National Security Implications of Leadership in Autonomous Vehicles

James A. Lewis

Digital technologies have created a transitional moment for societies. High-speed connectivity, cloud computing, and artificial intelligence (AI) are ubiquitous (even if not always visible) and are reshaping economies by creating new opportunities. This follows a pattern set centuries ago. Automation of basic tasks began in the eighteenth century and accelerated rapidly at the end of the nineteenth century, with a new wave of automation now well underway. Autonomous systems already create value across global markets by lowering costs and improving services. The ability to combine better sensors, more powerful computer processing, and faster connectivity expands the productivity of human labor, creates new services, and automates existing ones.

One of the most important parts of the next wave of automation is transportation, specifically the appearance of self-driving, or “autonomous,” vehicles (AVs). Self-driving cars offer immense gains in productivity and safety. The technologies developed for self-driving cars have broad commercial (and potentially military) implications. A self-driving car is a vehicle capable of navigating without a driver actively operating or monitoring it. Self-driving cars are a kind of specialized robot—not the humanoid robot common to popular culture, but self-operating devices that provide a commercially valuable service and automate routine tasks.

The impact of autonomous systems on the auto industry will be significant, as the technology behind AVs will reshape transportation and urban life as profoundly as the move from horses to cars. AVs are already a leading sector for private AI investment, reflecting the market’s estimate of their future importance.

Automation and the larger digital transformation create major challenges for national security, and the implications of AVs on national security deserve further attention. In addition to new opportunities, widespread deployment of AVs can also create new risks and vulnerabilities, particularly when considered in the context of tech competition between the United States and China.
National security can be defined as the condition where people can choose how they are governed and live in a world guided by the rule of law. To attain this requires an ability to defend the national interest and, increasingly, an ability to create and use technology in ways that support national security for both the near and long term. Technological leadership used to be seen as important for a few sectors, but its importance has spread across the entire economy. Innovation and the adoption of new technologies are the keys to the long-term growth needed for national security. This is particularly true for automobiles. Cars are now high-tech devices. Vehicles are built around semiconductors and software more than precisely engineered metal parts. The ability to build the cars of the future will be a good indicator of a country’s technological strength and abilities.

The Military Applications of Autonomous Vehicles

As much of the innovation and work on AVs is now happening in the private sector, it is reasonable to ask how much carryover there will be from commercial to military uses. In the early stages of developing AV technology, there was considerable overlap. As development progressed, there has been divergence, and the direct application of commercial autonomy will be smaller (the same way a combat aircraft and a passenger aircraft that share certain technologies can jointly benefit from research and development but are ultimately designed for fundamentally different purposes and requirements).

Autonomous devices that operate without human control are deeply attractive to militaries and are already deployed in aerospace and undersea vehicles by leading military powers. Autonomous ground vehicles are more challenging to develop, given the much more complex and varied terrain in which operations take place, but innovation in the commercial self-driving sector could improve military vehicles’ operations. This will be seen first in logistics and support vehicles (e.g., autonomous trucks), where the transition from commercial to military is simpler, and perhaps later in combat vehicles.

It is not an accident that the Defense Advanced Research Projects Agency (DARPA) was the government agency that began work on autonomous driving in 1984 with its Autonomous Land Vehicle program. DARPA then sponsored the earliest AV test in its Grand Challenges, which sought to accelerate the development of AV technologies by holding a race among prototypes for a cash prize. No one completed the first Grand Challenge in 2004. The second iteration, held in a desert area in 2005, was won by a university team which completed the 132-mile course in seven hours. DARPA held a third Grand Challenge two years later in a simulated urban environment, which was also won by another university team. These DARPA efforts, established in response to a 2001 National Defense Authorization Act mandate, jump-started the research into autonomous driving.

