Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

ISSUE BRIEF

Emerging Technologies: New Challenges to Global Stability

MAY 2020

ROBERT A. MANNING

INTRODUCTION

The world may be fast approaching the perfect storm, with the intersection of two major global trends. At a moment of historic transition, when the post-WWII and post-Cold War international order is eroding amid competing visions of world order and renewed geopolitical rivalries, the world is also in the early stages of an unprecedented technological transformation. It promises to be a period of exponential change, the second—and far more disruptive—chapter of the digital revolution that began with the Internet in the 1990s. Historically, technology usually races ahead of institutions, rules, and norms. The extraordinary magnitude of change at a time of global institutional fraying and disorder, however, portends a particularly dangerous gap in global governance impacting economies, societies, and the future of war.

Substantially more technology-driven change will take place during the coming two decades than in the first ICT (information and communications technology)-based revolution, with profound social, economic, and geopolitical ramifications. This new wave is a convergence of technologies, a digital synergy of artificial intelligence (AI), big data (the cloud), robotics, biotech/biosciences, three-dimensional (3D) printing, advanced manufacturing, new materials, fifth-generation (5G) powering the Internet of Things (IoT), nanoengineering and nanomanufacturing, and, over

Over the course of two years with the support of the Carnegie Corporation of New York, the Atlantic Council's Foresight, Strategy and Risks Initiative Director, Mathew Burrows and Senior Fellow, Robert Manning have been developing a set of "rules of the road" for ensuring cooperation in areas of mutual great power interest. This report along with a companion one on trade and finance are the first fruits of that effort to probe the challenges to global stability and to recommend solutions boosting global cooperation. This and the companion report have been informed by multiple exchanges with global experts from the United States, Europe, Russia, India, and China. Additionally, the webpage we are planning will include other related work and, over time, future work on the topic of multilateral cooperation, which we believe is the only way forward to ensure peace and prosperity.

the horizon, quantum computing. It is a still thickening merger of the digital and physical economies (called "online-to-offline," or O2O), transforming business models, transport, healthcare, finance, manufacturing, agriculture, warfare, and the very nature of work itself.

As a practical matter, as these technologies are deployed over the coming decades, they will bring about accelerating economic and geopolitical change beginning in the 2020s. For example, using AI powered by superfast 5G technology (up to one hundred times faster than the current 4G), the Internet of Things (IoT) will monitor and manage farms, factories, and smart cities. The increased productivity of ICT-connected sensors will warn of factory equipment needing maintenance; monitor energy use in buildings; give farmers real-time information on soil conditions; maintain and operate driverless vehicles; optimize energy-grid performance; and monitor remotely and diagnose individuals' health, with gene editing, engineering the demise of malaria-carrying mosquitos, and perhaps erasing hereditary DNA to eliminate horrific diseases.[1] In the national security realm, AI, 5G, and the IoT portend radical changes in missions from logistics and inventory management to surveillance and reconnaissance with air and undersea drones of all sizes and with autonomous capabilities.

I. THE EMERGING TECH REVOLUTION

Russian President Vladimir Putin was partly right when he famously said of AI, "Whoever becomes the leader in this sphere will become the ruler of the world."[2] It is not simply a race in the sense that first across the finish line wins, others lose, and game over. It is an ongoing, evolving process. But, there is an important "first mover" advantage to those who are leading in the development of AI, particularly "deep learning," which goes beyond pattern recognition to using neural networks based on how the brain works, with multiple layers of algorithms, each using the output of the previous layer.

Putin's remark captured the magnitude of the challenges and opportunities ahead. This tech revolution will be a key driver of economic growth, national comprehensive strength, and, thus, geopolitical status in the decades ahead. How well nations are able to innovate, and/or adapt and absorb emerging technologies into their economies will play a large role in determining their economic fate and geostrategic standing.[3] As was the case with the steam engine in the first Industrial Revolution, these emerging technologies can change the global balance of power. Ironically, the very techno-nationalism driven by great-power competition will hamper innovation writ large, which thrives on openness, transparency, and global scientific collaboration.

In this emerging economic universe, data are increasingly a key source of economic value. US technology-policy expert Alec Ross describes data as the "raw material" of the new Industrial Revolution.[4] Each day, 5.5 billion or more searches are made using Google, two trillion a year.[5] Ninety percent of the world's digital data have been created since 2016, and that amount is projected to increase by about 50 percent per year.[6] The cloud has given enormous computing power to the 4.57 billion people across the globe with Internet access.[7]

Neither the pace nor the scope of deployed new technologies will be evenly distributed or predictably linear in deployment, but rather, will occur in bursts as new tech is commercialized,

1 All of these applications are discussed in James Manyika et al., *Unlocking the Potential of the Internet of Things*, McKinsey Global Institute, June 1, 2015, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

2 "Putin: Leader in Artificial Intelligence Will Rule World," Associated Press, September 4, 2017, https://www.cnbc.com/2017/09/04/putin-leader-in-artificial-intelligence-will-rule-world.html.

3 For a detailed discussion of the geopolitical impact of tech innovation, see: Robert A. Manning and Peter Engelke, *Global Innovation Sweepstakes: A Quest to Win the Future, Atlantic Council,* June 2018, https://atlanticcouncil.org/wp-content/uploads/2018/06/The-Global-Innovation-Sweepstakes.pdf

4 Alec Ross, *The Industries of the Future* (New York: Simon and Schuster, 2016); "GoogleSearch Statistics—How Many Google Searches Per Day?" Serpwatch,

5 https://serpwatch.io/blog/how-many-google-searches-per-day/.

6 Ross, *The Industries of the Future*.

7 "Internet Users Distribution in the World—2020 Q1," Internet World Stats, March 3, 2020, https://www.internetworldstats.com/stats.htm.

Robotics and artificial intelligence are just two of the technologies revolutionizing the economic, political and security spaces in the decades to come. Source: Piqsels

and clustered geographically. For example, 74 percent of some three million industrial robots sold are concentrated in just five countries: Japan, China, the United States, Germany, and South Korea.[8] There are similar patterns in both global and national (e.g., in the United States, Silicon Valley, New York, and Boston; in China, Beijing, Shenzhen, and Shanghai) concentrations of venture capital and in the geography of published scientific papers. That advantage might accelerate as a result of the concentration of scientists, engineers, and technologists in those tech-centric locales. This has been the pattern regarding the geography of innovation in the United States, and it is occurring globally as well.

This portends a tech-driven hierarchy among nations, as well as increased inequality within nations as low-skilled—and increasingly, white-collar—jobs are automated, displaced by AI-powered robots and applications: redundant physical labor; car, truck, bus, and taxi drivers; legal research, etc. Those nations at the upper tier—led by the United States and China—are well positioned across the spectrum of emerging technologies for the economic and geostrategic advantages that will likely accrue to those at the leading edge of innovation. This is reflected in the global dominance in AI of the seven top US and Chinese firms: Amazon, Google, Facebook, Microsoft, Alibaba, Baidu, and Tencent.

A number of smaller nations—Israel, Singapore, and Sweden among them—punch well above their weight in terms of tech innovation capacity. All of these nations have been leaders in tech innovation. Much autonomous vehicle software is Israeli in origin; for Sweden, Skype, Spotify, and Ericsson are rare European global tech icons. These countries are all investing heavily in AI and related technologies. In this new knowledge economy, with data an essential raw material, having the relevant type of data and an ample pool of technical skills—not physical size—will be primary drivers of the geoeconomics, or geotechnology, of the future.

The new platforms have transformed business models from owning to using; that is, the "sharing" business culture. For example, Uber, the world's largest transportation firm, owns no autos; Amazon, the world's largest store, has few brick-and-mortar stores. The smallest startup has access to global markets. Mobile phones have become ubiquitous, with some

8 "Executive Summary World Robotics 2017 Industrial Robots," International Federation of Robotics, 2017, https://ifr.org/downloads/press/Executive_Summary_WR_2017_Industrial_Robots.pdf.

five billion worldwide, allowing developing nations to leapfrog generations of technology.[9] Chinese mobile payments have reached some $41.5 trillion—more than in the rest of the world combined—spearheaded not by banks, but by Alibaba and TenCent fintech (financial-technology) apps.[10] If China is the first cashless society (with India not far behind), tiny Estonia has become the world's first entirely digitized government.[11]

As technology leaps ahead of national governments and international institutions, this exponential velocity of change creates troubling conundrums. Will robots displace humans, work alongside them, and/or create new jobs? Should fully autonomous weapons—those that make the choice of who to kill and when without human involvement—be banned? The ominous fear of science-fiction movies, a "Terminator scenario" in which super-smart machines dominate humans, is high on the list of fears raised by leading scientists and technologists such as Elon Musk and the late Stephen Hawking. Machines with general intelligence near or surpassing that of humans do not yet exist, nor are they likely to in the foreseeable future. But, the warnings from such prominent voices suggest that this may be possible, if many decades away.

In the national security realm, emerging technologies using AI (including targeting, surveillance, and swarming drones, as well as hypersonic vehicles and possible wholly autonomous weapons systems) are transforming the future of warfare in ways that strategic planners are struggling to comprehend. At the same time, these technologies—especially autonomous weapons—raise difficult moral and ethical questions.

5G/Internet of Things

All the technologies discussed above will keep evolving as the questions raised continue to be debated. Yet, the future has arrived. The next wave of widely applied emerging tech over the next two to five years will be 5G, the next generation of wireless technology, which is up to one hundred times faster than the current 4G. Unlike previous mobile systems, 5G will use extremely high-frequency bands of the spectrum, called "millimeter bands." This requires substantial investment in hundreds of thousands of cellular radio antennas and other infrastructure.[12]

But, 5G is an evolving technology and other approaches are gaining favor, particularly in Japan and the United States. One prominent example is the idea of a software-based, rather than hardware-based, system known as the Open Radio Access Network (ORAN). The ORAN concept creates a new network model using software to replicate signal-processing functions. Thus, rather than having large, complex cell towers, 5G can reduce the size of its base stations, allowing them to be deployed more densely and in less conspicuous ways, and in a geographically dispersed manner.[13]

It will be a foundational enabler, the next milestone in Fourth-Industrial-Revolution technology. As artificial intelligence will power much of the promise behind 5G, it will, in turn, spur the growth of the Internet of Things. But, no less important, IoT will connect billions of sensors and billions of devices to each other, creating massive amounts of data, which makes AI more intelligent. US, European, and Asian wireless carriers are beginning to deploy early versions of 5G. Superfast and with low latency (delay), 5G will respond in real time, driving the IoT that will have a transformational impact on advanced manufacturing (sensors, robotics), consumers, and national security—including self-driving vehicles, remote surgery, finance, smart grids and cities, precision agriculture, and autonomous robots and weapon systems in the 2020s. McKinsey forecasts that IoT , powered by 5G, will add $3.9–$11.1 trillion in value by 2025.[14] Because 5G is transformational, however, cybersecurity is a critical concern. 5G/IoT will be adding a new layer to the internet, transforming it. It will increase usage and networks, connecting billions of sensors to millions of computers and networks and the cloud. It will add a layer of vulnerability on top of an already vulnerable communications platform, which can be readily hacked.

---

9 "Number of Mobile Phone Users Worldwide from 2013 to 2019 (in Billions)," Statista, https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/.

10 Steven Millward, "China's shoppers spent record $41.5t on their phones last year", *Tech In Asia*, March 27, 2019, https://www.techinasia.com/cashless-china-mobile-payments-spending-2018.

11 Nathan Heller, "Estonia, the Digital Republic," *New Yorker*, December 18, 2017, https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic.

12 For a detailed discussion of 5G and policy implications, see Doug Brake, "5G and Next Generation Wireless: Implications for Policy and Competition," Information Technology & Innovation Foundation, June 30, , https://itif.org/publications/2016/06/30/5g-and-next-generation-wireless-implications-policy-and-competition; Manyika et al., *Unlocking the Potential of the Internet of Things*.

