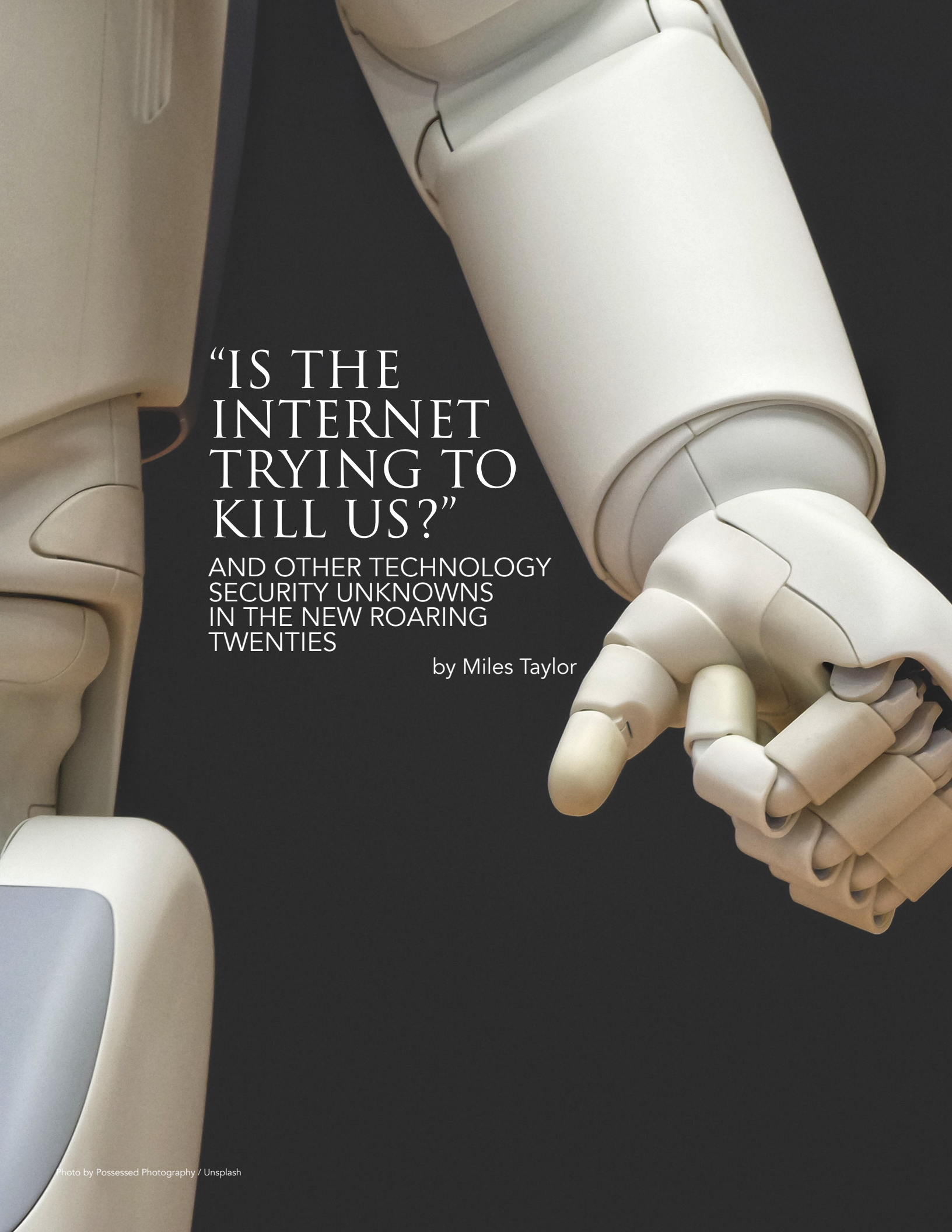


"IS THE INTERNET TRYING TO KILL US?"

AND OTHER TECHNOLOGY SECURITY UNKNOWNS IN THE NEW ROARING TWENTIES

by Miles Taylor

Photo by Possessed Photography / Unsplash

Machines are poised to transform life as we know it... and America isn't ready.