But the current geopolitical contest that threatens U.S. security is not a traditional military competition. It is a new kind of contest that underscores the importance of innovation capabilities and technology leadership. This means that having a strong AV sector, even if not directly applied to military use, is essential for national security. While there may be “spillover” effects from technology developed for commercial vehicles for military equipment, the primary contribution will be in strengthening digital industries. That is what will improve national economic performance and help reduce supply chain and espionage concerns. The importance of commercial development has grown. Since the end of the Cold War, advanced technologies have frequently originated in the private sector. The countries that will do best in economics and security will be those that have a strong private-sector tech base from which they can draw upon commercial technological developments.
The current geopolitical contest that threatens U.S. security is not a traditional military competition. . . . having a strong AV sector, even if not directly applied to military use, is essential for national security.

The main contribution of AVs to national security, however, does not come from self-driving tanks, but from the importance of the automotive sector to the nation. The automotive industry contributes 3.5 percent of U.S. GDP, making it one of the most important areas of industrial activity (as a comparison, the space and aerospace sector’s share is 4 percent). The development of autonomous and electric vehicles involves the ability to develop and deploy a broad range of important emerging technologies, such as AI, autonomy, and electric propulsion and batteries, and will drive progress in innovation in ways that shape many sectors. Even though the vast majority of the vehicle market is commercial and civilian, when looking at the value of economic strength to national security, AVs are a critical sector for overall national security.

**AV Development in the Context of Tech Competition**

The digital transition comes at a moment of significant geopolitical competition. The nature of global competition has changed and is increasingly a battle over technology and economic growth. The national capability to design, build, and innovate in technology will be crucial in this contest.

Technology creates new kinds of competition and conflict. Leadership in innovation and technology is central to global influence, prestige, and power. AVs are at the cutting edge of technology and are crucial to future U.S. strength. The United States has learned the hard way—in the case of telecom infrastructure manufacturing and Huawei’s extensive deployment and reach—that it is not in the United States’ interest to lose a strategic industry or to find itself dependent on an adversarial foreign power for key technologies. While there is minimal risk that the dynamic automotive sector in the United States would disappear like Nortel or Lucent, keeping this sector strong is essential for the national interest and national security. Automobiles are not an industry the United States can afford to lose any more than it would want to lose its aerospace industry.

Deploying fully autonomous cars is an immense technological challenge, requiring advances in computing, sensors, and networking. The first step has been the deployment of assisted driving systems, which are now relatively common in newer cars. Full autonomy is several levels beyond this and in various stages of testing by several companies. This involves further advances in sensors and processing. The work to meet these challenges will deepen the U.S. technological base and, by commercializing research, strengthen it. Companies will also need a supportive regulatory environment to be able to deploy AVs at commercial scale. For the United States, a strong technology base and supportive regulatory environment is crucial for national security and for maintaining its global influence and economic strength.

The ability to apply new technologies to commercial and security matters is as important as the ability to create them. Nations that have the companies and skills to develop AI and apply it to economic activities will be stronger and more secure. It is not surprising then that more and more countries are developing their own AI strategies, highlighting their importance for growth and safety. Sixty countries have already collectively issued over 600 AI policy initiatives, including governance efforts and financial support for
the sector. These policies will also help make the implementers more influential in the global arena, where global perceptions of tech leadership and economic performance provide substantial political benefit. This has been a core part of the United States’ international strength since landing on the moon in the late 1960s and is one reason why the competition with China creates such serious concerns.

For the United States, a strong technology base and supportive regulatory environment is crucial for national security and for maintaining its global influence and economic strength.

Adopting new technologies is the best path to creating wealth for countries such as the United States and the best way to increase productivity (which has been a problem for the United States and others, including China). AVs’ most important contribution to national security may come from increasing the United States’ productivity and wealth as part of the larger AI and robotics revolution.

The United States and China

There is a clear competition between the United States and China, and a major part of this competition is over leadership in technology. Both sides recognize the economic and security returns of technological leadership, and China has sought technological independence from the West for more than a century. The longer-term contest between the two is over how the world will be structured, and technological leadership is increasingly a determinant of national power.