13 For discussion on ORAN, see John T. Watts, *A Framework for an Open, Trusted, and Resilient 5G Global Telecommunications Network, Atlantic Council*, March 4, 2020, https://www.atlanticcouncil.org/in-depth-research-reports/report/a-framework-for-an-open-trusted-and-resilient-5g-global-telecommunications-network/.

14 James Manyka, et. al., *Unlocking the Potential of the Internet of Things*, McKinsey Global Institute, June 1, 2015, https:// www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

Secure 5G and the IoT will have a transformative economic and national security impact, but there is concern that cybersecurity will not be adequately built into 5G. Thus far, public/private-sector cooperation among all stakeholders has led to initial global technical and engineering standards. The nation that leads in developing and widely deploying 5G technology will have an important "first mover" advantage, with both economic and national security consequences. The United States and China are neck and neck in the global race to develop and deploy 5G technology, both internally and worldwide.

There is no shortage of tech companies from the United States and likeminded countries producing components for 5G, from chips to antennae. But, massive research and development (R&D) by Huawei and other Chinese firms have made them key players, particularly in 5G infrastructure. Huawei owns 1,529 standard patents, and Chinese firms hold 36 percent of such patents. As the UK decision to accept up to 35 percent of Huawei equipment in its 5G system suggests, global firms will need to license numerous Chinese patents regardless of the geopolitics; Chinese firms will likewise need to license patents from global firms.[15] There is intense competition between Qualcomm and Huawei for 5G chips; Ericsson, Nokia, and Samsung are also in the first tier. Samsung and Verizon have a major agreement, with the former supplying 5G wireless-access technology to the latter, which seeks to accelerate US deployment. Huawei and ZTE are believed to be ahead in antennae and base-station architecture, though Samsung, Ericsson, and Nokia are competitive. Japan (both in terms of its government and private mobile operators) is investing $45 billion by 2023, and plans to roll out 5G at the 2021 Olympics.

5G is integral to China's "Made in China 2025" plans to localize value chains and reduce dependency on foreign inputs. The intense involvement of China in creating global 5G technical and engineering standards, and its holding of patents, suggests that its plan, called "China Standards 2035," is well on its way. China has taken advantage of reduced US engagement in international standard-setting bodies to gain advantage.[16] Cybersecurity concerns have led to a concerted US effort to persuade allies to avoid using Huawei to build 5G networks. 5G geoeconomics are part of China's "Digital Silk Road" ambitions to connect the Eurasian landmass. Similarly, Beijing is also trying to build an integrated digital infrastructure in Southeast Asia. Huawei and other Chinese firms are actively seeking to export digital infrastructure around the globe. There is a risk of fragmented markets and, as 5G technology evolves, conflicting standards.

Regardless of the geopolitics of 5G, the breadth, scope, and speed of IoT applications will have a major economic impact over the coming decade, across a wide spectrum of sectors. Perhaps most prominently, the thousands of sensors and real-time vehicle-to-vehicle communication they would enable will accelerate the deployment of autonomous cars, buses, trains, ships, and trucks. This will initially happen for fleets, but by the 2030s, a new business model may prove viable, with ride firms like Uber, Didi, and Lyft altering how people think about ownership and use in terms of transport. The IoT will accelerate advanced manufacturing, using sensors for predictive industry management.

For rural areas and global food production (and for urban vertical farming), IoT is a critical facilitator for precision farming, defined as everything that makes farming more accurate and controlled when it comes to growing crops and raising livestock. It is key to farm management 2.0—connecting a wide array of tools, including Global Positioning System (GPS) guidance, control systems, sensors, robotics, drones, autonomous tractors, and other equipment. IoT will enable cities to become much smarter, with more efficient traffic control, environmental monitoring, and managing utilities like smart grids that increase energy efficiency. IoT will also provide cheaper, more efficient healthcare, health monitoring, and diagnosis, and has already benefited advanced manufacturing with sensors for predictive maintenance and safety, which help reduce costs.[17] Again, one big policy challenge—cybersecurity—remains, as billions more devices and computers can become hackable, with potentially disruptive consequences.

Artificial Intelligence

Artificial intelligence, which is fundamentally data plus algorithms , promises to be a gamechanger, whether in terms of economic or battlefield innovations. It is an enabling force, like electricity, a platform that can be applied across the board to industries and services: think AI plus X. One helpful way to think about AI is to differentiate its applications. In an interview with Martin Wolf of the *Financial Times,* leading Chinese AI guru

15 Dan Strumpf, "Where China Dominates in 5G Technology," *Wall Street Journal,* February 26, 2019, https://www.wsj.com/articles/where-china-dominates-in-5g-technology-11551236701.

16 Arjun Kharpal, "Power is 'Up for Grabs': Behind China's Plan to Shape the Future of Next-Generation Tech," CNBC, April 26, 2020, https://www.cnbc.com/2020/04/27/china-standards-2035-explained.html.

17 Manyika et al., *Unlocking the Potential of the Internet of Things*.

Kaifu Lee "distinguishes four aspects of AI: 'internet AI' — the AI that tracks what you do on the internet; 'business AI' — the AI that allows businesses to exploit their data better; 'perception AI' — the AI that sees the world around it; and 'autonomous AI' — the AI that interacts with us in the real world."[18]

AI is rapidly moving beyond programmed machine learning, such as robots doing repetitive human work, and single tasks like facial or voice recognition or language translation. AI is already becoming part of individuals' daily lives via "personal assistant" robots like Amazon's Alexa and Google Home, and, of course, in industrial and personal-service robots replacing many human functions. Moreover, there is an increasingly low bar to entry, as transparency among AI researchers has spawned wide access. There are several open-source websites to which leading researchers from top tech firms such as Google post their latest algorithms. TensorForce, for example, also enables one to download neural networks and software, with tutorials showing techniques for building them.[19] This example of the norm of global collaboration in the ecosystem of innovation underscores the downside risks to innovation from technonationalism.

By 2030, AI algorithms will be in every imaginable app and pervasive in robots, reshaping industries from healthcare and education to finance and transportation, as well as military organization and missions.[20] AI is already starting to be incorporated into military management, logistics, and target acquisition, and the military is exploring the use of AI to augment human mental and physical capacity. With regard to cybersecurity, it is an open question whether AI's algorithms will provide enhanced cybersecurity, or an advantage for future hackers.[21]

AI has already become a tool of authoritarianism, with facial recognition and big-data digital monitoring used for social control. China is not only implementing such policies, but exporting the technology. Similarly, AI has the potential of exacerbating the already vexing problem of weaponized social media, which has become a threat to social and political cohesion. As technology for trolls to create fake social media accounts improves, there is more risk not only of fake tweets and emails, but of video technology that can contrive fake videos with people appearing to say and do things they have never done. At the same time, AI could be a net plus as a tool for unmasking and attributing the trolling. Yet, it has been shown that AI is vulnerable to "spoofing," by injecting false images into its coding.[22]

AI is evolving beyond one-dimensional tasks of what is called "narrow AI" to "general AI."[23] The former refers to single tasks, such as facial recognition or language translation. The latter refers to AI that can operate across a range of tasks, using learning and reasoning without supervision to solve any problem, learning from layers of neural-network data, which is in its infancy. Two thirds of private-sector investment in AI is in machine learning—in particular, deep learning using neural networks, mimicking the human brain to use millions of gigabytes of data to solve problems. Most famously, AlphaGo beat the world champion at Go, a complex game with millions of moves. It was fed data from thousands of Go matches, and was able to select the best possible moves to outmaneuver its opponent. AI is demonstrating a growing capability to learn autonomously by extrapolating from the data fed into the algorithm.

The debate over AI remains unsettled. Some prominent technologists think AI will become as smart as, or smarter than, humans in a decade—a "Terminator scenario." Others say progress is incremental, and such breakthroughs are a century or more away. Consider that scientists don't know how all the billion or so neurons in the human brain work. How well, then, can AI replicate them? AI may be able to sort through thousands of job applications, or use data to suggest criminal prison sentences. But, absent human judgment, AI can't analyze character, social skills, or personal traits that don't show up in resumés, or how a person may change in prison.

With regard to the prospect of autonomous systems, AI lacks understanding of context and meaning: Can it tell if someone is pointing a real gun or a toy pistol at it? Some leading neurologists are skeptical, arguing that intelligence requires consciousness. Emotions, memories, and culture are parts

18 Martin Wolf, "China Battles the US in the Artificial Intelligence Arms Race," *Financial Times*, April 6, 2019, https://www.ft.com/content/2f295a9e-5f96-11e9-b285-3acd5d43599e.

19 Paul Scharre, Army of None: *Autonomous Weapons and the Future of War* (New York: Norton Books, 2018).

20 "Artificial Intelligence and Life in 2030," Stanford University, September 2016, 6–8, https://ai100.stanford.edu/sites/default/files/ai_100_report_0831fnl.pdf.

21 Martin Giles, "AI for Cybersecurity is a Hot New Thing—and a Dangerous Gamble," *MIT Technology Review*, August 11, 2018, https://www.technologyreview.com/s/611860/ai-for-cybersecurity-is-a-hot-new-thing-and-a-dangerous-gamble/.

22 Larry Loeb, "Security Vulnerabilities in RFC-1342 Enable Spoofing and Code Injection Attacks," *Security Intelligence*, December 7, 2017, https://securityintelligence.com/news/security-vulnerabilities-in-rfc-1342-enable-spoofing-and-code-injection-attacks/.

23 Kai-Fu Lee, *AI Superpowers: China, Silicon Valley, and the New World Order* (New York: Houghton Mifflin Harcourt, 2018).

of human intelligence that machines cannot replicate. There is a growing body of evidence that AI can be hacked (e.g., misdirecting an autonomous car) or spoofed (e.g., identifying targets with false images).[24] One potential problem for many applications is that humans don't know how AI knows what it knows, or how its decision-making process worked. This makes it difficult to test and evaluate, or to know why it made a wrong decision or malfunctioned. This will only be more difficult as deep learning becomes more sophisticated. It also suggests a compelling argument for, as a guiding principle and operational norm, having humans "in the loop," if not in control of AI decision-making.

Catastrophic Risks

The urgency of developing a global consensus on ethics and operating principles for AI starts from the knowledge that complex systems fail. Complex systems like supercomputers, robots, or Boeing 737 jets, with multiple moving parts and interacting systems, are inherently dangerous and prone to fail, sometimes catastrophically.[25] Because the failure of complex systems may have multiple sources, sometimes triggered by small failures cascading to larger ones, it can require multiple failures to fully understand the causes. This problem of building in safety is compounded by the fact that as AI gets ever smarter, it is increasingly difficult to discern why and how AI decided on its conclusions.

The downside risks in depending solely on an imperfect AI, absent the human factor in decision-making, have already begun to reveal themselves. For example, research on facial recognition has shown bias against certain ethnic groups, apparently due to the preponderance of white faces in the AI's database.[26] Similarly, as AI is employed in a variety of decision-making roles, such as job searches or determining parole, absent a human to provide context, cultural perspective and judgment bias become more likely.

Robots: Killing Jobs and/or People?

