party officials have science and engineering backgrounds, America remains a nation governed by lawyers. Washington, DC, the nation's political hub, is highly distinct from the West Coast's Silicon Valley, with each encampment often struggling to understand the other's priorities and needs. While foreign leaders such as David Cameron and Dmitri Medvedev have come to prioritize Silicon Valley as a stop on their state visits, Washington's politicians seldom leverage the strategic dimensions of their own national technological-innovation hub. For America to remain competitive from a geotechnological perspective, this must change.

Thriving in a dynamic and disruptive twenty-first-century global landscape will require not only geopolitical insights and geoeconomic knowledge but also geotechnological innovation and strategy. America's nuclear arsenal, battle groups and other military advantages cannot deter the forces of innovation that are diffusing and resulting in new modes of achieving power and influence. Emerging technologies and their exponential rates of change will be upon us much sooner than imagined and will upend not only established regimes but also the world's balance of power. Just as it was not foreseen what a crucial role Twitter and Facebook could play in the tumultuous political events of the Arab Spring, so too have robotics, AI, synthetic biology and a panoply of other emerging technologies been underestimated for the potent changes they portend in global affairs. The battle for geotechnological advantage among governments, corporations and substate actors has broader national-security and foreign-policy implications than have yet been realized. □