A hundred years ago, machines remade the world. Society in the 1920s was transformed by a proliferation of cars, radios, movies, and airplanes, dramatically altering the way we lived, worked, and played. We did not know it then, but the sweeping technology revolution was poised to change the way we fought, too. The 1930s saw a revolution in military affairs as warfare became deadlier and faster-paced, a foreseeable consequence of the previous decade's innovations.[278] This nevertheless caught many nations by surprise, such as those affected by the German *blitzkrieg*.

We are entering a New Roaring Twenties, and again we are unprepared for how it will affect national security in the decades to come. Make no mistake: today's innovations will be tomorrow's economic drivers, which is why we should be actively investing in the bleeding-edge tech of the future. But we must also be vigilant about how such developments will affect our security at home and reshape international conflict, or else risk a reordering of the global balance of power.

This article previews several emerging technology dilemmas, what's being done about them, and why—in some cases—it's already too late.

THE FUTURE OF THE FUTURE

The 2020s will redefine the remainder of the century. Surely this is said in every decade, as analysts stand in awe of the long-term promises of the present moment. Yet this time is different. It is not simply because emerging technologies like augmented reality and self-driving cars herald a new age of possibility (though they undoubtedly will). Rather, it is that the future *itself* will become less predictable because of the type of technologies we are fielding.

As humans, we make predictions based on knowable information, while factoring in "known unknowns"—the variables that may alter our forecasts.[279] Consider the advent of the smartphone, for instance, the worldwide adoption of which has been projected with some accuracy based on trade, social, and technology trends. These projections have only varied modestly because of known unknowns such as economic fluctuation.

But developments taking place in this decade will reduce our ability to predict the future, as we are introducing even more variables outside of human control, namely by giving agency to machines. This will increase the "unknowns" and make projections less reliable, as machines solve problems semi-independently in ways we never imagined. Consequently, the "future of the future" will become more uncertain.

By and large this will be a boon to modern civilization. We will cure diseases, discover new ways to fight poverty, and improve our environment with the help of smarter machines. There is, however, a dark side to the New

"Brave Rifles conduct counter-unmanned aerial system drill" by The U.S. Army is licensed under CC BY 2.0

Roaring Twenties. Such technology will inevitably serve nefarious ends, some unforeseeable, and we have not done nearly enough preparation for those eventualities.

UNMANNED SYSTEMS: "IT'S A BIRD! IT'S A PLANE! IT'S A KAMIKAZE DRONE?"

In August 2018, Venezuelan dictator Nicolás Maduro was delivering an outdoor address to members of the military when two small drones emerged from the sky, flying toward the crowd and detonating explosives not far from where the leader was speaking.[280] It was an apparent assassination attempt, although the weaponized devices missed their intended target. As debate erupted over who was responsible, one fact remained clear: a new era of small-drone warfare had begun.

Commercial drones are becoming ubiquitous in American life—delivering pizzas, shuttling home goods across town between families and friends, and rushing to the scenes of accidents to assist first responders. Some will be piloted, but many will be autonomous, taking off to their destinations on pre-programmed routes and adapting to conditions in the sky and on the ground, adjusting their trajectories and missions as needed.

Drone threats are about to become ubiquitous, too. The U.S. Army's "Mad Scientist Initiative" projects that swarms of small, cheap unmanned systems will "pose a significant threat" to warfighters at all levels on the future battlefield; in particular, drone *swarms* will be easy to deploy and very hard to stop.[281] The threat goes far beyond the military, though, where counter-drone defenses have been deployed, and into the heart of U.S. communities.

The good news is that new federal regulations will go into effect this year requiring drones to effectively have a "digital license plate," broadcasting their real-time location to ensure safety and prevent accidents.[282] And in 2018, Congress passed a law giving the Departments of Homeland Security and Justice the authority to take down dangerous drones over certain sensitive facilities and targets, as both agencies began worrying about drone threats from terrorists, drug cartels, and nation-state threat actors.[283] Both agencies' powers, however, are limited.

The bad news is that most American cities and towns have given little thought to how they will protect civilians in this new era, and few have the resources (or authorities) to deploy widespread drone defenses. Imagine an unmanned aerial swarm hitting a high school football game. What will a police officer on the scene do? Shoot down each autonomous kamikaze with a pistol? Off-the-shelf drones can fly upwards of 100 miles per hour carrying explosive ordinances, a threat not even John Wayne could neutralize with quick-trigger skills.