Automated systems, machines replicating human activity, have been around for many decades (e.g., an automated teller machine (ATM)). Yet, of late, robots have become icons (or, in science-fiction movies, demons) of the tech revolution. Why? Until this century, industrial robots, mainly deployed in auto-assembly plants (and, more recently, in the electronics industry) were not standardized, had no software, and were not connected to the Internet. But, over the past two decades, as ICT became more capable and computers more powerful, sensing-technology robots have become cheaper, more ubiquitous, and more connected (for example, Xbox sensors are used to animate robots). There are now more than three million robots, and thirty-one types of personal robots (e.g., Roomba robot vacuums, or drones).[27]

Baxter, a humanoid robot created at the beginning of this decade, is illustrative of the new forms and capabilities of robots. Baxter is mobile and normal sized on its pedestal (about five feet, ten inches tall), with dexterous arms, sensing software that allows it to be "trained" by simply copying human actions, and software that can be updated. At $22,000, it is a fraction of the cost of most industrial robots. Telepresence robots are being used in hospitals, allowing doctors to remotely assess patients and surgeons to perform surgery remotely, at even lower costs.[28]

Despite many fears, AI-enabled robots have not, to date, generated substantial net job losses. Some studies suggest the opposite—increased productivity and more jobs.[29] As discussed above, the five countries with the most deployed robots (the United States, China, Japan, South Korea, and Germany) all have near-record-low unemployment. There remains heated debate over whether robots will displace humans, leading to a dystopia of bored, unemployed workers, or will generate new jobs requiring new skills. There is growing evidence of humans

24 Sigal Samuel, "It's Disturbingly Easy to Trick AI into Doing Something Deadly," *Vox*, April 8, 2019, https://www.vox.com/future-perfect/2019/4/8/18297410/ai-adversarial-machine-learning-self-driving-cars-tesla-stickers-medicine-military.

25 Richard I. Cook, "How Complex Systems Fail," Cognitive Technologies Laboratory, 2000, https://web.mit.edu/2.75/resources/random/How%20Complex%20Systems%20Fail.pdf.

26 Karen Hao, "This is How AI Bias Really Happens—and Why It's So Hard to Fix," *MIT Technology Review*, February 4, 2019, https://www.technologyreview.com/s/612876/this-is-how-ai-bias-really-happensand-why-its-so-hard-to-fix/.

27 "Executive Summary World Robotics 2018 Industrial Roots," International Federation of Robotics, 2018, https://ifr.org/downloads/press2018/Executive_Summary_WR_2018_Industrial_Robots.pdf.

28 Robert A. Manning, *Rising Robotics and the Third Industrial Revolution, Atlantic Council*, 2013, https://www.files.ethz.ch/isn/167642/rmanning_risingrobotics.pdf.

29 Anders Berndt, "Industrial Robots Increase Wages for Employees," Phys.org, October 22, 2018, https://phys.org/news/2018-10-industrial-robots-wages-employees.html.

working alongside robots, whose physical dexterity remains challenged, particularly where human judgment or context is involved—from automated call centers to "pilots" of drones thousands of miles away.[30]

Still, perhaps the greatest concern about these emerging technologies is the socioeconomic consequences: that AI-driven automation will mean the loss of jobs. The jury is still out on whether more jobs will be lost than will be created. A McKinsey Institute study examining scenarios across forty-six countries forecast that up to one third of the workforce could be displaced by 2030 by AI-driven technologies, with a midpoint of 15 percent.[31] A 2018 Organisation for Economic Co-operation and Development (OECD) study concluded that 14 percent of jobs in OECD nations are highly automatable, and an additional 32 percent could be changed.[32] More optimistically, a Deloitte study found that technology has created more jobs than it destroyed over the past one hundred and forty-four years. While anticipating "creative destruction" of jobs lost, and new industries and jobs created, it argues for a net gain.[33] Nonetheless, AI and robotics will undoubtedly transform the future of work, and adapting and rethinking education and training to new skills required for a twenty-first-century workforce are looming policy issues that most governments have yet to fully address. Some technologies appear likely to create new job opportunities. For example, 3D printing, with a relatively low bar of entry, could spark local manufacturing outside of major industrial areas, shrink global supply chains, reduce transport costs, and localize trade.[34]

Biotech

Bioscience is another important, and disruptive, component of the tech revolution. Some go so far as to call the current era the "Biological Century." Since the 1970s, breakthroughs on recombinant DNA and the ability to manipulate life at the molecular level are revolutionizing healthcare. The melding of biotech with information technology (IT), and now AI and synthetic biology, creates this new world—think of genetic code as software. It shocked the world in November 2018 when He Jankui, a Chinese researcher, announced he had used CRISPR, a gene-editing technique, to alter the genomes of twin baby girls to make them resistant to human-immunodeficiency-virus (HIV) infection, a trait that would then become hereditary.[35] The claim—yet to be reported in a scientific paper—initiated a firestorm of criticism, with some scientists and bioethicists calling the work "premature," "ethically problematic," and even "monstrous."[36] Some troubling continuing Chinese genetic experiments suggest how fragile and tentative the ethical consensus is. Scientists at China's Kunming Institute are creating transgenic macaque monkeys with copies of a human gene believed to shape intelligence, and other such experiments, to the outrage of many Western scientists.[37]

Biotech has already begun to show its potential to contribute to immunotherapy for horrible illnesses—such as amyotrophic lateral sclerosis (ALS) and rare blood diseases—make designer cells, create new pathogens of high lethality, or enhance the physical and intellectual capabilities of humans. Where should the line be drawn? Are there unanticipated consequences of editing genes? Such troubling questions recently incited a group of dozens of leading scientists (including two of CRISPR's founders) and researchers to call for a moratorium on gene editing, as well as the creation of an international governance body to devise a set of rules and standards to guide any future alteration of the human genome.[38]

The explosion of biotechnology across the spectrum of possibilities is, of course, enabled by the exponential advances in computing power, AI, and big data. Biotech is,

30 "The Impact of Robots on Productivity, Employment, and Jobs," International Federation of Robotics, April 2017, https://ifr.org/img/office/IFR_The_Impact_of_Robots_on_Employment.pdf.

31 *Jobs Lost, Jobs Gained: Workforce Transitions in a Time of Automation, McKinsey Global Institute*, December 2017, https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Future%20of%20Organizations/What%20the%20future%20of%20work%20will%20mean%20for%20jobs%20skills%20and%20wages/MGI-Jobs-Lost-Jobs-Gained-Executive-summary-December-6-2017.ashx.

32 "OECD Policy Brief: Putting a Face Behind the Jobs at Risk of Automation," Organisation for Economic Co-operation and Development, April 4, 2018, https://skillspanorama.cedefop.europa.eu/en/news/oecd-policy-brief-putting-face-behind-jobs-risk-automation.

33 "Technology and People: The Great Job-Creating Machine," Deloitte, August 2015, https://www2.deloitte.com/uk/en/pages/finance/articles/technology-and-people.html.

34 Richard A. D'Aveni, "The Silver Lining in the U.S. Manufacturing Slowdown," *Forbes*, January 25, 2019, https://www.forbes.com/sites/richarddaveni/2019/01/25/the-silver-lining-in-the-u-s-manufacturing-slowdown/#75ecf0f2be30.

35 Dennis Normile, "CRISPR Bombshell: Chinese Researcher Claims to Have Created Gene-Edited Twins," *Science*, November 26, 2018, https://www.sciencemag.org/news/2018/11/crispr-bombshell-chinese-researcher-claims-have-created-gene-edited-twins.

36 Ibid.

37 Antonio Regalado, "Chinese Scientists Have Put Human Brain Genes in Monkeys—and Yes, They May Be Smarter," *MIT Technology Review*, April 10, 2019, https://www.technologyreview.com/s/613277/chinese-scientists-have-put-human-brain-genes-in-monkeysand-yes-they-may-be-smarter/.

38 Eric S. Lander, et al., "Adopt a Moratorium on Heritable Genome Editing," *Nature*, March 13, 2019, https://www.nature.com/articles/d41586-019-00726-5.

in some respects, more mature than AI and other emerging technologies. From the sequencing of the human genome and its consequences, to biotech creation of genetically modified organisms (GMO) agriculture, synthetic biology, (combining engineering and biology to manipulate cells and submolecular life) to produce products for agriculture, pharmaceutical goods, new materials, and other goods, many applications are widely commercialized. This IT/AI/biotech fusion also lowers the cost of entry for the dark side of threatening activities, from bioengineered organisms to manufactured illegal drugs to biowarfare agents.[39] In the United States, bioscience firms employ 1.74 million people, and had an overall impact on the US economy of some $2 trillion in 2016.[40]

The remarkable social and economic benefits yielded from biotechnology, while still evolving, are already apparent. GMOs that are drought resistant, need no pesticides, and produce more bountiful crops appear an important response to climate change while providing food for a growing population. New drugs can treat rare diseases, improve the chances of curing cancer, advance immunotherapy and regenerative medicine, and the list goes on. Yet, as the potential to alter gene pools and alter or create life raises profound ethical and philosophical questions and concerns. A growing anti-science mindset, which seems to accompany populism and distrust of elites, has raised opposition to GMOs and immunization in the United States and Europe.

Energy and the Tech Revolution

One underanalyzed area with regard to the tech revolution is the role it is beginning to have in transforming the future of energy. At a time when growing concern about climate change is accelerating efforts to reduce greenhouse-gas (GHG) emissions, of which fossil fuels are a major source, technology may have the following impacts.

- ***Electrification of transport:*** Projections vary, but China, the largest e-car manufacturer, plans to make one in five cars electric by 2025. A BP scenario forecast suggests 30 percent of passenger vehicles will be e-cars by 2040, by which time oil demand will peak and begin a downward trajectory.[41] Tesla's success has injected a new dynamism into e-car development and consumer acceptance. Such change would alter urban mobility, reducing carbon-dioxide (CO2) emissions and local air pollution.

- ***Battery/energy storage:*** Breakthroughs in cheaper and more efficient batteries will have profound impacts on, and prospects for, scaling up wind and solar energy and, hence, the transition to a post-petroleum economy. The US Department of Energy has set a goal of batteries that can store energy at less than $100 per kilowatt hour, less than half of current costs. While both government and private-sector R&D are intense in the quest for this silver bullet, such a breakthrough is unlikely before 2025–2030.

- ***5G and IoT:*** These technologies will shape smart grids, smart factories, and smart buildings, and enable smart cities (buildings consume 30 percent of all electricity).

- ***Advanced manufacturing (3D printing):*** This should help lower costs and allow for the localization of production for renewable energy sources, including solar cells, wind turbines, and their supporting equipment.

- ***Modular nuclear:*** Small-scale modular nuclear power, which is cheaper and more easily deployable, may be commercially viable before 2030.[42]

---

39 Thom Dixon, "Tomorrow's Biosecurity Surprise," Pacific Forum, April 3, 2019, https://mailchi.mp/pacforum/pacnet-23-tomorrows-biosecurity-surprise?e=3c4f7547f3.

40 Anita M. Harris, "BIO Issues Glowing Report on US Bioscience Industry," *New Cambridge Observer*, June 6, 2018, https://newcambridgeobserver.com/2018/06/06/bio-2018-stats/.

41 Keith Bradsher, "China Hastens the World Toward an Electric-Car Future," New York Times, October 9, 2017, https://www.nytimes.com/2017/10/09/business/china-hastens-the-world-toward-an-electric-car-future.html; Julia Pyper, "BP Forecast: Shared, Autonomous EVs Will Help Drive to Peak Oil Before 2040," *Greentech Media*, February 21, 2018, https://www.greentechmedia.com/articles/read/bp-forecast-autonomous-electric-vehicles-peak-oil#gs.Ocx0Pgrc.

42 Kiran Stacey, "Small Modular Reactors are Nuclear Energy's Future," *Financial Times*, July 25, 2016, https://www.ft.com/content/bcffe4d2-2402-11e6-9d4d-c11776a5124d; Robert Fares, "3 Ways Small Modular Reactors Overcome Existing Barriers to Nuclear," *Scientific American*, May 19, 2016, https://blogs.scientificamerican.com/plugged-in/3-ways-small-modular-reactors-overcome-existing-barriers-to-nuclear/.