China has a very different view of how societies should be governed, how international relations should be structured, and what its place should be among great powers. China is making a concerted and public effort to obtain superiority and to dominate key markets. The MIC2025 plan exemplifies the focus and importance of the technology sector. There are long-standing plans in China (albeit with mixed results) for a massive expansion of its technological capability. There is now a growing realization in the United States that it needs to respond to this, embodied in proposed legislation such as the Endless Frontier Act.

The desire in China to develop indigenous technological capabilities equivalent to the West dates back to the nineteenth century when European industrialization and its consequences displaced China from what it sees as its rightful place. China’s lack of advanced technologies allowed troubling European interventions in China’s sovereign affairs and began what the Chinese refer to as the “Century of Humiliation,” where the once-great power lost sovereign control to imperialist states in Europe. Almost two centuries later, after surpassing Europe economically, China believes it has reached a moment when it can return to the center of global power. The obstacle to this return is the United States.

There are many questions about this Chinese narrative of resurgence under the Chinese Communist Party’s (CCP) rule, but it meets compelling domestic political needs. The CCP’s claim to unchallenged rule is buttressed by powerful nationalist sentiments, long present in China as a reaction to the West and now exploited by the CCP. China’s president Xi Jinping has been clear in his views that the West is in decline and that a new world order should be centered on China. China’s rise has been propelled by a number of factors, including heavy state investment in technology, but also by illicit measures, including a disregard
for its World Trade Organization (WTO) commitments on the treatment of foreign companies, intellectual property (IP) theft, and a massive industrial espionage campaign targeting Western technology. China feels justified in these actions because of the Century of Humiliation and an artificial narrative about how the United States also relies on similar measures.

China’s goals are to ensure that its economic development and modernization continues, to end reliance on foreign technologies, and to build a technology base strong enough to produce high-tech weaponry and commercial products that, when combined with subsidies, can displace foreign competitors. China uses a hybrid state/market model. “Military-Civil Fusion” moves China’s economy much closer to a wartime footing, with a deep integration of the civilian and defense technological systems. Except in a few key areas, China’s innovation system remains weaker than that of the United States. Self-driving cars, however, are an area where there are several competitive Chinese firms and Chinese technology is strong. China’s government seeks to replace the United States in technological leadership and utilize technologies such as AVs to boost its military and economic competitiveness.

The 2021 annual threat assessment by the U.S. intelligence community addressed the risks to the United States’ national security from emerging technologies. The report concludes that China will maintain its policies to promote indigenous technological innovation, since Chinese leaders perceive these policies as the way to “reduce the dependence on foreign technologies, enable military advances, and sustain economic growth and thus ensure the CCP’s survival.” AVs and self-driving cars are part of this larger competition between the United States and China. They are also central to the competition over the development and use of AI. In all countries, this AI competition involves a blend of government funding and private actors driven in part or entirely by market incentives and government subsidies.

China already has a robust AV industry aimed at the commercial market. In early 2017, Qiushi (the official journal of the CCP) identified innovative military technologies, such as unmanned tanks and remote-controlled shop trucks, as a unique opportunity for China to exceed the United States in military power.

Both China and the United States have advantages and disadvantages in a contest that revolves around technology, research, and investment. The United States benefits from a robust entrepreneurial environment, a dynamic and risk-taking financial system, a strong research base, and an innovation community skilled at commercializing research. China also has an entrepreneurial private sector and a growing research sector, but the government’s willingness to invest large amounts over many years in its technological base is its primary advantage over the United States.

Chinese behaviors have eroded the commercial and technological globalization of the last three decades and, more importantly, pose a real national security risk to the United States. A world where China sets the rules will find that the rules are used to meet the needs of the CCP. Privacy is nonexistent in China and will be nonexistent in a world China leads. China will use its political power to confer commercial advantage on its companies at the expense of foreign competitors. This sounds harsh, but it is a description of the CCP, not of China itself.