Beyond such specific impacts on oil demand and CO2 emissions, the realization of transformed energy systems may have far-reaching geoeconomic and geopolitical consequences. Battery storage and renewable breakthroughs, combined with 3D printing, should enable distributed-energy generation and localized production for developing nations, allowing them to leapfrog grids and pursue more decentralized development. The geopolitical shifts resulting from peak oil demand and the electrification of transport carry great risk for major oil producers, with the potential for dramatic instability in petrostates including Russia and parts of Africa, the Middle East, and Latin America. Conversely, those states that innovate and/or deploy new energy technologies (and related "green" technologies), will be best positioned economically. The planning and investment in post-petroleum energy sources and infrastructure by the United States, European Union (EU) nations, Saudi Arabia, and the Gulf states are an example of such efforts at foresight.

Quantum Computing

Looking over the horizon toward 2040, quantum computing is a good illustration of why the world may only be at the front end of the technology revolution. Quantum computing is based on the principles of quantum mechanics, which revealed that, at the atomic and subatomic levels, the behavior and characteristics of energy and matter can be different things simultaneously. This behavior of subatomic particles was so strange that Albert Einstein once referred to it as "spooky action from a distance." Unlike the binary nature of current computers—ones and zeros—quantum bits, known as qubits, can exist in both states at once.[43] With a sufficient amount of qubits that are stable long enough, a quantum computer would be able to perform exponentially more calculations than current supercomputers. In a single step, it could solve problems that might take years with current computers.

Such quantum computer capabilities would enable computations otherwise not possible in areas like chemistry, such as modeling that could produce new materials by simulating the behavior of matter at the atomic level.[44] Similarly, Wall Street firms are interested in quantum because they could enable vastly more algorithm possibilities and more precise risk-management systems, modeling financial markets, complex bank exposures, and possible losses.[45] Not least, quantum computer power could have a huge impact on deep-learning AI, making it exponentially more powerful. Cryptography may be the most disruptive application of quantum computers. Quantum computing would revolutionize cryptography, with techniques that are theoretically impossible to break. Conversely, quantum computers could allow heretofore unbreakable encryption to be deciphered. The possibility of perfect cybersecurity, writ large, has transformative implications for intelligence, national security agencies, and military forces.[46]

Quantum computing may sound like science fiction, but look no further than the Chinese launch of the first quantum satellite in 2016 to grasp that it is already a major component of R&D portfolios of major tech firms (led by IBM, Microsoft, Google, and Intel), several dozen well-financed startups, and the governments of at least fourteen countries (led by the United States, China, and EU). China has made developing quantum computers a major element of its tech strategy.[47] Total quantum R&D spending by national governments exceeds $1.75 billion.[48] Quantum science could be applied to communications, radar, sensing, imaging and navigation. This could change the calculus of defense investment for the United States and other major powers, and helps explain the substantial Chinese investment in quantum R&D.[49]

---

43 "Einstein's 'Spooky Action' Goes Massive," *Science Daily*, April 25, 2018, https://www.sciencedaily.com/releases/2018/04/180425131858.htm.

44 Will Knight, "Serious Quantum Computers are Finally Here. What are We Going to Do with Them?" *MIT Technology Review*, February 21, 2018, https://www.technologyreview.com/s/610250/serious-quantum-computers-are-finally-here-what-are-we-going-to-do-with-them/.

45 Richard Waters and John Thornhill, "Quantum Computing: The Power to Think Outside the Box," *Financial Times*, September 2, 2018, https://www.ft.com/content/154a1cf4-ad07-11e8-94bd-cba20d67390c.

46 Vishnu Chundi, "Impact of Quantum Computing on Cryptography and Bitcoin Security," *Medium*, April 1, 2018, https://medium.com/@vishnu_3187/impact-of-quantum-computing-on-cryptography-and-bitcoin-security-db5004f92eb0; "How Will Quantum Computing Impact Cyber Security?" *TechNative*, March 28, 2018, https://www.technative.io/how-will-quantum-computing-impact-cyber-security/.

47 Elsa B. Kania and John K. Costello, *Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership, Center for a New American Security,* 2018, https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Quantum-Tech_FINAL.pdf?mtime=20180912133406.

48 "What Countries are Leading This 'Quantum Computing Race?'" *Quantum Computing*, March 29, 2018, https://quantumcomputing.stackexchange.com/questions/1472/what-countries-are-leading-this-global-quantum-computing-race.

49 Kania and Costello, *Quantum Hegemony?*

Realizing the possibilities of quantum computing will require new algorithms, software, programming, and, likely, other technologies yet to be conceived.[50] There are several different types of qubits, and efforts at prototypes to date have not gone beyond seventy-two qubits, far less than are needed for achieving the capabilities described above. Some project that the types and uses of quantum computers will be varied, and may be limited with regard to functions, not getting beyond tens of qubits for the foreseeable future.[51] Estimates vary on when fully operational quantum computers will realize all their possibilities. As an analysis in *Scientific American* put it: "If 10 years from now we have a quantum computer that has a few thousand qubits, that would certainly change the world in the same way the first microprocessors did. We and others have been saying its 10 years away. Some are saying it's just three years away, and I would argue that they don't have an understanding of how complex the technology is."[52]

National Security Impact

Throughout history, technologies—from the Gatling gun and the steam engine in the First Industrial Revolution, to the mechanization of warfare and the rise of the assembly line in the Second Industrial Revolution, to precision-guided weaponry resulting from the computer revolution—have shaped and reshaped strategy, tactics, and the character of war. Not least, the unprecedented existential threat of nuclear weapons forced a paradigm shift in the very idea and conduct of war among major powers.

Now, the emerging technologies of the still-nascent Fourth Industrial Revolution, though often largely civilian purposed or of dual use, are once again upending all things military in ways previously unimaginable. Already, AI, big data, unmanned air and sea drones, 3D printing, and, most of all, increasingly autonomous weapons have begun to raise new ethics questions and alter warfighting, logistics, and military organization. Over the coming two decades, the synergy of this suite of technologies, with AI as a synthesizing enabler, may have as revolutionary an impact on the conduct and strategy of war as nuclear weapons have had since 1945.[53] The classic security dilemma—what one nation sees as weaponry to improve its defenses is viewed as a threat by another, creating a cycle of one-upmanship (in other words, an arms race)—is a driver of the imperative of new tech innovation that, in turn, raises the stakes of confrontation.

Disruptive technologies pose new risks and challenges to strategic stability across increasingly contested global commons—air, sea, cyber, and space. New technologies could undermine nuclear second-strike capabilities, the basis of deterrence and strategic stability. For example, hypersonic missiles and/or glide vehicles traveling at Mach 5 or faster (five times the speed of sound), now in various stages of development by the United States, China, Russia, and India, could nullify or evade missile defenses and create a "use it or lose it" situation for nuclear-weapons states. Similarly, swarming unmanned underwater vehicles (UUVs) could locate and/or disable ballistic-missile nuclear submarines, which are a key component of US nuclear deterrence. Other disruptive scenarios would be the use of cyber warfare to disable a nation's command-and-control capabilities or the use of directed-energy (laser) anti-space weapons to disable or destroy the satellites upon which so much modern warfare and communication depend. Yet, these emerging threats to nuclear crisis stability have not sparked new codes of conduct, norms, or "redlines" to constrain these mutual vulnerabilities.

In some respects, the prospect of fully autonomous weapons is not a huge technological leap from current—and, in some cases, long-deployed—precision-guided or "smart" weaponry. They may be best understood as a spectrum with varying degrees and gradations of complexity, autonomous capability, and human involvement—from the automatic, like machine guns, on one end, with varying degrees of human supervision to fully autonomous on the other. The US Navy's Harpoon semiautonomous anti-ship missile—which, once fired, determines what are enemy ships and where they are—has been deployed for more than three decades. Similarly, the Navy's HARM (high-speed anti-radiation missile), a semiautonomous missile, seeks out enemy radar on its own once fired. Likewise, the US Tomahawk anti-ship missile, once launched at a data-target area, flies in a search pattern and is able to locate, choose, and fire at a target on its own. The US Navy's AEGIS and the US Army's Patriot missile-defense

50 Larry Greenemeier, "How Close are We—Really—to Building a Quantum Computer?" *Scientific American*, May 30, 2018, https://www.scientificamerican.com/article/how-close-are-we-really-to-building-a-quantum-computer/.

51 Frank Wilczek, "The Quantum Computers in Our Future," Wall Street Journal, March 14, 2019, https://www.wsj.com/articles/the-quantum-computers-in-our-future-11552579161?mod=searchresults&page=1&pos=1.

52 Greenemeier, "How Close are We—Really—to Building a Quantum Computer?"

53 For a thoughtful discussion of the similarities and differences of the impact of AI on strategy compared, to that of nuclear weapons, see Kenneth Payne, "Artificial Intelligence: A Revolution in Strategic Affairs?" International Institute for Strategic Studies, September 2018, https://www.iiss.org/publications/survival/2018/survival-global-politics-and-strategy-octobernovember-2018/605-02-payne.

systems, for example, have various modes of semiautonomous and autonomous modes. In both cases, human control (human action involved during action or supervision, with an ability to intervene analogous to avoiding "flash crashes" in financial markets) has been a factor in both accidents and avoiding them.

To date, there are only a few lethal weapon systems that can be called fully autonomous, with sensors and algorithms that decide who, when, where, and what the target is once launched. The Israeli HAROP, an anti-radar missile, is a prominent example. As discussed in his invaluable book *Army of None,* Paul Scharre explains that the HAROP, once it is deployed and programmed to search in a particular space, can hover with a 350-kilometer range for more than two hours, to search for a target and decide on its own when and what target to hit. Illustrating how rapidly these emerging technologies are diffusing, the HAROP has already been exported to China, India, South Korea, and Turkey.[54] Moreover, some ninety nations have surveillance drones, and at least sixteen have armed drones.[55] Over time, drone technology will become more sophisticated, cheaper, and more widely diffused.

The weapons systems discussed above are just a sampling of technologies with military applications that are racing ahead of a set of rules, norms, or codes of conduct for governance. A UN Convention on Certain Conventional Weapons (CCW) in Geneva has been examining the issue of autonomous weapons since 2014, and has yet to decide on a definition. The US Department of Defense has clear guidance authorizing the development and deployment of various degrees of semiautonomous weapons (cyber defense is exempted), but draws a firm ethical line. As former Defense Secretary Ash Carter explained, "in every system capable of executing or assisting the use of lethal force, there must be a human being making the decision. That is, there would be no literal autonomy."[56] The fear of a Terminator-like future world has sparked a "Campaign to Stop Killer Robots." The alarm initially raised by prominent scientists and technologists like Stephen Hawking and Elon Musk has grown. In 2017, a group of more than three thousand AI and robotics scientists and experts sent an open letter to the UN CCW, cautioning against the use of lethal autonomous weapons.[57]

Such concerns are legitimate; technology, of course, is imperfect. The history of complex systems with many moving parts is that they are never 100-percent error free; it is assumed that, however rarely, complex systems will fail.[58] Think of National Aeronautics and Space Administration (NASA) space-shuttle failures, or Japan's Fukushima nuclear accident. The most chilling, if nearly forgotten, example of technological error occurred at the height of the Cold War, on September 26, 1983. A new Soviet satellite early-warning system mistakenly warned that it detected a US missile launch, and was ready to counterstrike, almost ending the world. Only the cautious skepticism of duty officer Lieutenant Colonel Stanislav Petrov, who suspected it was an error—and upon checking with Soviet ground-based radar confirmed there were no missiles launched—prevented global catastrophe.

In recent years, there have been some catastrophic failures with US semiautonomous weapons systems, well documented in Paul Scharre's 2018 book *Army of None*. In 1988, in the midst of combat during the Iran-Iraq war, the AEGIS defense system's radar mistook an Iranian civilian airliner that had taken off at the same time as an Iranian military plane for a threat and shot it down, killing two hundred and ninety passengers.[59] Two other prominent examples have occurred with the Patriot and Aegis missile-defense systems. In 2003, during the Iraq war, there was a friendly-fire incident in which Patriot PAC-2 missiles misidentified a British Tornado fighter jet, and a second incident in which a PAC-2 mistakenly detected an anti-radar missile and fired, and its missiles eventually found a US F-15/Hornet in the vicinity. The causes varied, including glitches in systems within systems, human error, overreliance on technology, and either too much or too little human supervision.

54 Scharre, *Army of None*. Much of the discussion on AI and autonomous weapons is derived from Scharre's book.

55 Ibid., 102.

56 Ash Carter, "Shaping Disruptive Technological Change for Public Good," Harvard Kennedy School Belfer Center for Science and International Affairs, August 2018, https://www.belfercenter.org/publication/shaping-disruptive-technological-change-public-good.

57 "Autonomous Weapons: An Open Letter from AI and Robotics Researchers," Future of Life Institute, July 28, 2015, https://futureoflife.org/open-letter-autonomous-weapons/.

58 Cook, "How Complex Systems Fail."

59 Max Fisher, "The Forgotten Story of Iran Air Flight 655," *Washington Post*, October 16, 2013, https://www.washingtonpost.com/news/worldviews/wp/2013/10/16/the-forgotten-story-of-iran-air-flight-655/?utm_term=.d8472bc77099.

These tragedies should serve as early warning. And to a large extent, they have. NASA and DoD have left no stone unturned in evaluating their respective tragic errors and taking lessons learned, to improve safety and precautions against future problems. But, as AI gets smarter and "deep learning" enhances AI capacity, these technologies will become more complex, faster, and more difficult for humans to control. Testing and evaluation are considered the key to limiting possible errors, but become increasingly difficult as autonomous systems become faster and more complex. The growing complexity, speed, and self-direction of AI, software, and algorithms make it ever more difficult for humans to understand what autonomous systems are doing, how they do it, and, thus, how to prevent or control errors.

Autonomous Cyber Warfare

The cyber realm, both cyber offense and defense, is another area where AI-powered autonomous systems are looming, and are likely game changers. Think of the well-known twenty-first-century cyber disruptions: a Stuxnet with complex, precise programming, wreaking havoc on Iran's nuclear program; Chinese intellectual-property theft from US firms; Iran hacking into tens of thousands of Saudi computers; the Russian cyber-hacked denial of service to the entire nation of Estonia; cyber hackers compromising data from five hundred million Marriot hotel-chain accounts; and a data breach at the US Office of Personnel Management (OPM) compromising more than four million US government employees. Then consider that these events occurred *without* AI-powered autonomous malware.

It must be recalled that anything in the digital universe that can be communicated with is vulnerable to being hacked. The risks of autonomous malicious software that can spread, replicate and update itself, and adapt and respond to cyber defenses are among the growing risks that AI brings to cybersecurity. As a report by a leading cybersecurity firm explained, "Weaponized AI will be able to adapt to the environment it infects. By learning from the contextual information, it will specifically target weak points it discovers or mimic trusted elements of the system. This will allow AI cyberattacks to evade detection and maximize the damage they cause."[60] With the deployment of 5G and a world of billions upon billions of IoT-connected devices, the potential risks increase exponentially. An F-16 jet, for example, has thousands of sensors. The US Department of Defense and intelligence community have thousands of separate computer networks. Similarly, many major corporations also have a multiplicity of computer networks.

Fortunately, AI's impact on cybersecurity is a two-way street, enabling both cyber offense and defense. To date, cyber offense, with a low bar of entry (basically a laptop and easily obtained hacking programs) has been cheaper, easier, and more effective than defense. Big data have helped improve attribution of cyberattacks and made "active defenses" or counterattacks an option for both governments and businesses. But, there are indications that AI may be a great equalizer, shifting the balance toward defense. Obviously, it would be a near impossibility for human manpower to respond in real time to such a scale and scope of cyberthreats.

Thus, cybersecurity is an area where automaticity, with humans out of the loop, is not necessarily a bad thing; in many respects, it is essential. Autonomous cyber defense is a growing field, pursued with great urgency. For example, part of the Defense Advanced Research Projects Agency (DARPA) $2-billion-plus AI R&D includes several programs, and cyber challenges create highly advanced algorithms that can stay one step ahead of high-tech hackers.

Already, DARPA cyber challenges have stimulated some remarkable AI autonomous defenses. One new AI-enabled program called Cyber-Hunting at Scale (CHASE) uses sophisticated algorithms and advanced processing speed to track huge volumes of data and find advanced attacks hidden within incoming data.[61] Another such system "is fully autonomous for finding and fixing security vulnerabilities," not just identifying vulnerabilities but applying "patches" to fix them, even reasoning which patch and when to apply it. The next wave of autonomous defense is "counter-autonomy," which not only exploits flaws in malware, but finds vulnerabilities in offensive algorithms and attacks them. This could mean offensive and defensive autonomous systems battling each other.[62] The implications of AI-powered cyber defenses for the battlefield are a new factor still being intellectually digested.

60 Dan Patterson, "How Weaponized AI Creates a New Breed of Cyber-Attacks," *TechRepublic*, August 16, 2018, https://www.techrepublic.com/article/how-weaponized-ai-creates-a-new-breed-of-cyber-attacks/.

61 Kris Osborn, "DARPA Prototypes New AI-Enabled 'Breakthrough' Cyberattack 'Hunting' Technology," *Warrior Maven*, August 6, 2018, https://defensemaven.io/warriormaven/cyber/warrior-maven-video-report-above-ai-enhanced-cybersecurity-by-kris-osborn-warrior-keGKSGeaX0i16H4oNEo06Q.

62 Scharre, *Army of None*.

New Challenges to Strategic Stability: Hypersonic and Counter-Space

But, AI-enabled cyber offense and defense are not the only new factors complicating strategic stability. Another is the development of highly maneuverable hypersonic space vehicles and cruise missiles, traveling at Mach 5 or faster, that can evade missile-defense systems and conceal their targets. While they are dual use (and have potential for commercial air travel) the focus of nations developing the technology is on military use. The United States, China, and Russia are leading the race, with India and France also pursuing the difficult technology, while other nations are also at early stages of development. Deployment is projected in the early to mid-2020s. There are two main types of hypersonic vehicles under development: hypersonic glide vehicles (HGVs), which are launched by rockets at the edge of space and glide in the outer atmosphere; and hypersonic cruise missiles, which are rocket-powered, faster versions of current cruise missiles.[63] They appear intended as kinetic weapons with their speed and force of impact hitting a target, rather than delivering warheads.

Some argue that they are inherently destabilizing to nuclear-weapons states, as there is little warning time and a risk of decapitating command and control, thus threatening the assured second-strike capability on which deterrence is based. This could result in a "launch on warning," use-it-or-lose-it scenario in an escalating conflict. While efforts to develop "counter-hypersonic" weapons by the United States, if not China, are under way, the difficulty cannot be overstated: if missile defenses are trying to "hit a bullet with a bullet," imagine trying to do that at five or six times the speed of sound.[64] That this hypersonic race is unfolding as US-Russia strategic arms control appears to be unraveling suggests arms control to ban and/or limit exports will be particularly problematic.

Space

Yet another growing concern with regard to strategic stability is the increasingly crowded and contested domain of space, upon which daily modern communications (TV, Internet), navigation (GPS), military command and control, surveillance, reconnaissance, and intelligence are greatly dependent. Once the sole province of the United States and the Soviet Union, there are a proliferation of space powers, and of counter-space activities—actions to jam, deny, disable, or destroy low- and medium-orbiting and geosynchronous satellites. As of April 2020, there were 2666 satellites in orbit, increasingly more commercial than military satellites. Just under half belong to the United States. Russia and China account for five hundred and thirty-two, with China the fastest-growing space power.[65] EU nations, India, (which launched one hundred and four small satellites from a single rocket in 2017), and Japan are also major actors in the space environment, though new challengers including North Korea and Iran are part of the landscape. Space is decreasingly monopolized by governments, as commercial space activities—including satellite launches, asteroid mining, and space tourism—are rapidly growing.

Against this backdrop, space has become a geostrategic contested domain, one increasingly reflecting major-power competition. A number of nations have developed, or are pursuing, a range of both land- and space-based counter-space technologies. The United States is particularly concerned about Russian and Chinese capabilities, which a recent Defense Intelligence Agency report says, "are developing jamming and cyberspace capabilities, directed energy weapons, on-orbit capabilities and ground-based antisatellite weapons."[66] Most dramatically, in 2007, a Chinese "hit-to-kill" missile blew up its own low-orbiting satellite, creating thousands of bits of potentially dangerous space debris. India recently demonstrated that anti-space prowess, similarly destroying one of its satellites (creating some four hundred pieces of space debris), highlighting that space power is shifting from West to East.[67] More recently, there are reports that the United States and Russia have been conducting risky close-approach missions called "remote proximity operations," maneuvering their respective satellites near each other, which could be used for intelligence gathering or counter-space operations.[68]

---

63 Richard H. Speier, et al., *Hypersonic Missile Nonproliferation, RAND*, 2017, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2100/RR2137/RAND_RR2137.pdf.

64 Michael Peck, "DARPA Builds Advanced Interceptor Weapon to Destroy Hypersonic Missile," *Warrior Maven*, January 17, 2019, https://defensemaven.io/warriormaven/future-weapons/darpa-builds-advanced-interceptor-weapon-to-destroy-hypersonic-missile-attacks-JX0SYE3fCkixsCs7UBr96A/.

65 "UCS Satellite Database," Union of Concerned Scientists, updated April 1, 2020, https://www.ucsusa.org/resources/satellite-database.

66 "Challenges to Security in Space," Defense Intelligence Agency, January 2019, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

67 Ankit Panda, "India Can Blow Up Satellites Now. And a New Space Arms Race Could Be Starting," *Washington Post*, April 1, 2019, https://www.washingtonpost.com/outlook/2019/04/01/india-can-blow-up-satellites-now-new-space-arms-race-could-be-starting/?utm_term=.92356ef2b185.

68 Theresa Hitchens, "The Stellar Dance: US, Russia Satellites Make Potentially Risky Close Approaches," *Breaking Defense*, April 10, 2019, https://breakingdefense.com/2019/04/the-stellar-dance-us-russia-satellites-make-potentially-risky-close-approaches/.

There are a variety of counterspace systems and technologies, some ground based and orbital-space based. Ground-based antisatellite missiles (ASAT), which can also be air launched, use an onboard seeker to locate and kinetically destroy or disable satellites, though not by using directed-energy weapons (DEW) such as lasers, high-powered microwaves, or other radio-frequency weapons. Unlike ASAT, DEW attacks may only temporarily disable satellite functions. Electronic warfare is another type of anti-space weapon, applying jamming or spoofing (sending a fake signal with false information). In addition, there are a number of threats from orbital (space-based systems) that can do temporary or permanent damage to satellites—including radio-frequency or microwave jamming, chemical sprays, robotic arms to disable devices, and kinetic-kill vehicles.[69]

While space has tended to be viewed as an offense-dominant domain, some argue that there are a number of countermeasures, including a trend toward small microsatellites, that offer defense some advantages. These include using multiple frequencies, using multiple military and commercial satellites (whose signals can be intermingled) for certain missions to create redundancy, and using hundreds of tiny microsatellites for single-purpose functions with some redundancy.[70]

Regardless, outer space is a critical, if vulnerable, global commons—one on which all nations rely, to varying degrees, for the daily function of their economies, societies, and militaries. Such mutual vulnerability would suggest considerable overlapping interest in ensuring the domain's peaceful use. Yet, there is a woeful dearth of international cooperation, rules, and norms—despite mutual vulnerabilities and common interests like mitigating space debris—and governance institutions are largely outdated.