Today, China has the world’s second-largest economy, supported by state-directed investment, is conducting aggressive industrial espionage programs globally over the internet, and is exhibiting a continued unwillingness to observe trade obligations. Using a Chinese AV, with all its internet connections, could be as risky as using Chinese telecoms.
**Autonomous Vehicles Will Create New Cybersecurity Risks and Vulnerabilities**

Cybercrime is a lucrative activity. It cost the global economy more than a trillion dollars in 2019, and the rate of increase in costs has accelerated since 2010. Cybercrime harms public safety, undermines national security, and damages economies. Ransomware, phishing schemes, and cryptocurrencies make it easier to succeed and monetize cybercrime and, when combined with the sanctuary offered by big countries, help explain the rapid increase. AVs, given their reliance on software, computing, and connectivity, could be a new vector for cybersecurity risks.

Cars have become rolling computers, loaded with cameras, microphones, and other sensors, all operated by complex software. Increasingly, modern cars connect to the internet and collect information on location, speed, and perhaps on driver communications (e.g., text, email, voice). This means that data from cars can be accessed remotely, with the owner’s permission or perhaps without it. Manufacturers already use this information for safety, convenience, predictive maintenance, and increasingly for entertainment. Future cars will collect even more data.

Some of that data can reference locations and geographical features. Cross-border data transmission can be problematic if sensitive information is being collected. A 2017 paper from the Chinese Academy of Telecommunication Research of China’s Ministry of Industry and Information Technology addresses that collection of information and considers it a matter of national security if foreign cars are used in China.

Anything that is connected to the internet is vulnerable. The hardware and software behind AVs create a range of opportunities to hackers, as does the need to integrate hardware and software. Many different systems interact in a self-driving car and provide opportunities for hacking to manipulate different systems, including navigation, entertainment, or connectivity with other cars and infrastructure. Given their reliance on continuous communication, another concern is external manipulation of AV systems. From manipulating indicators or attacking the camera system to read speed signs incorrectly, to tampering with road paint to misguide the vehicle, AVs contribute to a vulnerable threat environment.

In-vehicle and inter-vehicle communication systems are necessary for the safe operation of AVs. In similar ways to the vulnerabilities created by the Internet of Things (IoT), the “Internet of Vehicles” (IoV) creates new challenges for cybersecurity. Cars have become another device at the edge of the network where connectivity tempts attackers. Vehicles require not only that their systems be able to communicate with each other, but also connect with other AVs or infrastructure relying on a wireless network.

*Anything that is connected to the internet is vulnerable. The hardware and software behind AVs create a range of opportunities to hackers, as does the need to integrate hardware and software.*

Supply chains can be compromised from the start. If AVs come from an untrustworthy source or if there are supply chain risks, even the best cybersecurity will not have an impact in risk reduction. A vehicle could be 100 percent unhackable, but if the manufacturer has built-in access and collection or if the information collected by the vehicle is sent over the internet to a hostile country, it will circumvent any defense. There is no need for a back door when the manufacturer has the key to the front door.
Recent events highlight the potential for cybersecurity risks with AVs. Ransomware attacks, where an individual car or a class of cars could be rendered inoperable until a ransom is paid, are possible. While these could be aimed at individual car owners, it is more likely that cybercriminals will go after fleet operations or car manufacturers as better-paying possibilities. While a strong domestic AV industry will not eliminate cybersecurity risk, it would be much more preferable than a supply and car industry located in a hostile competitor.

**Espionage and Autonomous Vehicles**

The concerns regarding cybersecurity and data protection are not only important for user protection, but also in the context of national security and geopolitical competition with China. The trove of data collected by AVs, paired with cybersecurity vulnerabilities, creates an appealing target for intelligence collection. AVs will require thinking of cars in a new way when it comes to espionage risk.