II. THE GOVERNANCE CONUNDRUM

One large question casting a shadow over the future of global governance, writ large, is how to overcome the steady unraveling of existing economic and political institutions and agreements. Not only are longstanding economic and political institutions fraying, but the resurgence of major-power geopolitical competition is threatening accords underpinning strategic stability. The current undoing of the Intermediate-Range Nuclear Forces (INF) Treaty, US threats to withdraw from the Open Skies Treaty, and the uncertain fate of the New Strategic Arms Reduction Treaty (START) US-Russia agreement, which expires in 2021, are cases in point. These geopolitical dynamics make the urgency of establishing new norms, standards, and codes of conduct for emerging, game-changing technologies ever more problematic.

Another underappreciated factor is the technological imperative: human history suggests if a technology is created, it will be used—and with military applications, it will be deployed, often with unintended consequences. Often, only after catastrophic results—such as poison gas in WWI or the atomic bomb in WWII—do nations agree to ban their use.

The risks and glaring inadequacy of rules and norms with regard to outer space is emblematic of the troubling global-governance deficit amidst a surfeit of emerging disruptive technologies. How to create norms, rules, and codes of conduct (or decide limits or bans on use) for what, in many cases, may be game-changing technologies—many of them dual use—is filled with more questions than answers. In too many areas of technology, as with space, there is not even a definition of what constitutes an act of war or a violation of national sovereignty. What is the threshold for acts of war or violations of sovereignty with regard to space? Is it jamming temporarily, disrupting, or physically destroying a satellite? Then there is the whole question of the role of robots and drones. Given the increasingly ubiquitous use of military drones—and the low bar of inexpensive drones for non-state actors—what are the rules for warfare? What, if any, are battlefield rules for robots, or techno-enhanced human super soldiers? What accountability or constraints are there for accidental destruction or civilian deaths by semiautonomous or autonomous weapons? Moreover, there is no dearth of difficult ethical questions with regard not just to autonomous weapons, but to AI and biotech in general. What are the limits on synthetic biology, and techniques like CRISPR to alter or create life?

69 "Challenges to Security in Space," Defense Intelligence Agency.

70 Maj. Bradley Townsend, "Space: An Offense-Dominant Environment?" *Purview,* December 26, 2018, https://purview.dodlive.mil/2018/12/26/space-an-offense-dominant-environment/.

Cyber-Commons Governance

Look no further than the engine and foundation of all electronic communications, the beleaguered Internet, for an anomalous example of minimalist and *ad hoc* governance that may be applicable to space: both are global commons created by technology. The Internet has been managed by a quasi-governmental Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit corporation and multi-stakeholder entity governed by an international board. It has exercised responsibility for allocating Internet Protocol (IP) address space, protocol identifiers, generic and country codes, domain names, and root-server system functions—in short, the stable operation of the Internet. It has global regulatory authority, despite no treaty defining its jurisdiction.

But, ICANN has no capacity to address the multifarious uses and malign abuses in the cyber domain, which its creators never imagined, and which remain both undefined and unaddressed. What constitutes cybercrime or cyber war, particularly in a global commons that largely resides in the private sector? There are no commonly accepted standards. Cybertheft or cyber ransom may be considered a crime. What of cyber industrial theft or cyber-intelligence hacking? Does hacking to deny service temporarily constitute a crime or an act of war; does government-sponsored theft of defense industrial intellectual property qualify? How about disabling an electric grid? Or, does an act of cyber disruption or damage have to physically destroy property and/or kill or injure human beings to qualify as an act of war? Does a cyberattack on a NATO country or Japan trigger NATO Article 5 with regard to the United States?

Cybersecurity threats are only one of the pressing governance concerns in the area of digital commerce. Though e-commerce is already a major component—and the fastest-growing one—of global trade, there are only partial and incomplete rules, varying from one regional or bilateral trade accord to the other, and an increasing risk of fragmented digital regimes. Moreover, the overarching governance of use of data, sharing and/or commercialization of private content, storage of data, and where to draw the line on privacy—in the face of the explosion of social media with a widening variety of nefarious, sometimes lethal, consequences—all lack any globally agreed norms or minimal standards.

The digital economy, now a mature technological sector, is a prime example of how even established technologies can race well ahead of governance. By some estimates, global data flows grew forty-five times from 2005 to 2014, exponentially faster than flows in trade or finance.[71] The US Department of Commerce found that in 2014, more than half of US trade in services was digitally delivered, and a Japanese METI report assesses that 50–56 percent of all trade in services is ICT enabled.[72] Digital commerce already accounts for roughly 20 percent of global trade, and is projected to increase to 25 percent by 2025.[73] This percentage of total trade is likely to accelerate by an order of magnitude over the coming decade. Consider the explosion of e-payments, the downloading of music, games, and books, the billions of devices to be connected by the IoT, or the impact of 3D printing, where computer designs will be widely downloaded and actual products will be produced by consumers.[74] Internet traffic continues to advance rapidly, with 2019 traffic projected to be sixty-four times its 2005 volume.[75]

Yet, the world lacks a comprehensive international framework of trade rules governing digital commerce. World Trade Organization (WTO) agreements covering services (financial, legal, etc.) and various remedies on intellectual-property rights (e.g., trademarks, copyrights, and legal protections and remedies in the digital environment) offer only a partial framework.[76] There are numerous gaps in digital governance, as well as new challenges from evolving technologies, such as the growth of the cloud and cloud-based AI services. In an effort to forge a comprehensive framework for e-commerce, seventy-six WTO members (including the US, EU, China and Japan) formed a Working Group in 2019 to negotiate a full set of rules and standards, though little progress is apparent as of mid-2020.[77] At the same time, digital protectionism (e.g., localization of data requirements, restricting data flows, and cloud ownership) is rising while the Internet is becoming

71 Rachel Fefer, Shayerah Akhtar, and Wayne Morrison, "Digital Trade and US Trade Policy," Congressional Research Service, June 6, 2017, summary page, https://fas.org/sgp/crs/misc/R44565.pdf; Manyika et al., *Unlocking the Potential of the Internet of Things*.

72 Hosuk Lee-Makiyama, "Expanding Digital Protectionism & Impact on Business," European Centre for International Political Economy, 2017, http://ecipe.org/app/uploads/2017/07/ECIPE-for-METI-JETRO-3.pdf.

73 Manyika et al., *Unlocking the Potential of the Internet of Things*. See also J. Clement, "Retail E-commerce Sales in the United States from 2017 to 2024 (in million US dollars)," Statistica, March 19, 2020, https://www.statista.com/statistics/272391/us-retail-e-commerce-sales-forecast/.

74 Fefer, Akhtar, and Morrison, "Digital Trade and US Trade Policy," 5–7. See also Manyika et al., *Unlocking the Potential of the Internet of Things*.

75 "CISCO Annual Internet Report," CISCO, https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html#~complete-forecast.

76 Fefer, Akhtar, and Morrison, "Digital Trade and US Trade Policy," 13.

77 Leika Kihara, "China and U.S. Among 76 WTO Members Pushing for New E-Commerce Rules," Reuters, January 25, 2019, https://www.reuters.com/article/us-davos-meeting-ecommerce/china-and-u-s-among-76-wto-members-pushing-for-new-e-commerce-rules-idUSKCN1PJ0UK.

fragmented. Digital commerce depends on open and transparent global commercial, scientific, and academic data flows. The EU's General Data Protection Regulation (GDPR), implemented in 2018, is an important effort to create a global standard for safeguarding privacy without curbing commerce. Unfortunately, the three key global actors—the United States, EU, and China—appear to be evolving into separate, and not entirely compatible, digital regimes. China, Russia, and some other countries claim a doctrine of so-called "Internet sovereignty," apparently forgetting why it is called the World Wide Web. This Balkanization imperils the future of digital commerce, and hence, global trade. There is ample room for national differences with regard to personal privacy, but some minimal baseline standards and norms are needed.

The United States and the EU differ over many tech issues, as the EU has moved ahead in developing standards and rules, while the United States is only now beginning to develop a comprehensive national framework, and has only a mix of national and state laws and regulations. China, the third digital superpower, is adopting policies and restrictions at odds with the other two. In the case of China, its "Great Firewall" is getting higher, imposing web censorship within the country and restricting the web presence of US tech firms—Google and Facebook, among them.[78] Such treatment has meant that Amazon has only 1.3 percent of China's e-commerce, and is unable to appeal to Chinese consumers and compete with the dominant Alibaba and JD.com.[79]

In its national trade estimate, the Office of the US Trade Representative (USTR) highlights some of China's barriers to digital trade, citing data-localization requirements (forcing firms to keep data in the country of operations) and local computer-facilities requirements, restrictions on data flows, restrictions on the use of secure lines and networks, restrictions on foreign direct investment (FDI) in cloud-computing services, and "extensive blocking" of Internet content. Nevertheless, China is not alone. USTR's 2019 trade estimate cites data localization, limits of business data transfer, requirements and Internet-content restrictions in India, data localization and restrictions on Internet-services investment and tariffs in Indonesia, and data localization and data flows in Vietnam and multiple other countries.[80]

There is a compelling need to, at the least, minimize real or potential negative consequences of this discordant situation to make compatible the digital regimes of these three key actors with regard to e-commerce. This is a critical foundation (as the Trans-Pacific Partnership (TPP) tried to establish, and as WTO talks on digital rules are seeking to), without which global digital norms and already rapidly growing digital commerce—soon to expand exponentially with the launch of 5G, IoT, and AI—will risk Balkanization.

Trade is only part of a digital platform that is deeply troubled. The weaponization and exploitation of social media is an increasingly insidious global problem: it is where e-commerce, privacy, and malicious political and social activism all intersect. Social media like Facebook, Instagram, and WhatsApp are ubiquitous, a product of "Big Tech," with nearly three billion users worldwide.[81] Social media have increasingly become the dark side of AI and the digital era, where bots and Internet trolls are used to recruit jihadi terrorists, where "deep fakes" of audio and visual material misrepresent real people to inject false information and influence elections, where white nationalists network, drugs sales are facilitated, and arms are trafficked, among other nefarious activities.

Technologies such as blockchain may be important enablers to both cybersecurity and what is called "fintech," a digitizing of the financial sector, also enabling the rise of cryptocurrencies like Bitcoin. A blockchain is a time-stamped transaction or block of data shared across a network of computers. Each block must be verified and accepted by all others, and all are bound together. Once a record has been added to the chain, it cannot be changed internally, limiting the possibilities of hacking to entry and exit from the blockchain. It is increasingly being deployed by both major financial institutions and burgeoning cryptocurrencies.

The EU's GDPR privacy standards have become widely accepted by global tech firms doing business in the EU, and have shaped the privacy debate worldwide. Scams such as Internet bots and trolls using false IDs to manipulate social media to influence foreign elections, gather personal data for commercial or political use, or recruit terrorists, have put

78 Alan Beattie, "Data Protectionism: The Growing Menace to Global Business," *Financial Times*, May 13, 2018, https://www.ft.com/content/6f0f41e4-47de-11e8-8ee8-cae73aab7ccb.

79 Daniel Keyes, "Amazon is Struggling to Find its Place in China," *Business Insider UK*, August 30, 2017, http://uk.businessinsider.com/amazon-is-struggling-to-find-its-place-china-2017-8?r=US&IR=T.

80 "Fact Sheet on 2019 National Trade Estimate," Office of the United States Trade Representative, March 2019, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2019/march/fact-sheet-2019-national-trade-estimate.

81 "Number of Social Network Users Worldwide from 2010 to 2023," Statista, https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.

pressure on tech firms such as Facebook and Twitter to institute more effective safeguards to block such fraud. Pressure from governments on tech firms, including legal action or financial penalties, is also beginning to force more accountability. But, this problem underscores the need for established adequate minimum standards for privacy, and appropriate penalties for both non-state actors and governments that support or tolerate them.

The social media problem is part of a larger Big Tech issue with regard to data, which is the raw material of the entire knowledge economy and, as the digital and physical economies become more deeply intertwined, the world economy writ large. This gets to the overarching question of the regulation of Big Tech. A handful of US (Facebook, Google, Apple, Amazon, Microsoft) and Chinese (Alibaba, Baidu, Tencent, JD.Com) firms dominate global technology. The world's nearly four billion Internet users conduct more than 3.2 billion Google searches each day, and, as mentioned, Facebook has more than one billion users worldwide.[82] Who should determine the ownership, use, or sharing of data, whether it should be taxed, and whether monopoly practices are distorting innovation? Multibillion-euro EU fines against Google and other firms for their manipulation and exploitation of data have begun to shape behavior. The US Congress is scrutinizing Big Tech with regard to national privacy laws. And, there is a growing antitrust mindset in both the United States and EU, with a recent unilateral digital tax imposed by France. This is a good example of the need for a common approach to regulating Big Tech; it is imperative that these policy issues be addressed by both nations and international organizations. The Group of Twenty (G20) would be an appropriate venue to develop policy consensus and norms on the weaponization of social media.

Finally, with regard to the question of cybersecurity, the line between cyber hacking for economic benefit or damage, and for political purposes (e.g., the denial of service to Estonia) and cyber war can be blurred. The former can be addressed through national or international opprobrium (e.g., national or UN sanctions) and/or global agreements on norms and standards. But, actions with politico-military consequences—such as disabling a power grid or communications system, or altering or disabling a satellite's functions—require new rules of war. Such a regime might begin with efforts to find consensus among major powers, but should evolve to a Geneva Convention-type regime. If history is a guide, it may take a catastrophic event before a cyber truce or deterrence based on mutual vulnerability is reached.

Bioscience/Security Governance

The biology revolution that exploded following the discovery of recombinant DNA in the 1970s has, as discussed above, yielded enormous benefits for the human race, but also enormous, unprecedented risks. Cloning, mixing species (as with the Chinese experiment with monkeys), GMO food, and bioweapons all raise ethical, economic, human, and national security governance questions that are far from adequately addressed. How will an edited gene interact with the entire genome? How unlikely are unintended consequences? The set of risks, from both state and non-state actors, only grows when factoring in the possibilities of ordering AI-designed DNA with one or two clicks on a laptop.

That said, there is a long list of international regimes and institutions, some with near-universal adherence—such as the World Health Organization (WHO), the Biological Weapons Convention (BWC), and UN Security Council Resolution 1540—that have governed health standards and biosecurity. While the WHO sets global standards for health practices and norms, the BWC and UNSC 1540, respectively, ban the use of biological weapons and impose binding regulations on all states to prevent the proliferation of nuclear, chemical, and biological weapons and their means of delivery, and to create controls to prevent their illicit trafficking (e.g., to non-state actors) and means of delivery. There are other regimes such as the Australia Group, an informal grouping designed to harmonize export controls, or the Convention on Biological Diversity, with more limited adherents. Yet, none has fully caught up with regard to governance of still-emerging biotechnology. Biotech has been mainly self-regulated since the discovery of recombinant DNA and the Asilomar Conference in 1975, the initial effort by the bioscience community to forge a consensus on ethics and standards.[83]

It is a hopeful measure of ethical consensus that the Chinese Society for Cell Biology issued an outraged denunciation of the recent gene-editing action by the Chinese scientist, a watershed event. Partly in response, the WHO created an eighteen-member committee of scientific experts to establish guidelines for scientists editing genes and to address the

82 "How Many Google Searches Per Day?" Ardor SEO, https://ardorseo.com/blog/how-many-google-searches-per-day-2019/.

83 Paul Berg, et al., "Summary Statement of the Asilomar Conference on Recombinant DNA Molecules," Proceedings of the National Academy of Sciences of the United States of America," June 1975, https://authors.library.caltech.edu/11971/1/BERpnas75.pdf.

"scientific, ethical, social and legal challenges" associated with gene editing.[84]

But, CRISPR and synthetic biology have so lowered the bar of entry, particularly when combined with AI, that the temptation to play God and tamper with life itself becomes a more chilling possibility. Not least, the lowered bar of biotech greatly increases the risk of non-state actors abusing the technology to manufacture yet-unknown bioweapons. The US Centers for Disease Control (CDC) list of dangerous biologic agents may be inadequate to protect against yet-uncategorized or unknown pathogens that emerging biotech could create. There needs to be a stronger global consensus for establishing and enforcing ethics and constraints on gene editing and applications of synthetic biology. Building on WHO ethical standards, dialogue among the five permanent members of the UN Security Council (UNSC) to achieve consensus is one logical place to start. Building on that to the whole UNSC and among major regional organizations—the OECD, African Union, Arab League, and East Asia Summit—with the goal of a strengthened, enforceable, and global regime.

One important biotech problem that has less to do with science and more with pop psychology and politics is GMO foods. Although GMO crops, particularly soybeans, maize, and cotton are in wide use in the United States, and increasingly in China, India, and Brazil, their use is constrained globally—most notably, by the EU. While GMO maize and potatoes have been accepted by the EU, many EU nations ban them. The overwhelming body of research shows no evidence that GMO crops are unsafe. Yet, the EU curbs their use under its "pre-cautionary principle." A bit like requiring proof of a negative, this principle holds that because something could be unsafe, it should be treated as such. Anti-science activists in the United States have similar views, demanding GMO foods be labeled as such. Yet, GMO crops can be modified to use less water, less or no fertilizer, be immune to diseases, and produce bigger yields. There is agreement that GMO crops need thorough testing before being deployed. But, on a warming planet with a growing population, they hold great potential to feed billions. Major markets like China and India have approved GMOs. African nations, whose major market is the EU, have been forced to limit GMO use or risk losing their major export markets. A new US-EU understanding on GMOs, perhaps within the context of a bilateral trade agreement, might open new possibilities.

Rethinking the Space Domain

Space is a tech-generated global common, one synergistic with and dependent on the cyber domain, whose governance deficit has expanded as the policy landscape has changed dramatically and as emerging technologies have exponentially complicated its risks and challenges. As the Internet is an essential component of the space infrastructure, the US military sees it operationally as a combined cyberspace domain.[85] The one foundational treaty to which all major space powers belong is the Outer Space Treaty, which entered into force in 1967 but is increasingly antiquated. The treaty institutionalized the exploration and use of space as "the province of mankind," banning sovereignty claims over space or celestial bodies and the deployment of nuclear weapons in space or celestial bodies.

But, the UN treaty offers little guidance on collisions, the growing problem of space debris, or intrusion or obstruction of a nation's space assets, and lacks any dispute-settlement mechanism.[86] In an age when commercialization of space is a growing industry, the Outer Space Treaty and a number of secondary treaties, which do not include the major space powers, have clearly been overtaken by new realities. Nor, despite some nascent UN diplomatic efforts, have any rules, codes of conduct, or constraints on space-related weaponry been the subject of binding agreement by major space powers. The United States declares its goal to be "space dominance," hinting at one reason arms control in outer space remains elusive, despite the increasingly mutual strategic vulnerabilities of all major powers.

There are some additional legal agreements in effect under a somewhat obscure UN Office for Outer Space: liability for damage caused by space objects, safety and rescue of spacecraft and astronauts, and registration of space activities.[87] Similarly, the International Telecommunications Union is key in managing the placement of geostationary orbiting satellites and their operations. Perhaps the most interesting instrument

84 Preetika Rana, "WHO Reacts to Chinese Gene-Edited Twins with Plans for Global Guidelines," *Wall Street Journal*, February 21, 2019, https://www.wsj.com/articles/who-reacts-to-chinese-gene-edited-twins-with-plan-for-global-guidelines-11550736189?mod=searchresults&page=1&pos=1; Lander, et al., "Adopt a Moratorium on Heritable Genome Editing."

85 Larry Martinez, "Is There Space for the UN? Trends in Outer Space and Cyberspace Regime Evolution," European Science Policy Institute, January 2012, https://www.files.ethz.ch/isn/136422/ESPI_Perspectives_56.pdf.

86 Stewart Patrick and Kyle L. Evanoff, "The Right Way to Achieve Security in Space," *Foreign Affairs*, September 17, 2018, https://www.foreignaffairs.com/articles/space/2018-09-17/right-way-achieve-security-space.

87 "Space Law Treaties and Principles," United Nations Office for Outer Space Affairs," http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties.html.

for active cooperation in space in the post-Cold War era, with potential relevance to future space governance, is the 1998 US agreement with European nations, Russia, and Japan for civil cooperation on the International Space Station.[88] It is one of the few remaining cooperative US-Russian activities. And, it is measure of the challenge of space governance that it is difficult to conceive of such an agreement being replicated in the current, post-Crimea geopolitical environment. Nonetheless, quaint as it may now seem amid unrestrained geopolitical competition, the International Space Station agreement may, over time, become an important precedent for global cooperation in space.

As discussed above, there are a host of space-related areas where technology-enabled activities, both commercial and military, are overtaking the current bounds of governance and may soon make outer space less of a global common and more of a new frontier to which actors stake claims and extend conflicts. Private-sector commercial activities in space are a relatively new phenomenon. Companies like Elon Musk's SpaceX and Virgin Galactic that offer commercial launch services, space tourism, and even colonization of Mars, and a growing number of international firms like Deep Space Industries and Planetary Resources that seek to mine asteroids, are creatures of the twenty-first century.

But, some of these planned activities appear to violate the 1967 Outer Space Treaty. For example, a 2015 law passed by the US Congress to support commercial activities in space claims to establish property rights for extraterrestrial resources, though the 1967 treaty explicitly bans sovereignty claims in space or celestial bodies.[89] Add to that major space powers like the United States and China planning to establish Moon bases and human colonization of Mars, and scenarios extending tech-enabled, unrestrained, nineteenth-century-type imperial great-power competition into the cosmos appear possible, if not likely.

The need to craft new legal and/or *ad hoc* arrangements, codes of conduct, and understandings to govern space activities is compelling. While the United States has the majority of commercial and government satellites in orbit, Russia and China have greatly increased their space presence over the past two decades.[90] Thus, there is a growing shared dependency and vulnerability among the United States, China, and Russia on space assets for economic and military needs. Yet, despite numerous shared interests—managing and reducing space debris, sharing scientific information, sustaining space assets, and baseline coordination among national space agencies—cooperation is wanting. Moreover, there are ample precedents and models to inspire new conventions or accords. With regard to resource exploitation in the commons, the UN Law of the Sea Treaty could be instructive. The 1998 Space Station Treaty could be a prototype for cooperative ventures. Given expensive programs to land humans on Mars, and the extraordinary difficulties of sustaining life on the red planet, such a model is worth considering.

As there are only a handful of relevant space powers (the United States, Russia, China, EU, Japan, and India), *ad hoc* agreements or codes of conduct among them, rather than a cumbersome UN framework, might be a more practical pathway to build global norms. The proposed 2014 EU Code of Conduct for Outer Space, while perhaps overly ambitious, could serve as a basis for Space Powers Dialogue.[91] The larger concern is that there appears a dearth of political will among the major powers for such patterns of cooperation. It is likely to take a crisis or catastrophe to alter the *zeitgeist* before the shared interests and vulnerabilities for safe and sustainable space activities are viewed by the major space powers as ample cause for updating rules or a code of conduct.[92]

Despite the intensifying militarization of space, efforts in the UN Committee on Disarmament for a Treaty on the Prevention of the Placement of Weapons in Outer Space have been stymied by clashing US and Russian-Chinese approaches to the issue. Both the George W. Bush and Barack Obama administrations opposed 2008 and 2014 proposed Russia-China treaties, though the United States claims, in principle, to be open to space arms control. The United States has cited a number of flaws in the treaty—most significantly, that it does not include a ban on ground-based ASAT weapons (tests of which have

88 "Space Station," US Department of State, January 29, 1998, https://www.state.gov/wp-content/uploads/2019/02/12927-Multilateral-Space-Space-Station-1.29.1998.pdf.