It is unlikely that the governments of other major car producers—Germany, Japan, and Korea—will exploit this advantage. They have no political or security motive to do so. China is another matter, however. A 2020 survey of Chinese espionage by CSIS found 152 publicly reported instances of Chinese espionage directed at the United States since 2000. This did not include espionage against U.S. firms or persons located in China, nor did it include the more than 1,200 IP theft cases brought by U.S. companies against Chinese entities. U.S. officials have repeatedly stated that China’s espionage efforts exceed in scope and scale what was seen in the Cold War. This is because global digital networks and technologies provide China with immense new opportunities for espionage.

In China, the 2017 National Intelligence Law permits the Chinese government to demand and receive information from Chinese companies and citizens. Article 14 reads that “state intelligence work organs, when legally carrying forth intelligence work, may demand that concerned organs, organizations, or citizens provide needed support, assistance, and cooperation.” Legally carrying forth intelligence work means any action authorized by the CPP leadership, which keeps close control over China’s intelligence agencies and activities.

This means that data on location, behavior, and potentially conversations from the operators of Chinese-made cars could be accessed by the government over the internet. China is the world’s largest surveillance state, and Chinese network technologies provide the Chinese government with the tools for monitoring behavior and collecting information on residents in its territory—early examples include “Golden Shield” (a massive communications surveillance program) and “Green Dam” (a monitoring and censorship program required on laptops in China). China may have tipped its hand about intent when it banned Tesla vehicles from driving into military facilities and housing compounds for personnel working in sensitive industries and state agencies. (Tesla has attempted to placate the Chinese by promising to hold all Chinese data in China.) The features that allow the collection and exfiltration of data potentially make cars an ideal surveillance platform.

**The Road Ahead**

If this contest did not involve an unscrupulous and adversarial foreign power, it would be a normal commercial competition among companies, governed by the rules that apply to trade and the protection of IP. Commercial competition shapes U.S., European, Korean, and Japanese auto companies, but the same is not always true for China, where the government can play a much more directive role. That difference is what makes the contest over AVs so important.
There is a strong research base in Europe, and a long heritage of skilled engineering, but they have had difficulty commercializing the results of research. This may be less of a handicap in self-driving cars, given the strength and central position of the German auto industry, as long as Europe has access to leading-edge AI research and microelectronics from European and non-European sources. The contest takes place in a complicated international political environment. The chief complication is with Europe. Simply put, Berlin is a major driver of European policy, and it is currently unwilling to push hard on China because it is an essential market for Germany’s car industry—even though the Germans fear that China’s ultimate intent is to ransack their automotive technology and displace German carmakers. This could damage a major U.S. security and economic partner in ways that harm both its interests and those of the United States. Trends in European politics suggest this more relaxed approach to China may be changing as suspicions about China’s economic and political power grow.

The United States has also begun to address the decades-long shortfall in public investment on research and technology. The United States is unused to being challenged and was not prepared for this challenge from China. It has relied on technology to provide a qualitative advantage over opponents since World War II, but the requirements for technological advantage have changed. In the past, technological superiority was produced by a superb scientific establishment, long-term federal support for research, and close links between the research and industrial communities. Both support and linkages atrophied in the last few decades. More importantly, technological innovation is now led by the private sector and oriented toward commercial markets. This is where qualitative advantage for national security will come from in the future.

Technological progress is cumulative and continuous, and the pace at which nations adopt new technologies will help to determine their security relative to others. The nation that “dominates” AI (to quote Russian president Vladimir Putin) will not be “the ruler of the world,” but the nation that is best at creating and accommodating technological change will do better in economics and security than others. The ability to employ AI and autonomous systems to gain better performance, new digital services, and create wealth is at the core of the new international competition and an area where the United States must ensure that its policies and regulations keep it competitive. No nation will “dominate” AI or the AV market, but being a leader in autonomy is a vital U.S. interest and crucial for national security.

James Andrew Lewis is a senior vice president and director of the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C.

This report is made possible by support from Cruise LLC.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

© 2021 by the Center for Strategic and International Studies. All rights reserved.