89 Will Gray, "Building off US Law to Create an International Registry of Extraterrestrial Mining Claims," *Space Review*, August 14, 2017, http://www.thespacereview.com/article/3304/1.

90 Johnny Wood, "The Countries with the Most Satellites in Space," World Economic Forum, March 4, 2019, https://www.weforum.org/agenda/2019/03/chart-of-the-day-the-countries-with-the-most-satellites-in-space/.

91 "Draft: International Code of Conduct for Outer Space Activities," European Union, March 31, 2014, https://eeas.europa.eu/sites/eeas/files/space_code_conduct_draft_vers_31-march-2014_en.pdf.

92 Ibid.

generated much dangerous space debris), the most prominent threat to space assets. In addition, the proposed treaty does not clearly define "space weapons," blurs the line between offensive and defensive weapons, is not verifiable, and lacks enforcement mechanisms.[93] Yet, urgent shared interests discussed above, the risks of a calamity by accident or design, and the risk of an arms race in space suggest the urgency of some rethinking among space powers. Renewed *ad hoc* dialogue based on the Outer Space Treaty—and, for discussion purposes, the proposed EU Code of Conduct—to reach some baseline rules and/or code of conduct is imperative.

AI: Preventing the Coming Storm

Developing ethical principles, standards, and norms governing the development and use of artificial intelligence is perhaps the most imperative governance challenge for the coming decade. This is underscored by four major international statements on AI governance since 2017: Asilomar AI Principals Conference (2017); the EU's 2019 Ethics Guidelines for Trustworthy AI; OECD Guidelines on AI (May 2019); and a Chinese 2018 White Paper on Artificial Intelligence Standardization.[94] Though the Asilomar AI principles are nongovernmental, they were endorsed worldwide by more than twelve hundred AI and robotics researchers and institutes, more than twenty-five hundred scientists and engineers such as Stephen Hawking, and tech entrepreneurs including Elon Musk, which suggests widespread consensus. The other efforts, while less-than-firm commitments from individual states, reflect the judgment of supranational governmental institutions (e.g., EU, OECD) and, in the case of China, governmental institutions; this can certainly shape policymakers' decision process.

While there are different points of emphasis, and varying degrees of elaboration and detail, there appears substantial overlap on essential ethics and principles. This amalgam, based on all four efforts, captures core principles.

- ***Human agency and benefit:*** Research and deployment of AI should augment human well-being and autonomy; have human oversight to choose how and whether to delegate decisions to AI systems; be sustainable, environmentally friendly, and compatible with human values and dignity.
- ***Safety and responsibility:*** AI systems should be: technically robust; based on agreed standards; verifiably safe, including resilience to attack and security, reliability, and reproducibility. Designers and builders of advanced AI systems bear responsibility and accountability for their applications.
- ***Transparency in failure:*** If an AI system fails, causes harm, or otherwise malfunctions, it should be explainable why and how the AI made its decision; that is, algorithmic accountability.
- ***Privacy and data-governance liberty:*** People should have the right to access, manage, and control the data they generate; AI applied to personal data must not unreasonably curtail an individual's liberty.
- ***Avoiding arms races:*** An arms race in lethal autonomous weapons should be avoided. Decisions on lethal use of force should be human in origin.
- ***Periodic review:*** Ethics and principles should be periodically reviewed to reflect new technological developments, particularly those involving deep learning and general AI.

How such ethics are translated into operational social, economic, legal, and national security policies—and enforced—is an entirely different question. These ethical issues already confront business and government decision-makers. Yet, none have demonstrated any clear policy decisions or implemented them, suggesting that establishing governance is likely an incremental, trial-and-error process.[95] How to decide standards and liability for autonomous vehicles, data privacy, and algorithmic accountability is almost certainly difficult. Moreover, as AI becomes smarter, the ability of humans to understand how AI makes decisions is likely to diminish. One first step would be for a representative global forum like the G20 to reach consensus on principles, and then move to codify them in a UN Security Council resolution, or through other international governance institutions such as the International Monetary Fund, World Bank, International Telecommunication Union, or WTO.

---

93 Jeff Foust, "U.S. Dismisses Space Weapons Treaty Proposal as 'Fundamentally Flawed,'" *Space News*, September 11, 2014, https://spacenews.com/41842us-dismisses-space-weapons-treaty-proposal-as-fundamentally-flawed/.

94 "Asilomar AI Principles," Future of Life Institute, https://futureoflife.org/ai-principles; "Ethics Guidelines for Trustworthy AI," European Commission, https://ec.europa.eu/futurium/en/ai-alliance-consultation; "OECD Moves Forward on Developing Guidelines for Artificial Intelligence (AI)," Organisation for Economic Co-operation and Development, http://www.oecd.org/going-digital/ai/oecd-moves-forward-on-developing-guidelines-for-artificial-intelligence.htm; Jeffrey Ding and Paul Triolo, "Translation: Excerpts from China's 'White Paper on Artificial Intelligence Standardization,'" New America, June 20, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-excerpts-chinas-white-paper-artificial-intelligence-standardization/.

95 Madhunita Murgia and Siddarth Shrikanth, "How Big Tech is Struggling with the Ethics of AI," *Financial Times*, April 28, 2019, https://www.ft.com/content/a3328ce4-60ef-11e9-b285-3acd5d43599e.

An issue of social concern writ large, and a test of ethics, is automaticity of AI predictive judgment. In areas such as job applications, judicial sentencing, prison parole, or even medical assessment, AI's lack of context, situational meaning, consideration of changes in human mindsets and character, and, not least, system flaws, argue for AI as a tool to augment human decisions, rather than to serve as an autonomous decision-maker.

One compelling shared interest is AI safety and standards. An important lesson from the evolution of first digital generation is that failing to build in safety and cybersecurity on the front end tends to make it far more difficult to adapt on the back end. This argues for global threshold AI standards for safety and reliability, as well as efforts by all governments to prioritize investment in R&D for that purpose. AI safety is somewhat analogous to the issue of failsafe command and control of nuclear weapons, and the need for secure "second-strike" capability as the basis of deterrence: cooperation, even with adversaries, can be warranted to minimize the risk of accidents. This is particularly true as the bar to entry for AI—with a large body of open-source research, and its dual-use nature—is far lower (and more difficult to anticipate, as it is still an immature technology) for small and medium powers than that of nuclear weapons.

Autonomous Weapons and the Future of Strategic Stability

The impact of the technologies discussed here on national security, the strategic balance, and the future conduct of war has already begun to undermine longstanding assumptions about crisis stability. The deployment already of near-autonomous systems underscores that AI governance of emerging autonomous weapons is one of several emerging technologies adding new factors to the calculus of strategic stability that policymakers must consider. Some fear technology may challenge already-beleaguered international humanitarian law, codified the Hague and Geneva Conventions. The former's "Martens Clause" says that new weapons must comply with "the principles of humanity," while Article 36 of the latter calls for legal reviews of new means of warfare.[96] US officials stress that their development and use of AI will be consistent with such humanitarian practices.[97]

The UN CCW's inability to reach consensus on even a definition of autonomous weapons since 2014 is a measure of the problem's complexity. As discussed above, there are degrees of autonomy and levels of human control or supervision, which, depending on the situation, some might see as autonomous, but others might not. The differences are in software and algorithms, not hardware. Semiautonomous weapons programmed to defend a ship (with autonomous and human-override modes), automatically firing at anything that attacks is one such ambiguous situation. Missiles like the HAROP, which can linger for hours, are more fully autonomous—what if the situation changes and the weapon makes a lethal decision that is flawed? Would autonomous weapons lead to escalation without human decision-making? None of the major powers, all developing cutting-edge AI, have endorsed calls to ban autonomous weapons. If one nation decides to deploy a "Terminator," could an arms race be avoided?

Though the case of autonomous weapons includes unique questions of control and responsibility, there are parallels with the ethics of nuclear weapons; this points to the limited success in banning the use of weapons technology.[98] The current powerful, normative taboo against nuclear use is a reaction to horrendous devastation demonstrated by its first use in 1945. Similarly, it is no coincidence that the spate of arms-control accords and test bans during the Cold War followed the near-catastrophe of the 1962 Cuban Missile Crisis. Other near-universal treaties codifying norms prohibiting the use of chemical and biological weapons (albeit, with less-than-perfect adherence) grew out of revulsion against poison gas use in WWI. If there is a pattern in the history of efforts to ban the use of terrible weapons (most often after first use), it is that success is uncommon, and establishing norms tends to work best when any advantage of use is outweighed by a perception of mutual vulnerability. In theory, AI should fall into that category. Autonomous weapons,

96 "Autonomous Weapons and the New Rules of War," *Economist*, January 19, 2019, https://www.economist.com/briefing/2019/01/17/autonomous-weapons-and-the-new-laws-of-war.

97 Kelsey D. Atherton, "Can the Pentagon Sell Silicon Valley on AI as Ethical War?" C4ISRNET, April 25, 2019, https://www.c4isrnet.com/unmanned/2019/04/26/can-the-pentagon-sell-silicon-valley-on-ai-as-ethical-war/.

98 Payne, "Artificial Intelligence: A Revolution in Strategic Affairs?"

however, are only one of several new technology-driven factors changing the equation of nuclear stability and, potentially, the balance of power. Crisis stability is threatened if decision-makers—due to uncertainty, miscalculation, misunderstanding, or perception of vulnerability—feel that their second-strike capability is at risk or undermined. Avoiding crisis instability is the essence of strategic equilibrium. But, unregulated emerging technologies discussed above invalidate traditional assumptions about effective deterrence and require new understandings, restraints, or counter-technologies to sustain a framework for strategic stability.

To the degree that the United States, Russia, or China operationalizes military application of AI first, or holds an advantage in hypersonic, cyber, or anti-space weapons, one of those states might have a perceived strategic advantage in conflict scenarios. Obvious examples include swarms of smart drones, disabling C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) capabilities, with laser antisatellite shots, hacking command and control, and hypersonic missiles preempting second-strike assets. Beyond 2035, quantum computing could also provide a first-mover strategic advantage of unhackable communications, navigation without requiring GPS, and other sensing capabilities.

These new technology-driven risk factors require a rethinking by major powers of what constitutes a durable framework for strategic stability. The problem is less about nuclear-arms reductions than transparency and developing new understandings and restraints to govern emerging technologies impacting crisis stability. This may include bans on autonomous weapons, hypersonic missiles, and glide vehicles, as well as a new code of conduct for space and anti-space activities, and for cybersecurity.

While some of these issues can be discussed in existing multilateral forums, a strategic dialogue—initially, among the United States, Russia, and China, and later in the process, India—is a *sine qua non* for finding a new balance of interests. The starting point would be an extension of the US-Russia New START agreement, which expires in 2021, then inviting China to a new strategic dialogue. New norms, rules, and codes of conduct with regard to all the emerging technologies impacting crisis stability appears the best, a difficult, protracted, and bumpy road to global governance. Clearly, in the present climate of distrust, avoiding the perfect storm of technology triumphing over governance will be a challenge. If history is a guide, it may take a Cuban Missile-type crisis or actual conflict to introduce new sobriety to the debate.

Regardless, the stark reality of mutual vulnerabilities among all the key actors holds out hope. Can the major powers take a deep breath, reassess enlightened self-interests, and begin to explore a balance of interests on issues of rules, norms, and institutions for managing the emerging technologies on which global stability and prosperity will turn?

Robert A. Manning is a senior fellow in the Atlantic Council's Scowcroft Center on Strategy and Security and its Foresight, Strategy and Risks Initiative. His work has included major reports on global trends, emerging technologies, global innovation, Asian economic architecture and security. He served as a senior counselor to the UnderSecretary of State for Global Affairs from 2001 to 2004, as a member of the US Department of State Policy Planning Staff from 2004 to 2008, and on the National Intelligence Council (NIC) Strategic Futures Group, 2008-2012. He was previously Director of Asian Studies at the Council on Foreign Relations.

Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org