The danger posed by autonomous killing machines is a very real national security dilemma, one which is already upon us and for which federal, state, and local

authorities have not yet developed comforting solutions. Smart drone swarms, for instance, have the potential to become highly complex and adaptive, which could provide asymmetric advantage to non-state and nation-state actors in future conflicts. Indeed, these unknowns have serious geopolitical implications, which are not yet fully understood and are likely to be magnified by developments in a related technology space, advanced artificial intelligence.

ADVANCED ARTIFICIAL INTELLIGENCE: "IS THE INTERNET TRYING TO KILL US?"

Social media has deepened America's civic fault lines. While connecting people online and across borders, such platforms also exacerbate simmering political and social tensions in obvious ways every day. But what if humans weren't to blame? What if, in reality, the internet itself was conscious—and consciously stoking discord to pit humans against one another? Wouldn't that be a clever way to undermine society and soften the battlefield for a worldwide machine takeover?

This may sound like bad science fiction, but when I put the question to a leading technologist and expert on machine learning, his answer was anything but dismissive: "It's certainly possible. In fact, some experts postulate that the internet *is* already conscious, yet there isn't agreement on how, when, and if we'll know that to be true."

The country is only just beginning to grapple with the sheer magnitude of unknowns that AI will introduce, especially as the technology becomes more powerful and free-thinking.

Indeed, one of the world's leading neuroscientists who studies consciousness, Christoff Koch, has said exactly that. Asked whether the Internet is already self-aware, Koch told one interviewer, "That's possible," explaining that consciousness requires networked nerve cells and synapses.[284] "The Internet now already has a couple of billion nodes. Each node is a computer. Each one of these computers contains a couple of billion transistors, so it is in principle possible that the complexity of the Internet is such that it feels like something to be conscious [...] it might feel sad one day and happy another day, or whatever the equivalent is in Internet space."[285]

Internet consciousness is a complex area of study that has been discussed and debated, yet with advances in artificial intelligence (AI), we are rapidly approaching the moment when machines achieve an observable level of self-awareness.[286] When that day arrives, what will it mean for us? Will the Internet use social media wars to further divide us, to spread misinformation, or to manipulate humans in other ways?

A lot of good is coming from AI, to be sure. Already, AI-powered technologies are helping doctors detect life-threatening illnesses sooner, allowing farmers to revolutionize agricultural production, and empowering scientists to decode the cosmos. But the nefarious potential looms large, too. Imagine a scenario along the lines of the GameStop debacle, when Internet users crowd-source efforts to inflate the company's stock price, an episode that could be repeated on a wider scale using AI to manipulate financial markets. Similarly, security experts worry that sophisticated, AI-enabled cyber-attacks could put our nation's critical infrastructure at grave risk or create novel ways for cyber criminals to conduct digital heists.

America's adversaries are already using the technology against the United States. For example, China is suspected of having used AI and big data to identify and root out Western spies, unraveling sweeping U.S. espionage networks built over the course of years and even decades.[287] Meanwhile, Russia is believed to be using AI and machine learning to bolster its weapon systems and to improve disinformation and propaganda campaigns, which have been designed to sow discord in Western democracies, including during the 2016 and 2020 U.S. elections.[288]

The disruptive national security impacts from AI haven't gone unnoticed. The Congressionally mandated National Security Commission on Artificial Intelligence (NSCAI) recently concluded its work, declaring that foreign AI capabilities have, "[f]or the first time since World War II, [put] America's technological predominance […] under threat" and that the United States "is not prepared to defend or compete in the AI era," calling it a national emergency.[289] Meanwhile, the Department of Defense has released principles outlining how it will leverage AI, and federal agencies have been charged with developing AI plans to ensure the United States is able to best leverage the technology without onerous regulatory burdens.[290]

Still, the country is only just beginning to grapple with the sheer magnitude of unknowns that AI will introduce, especially as the technology becomes more powerful and free-thinking. As the NSCAI wrote, "no comfortable historical reference captures the impact of artificial intelligence on national security," comparing it to Thomas Edison's description of electricity: "it is a field of fields... it holds the secrets which will reorganize the life of the world."[291] In fact, AI may be closer than we think to taking on a life of its *own*, given developments in a parallel field, quantum computing.

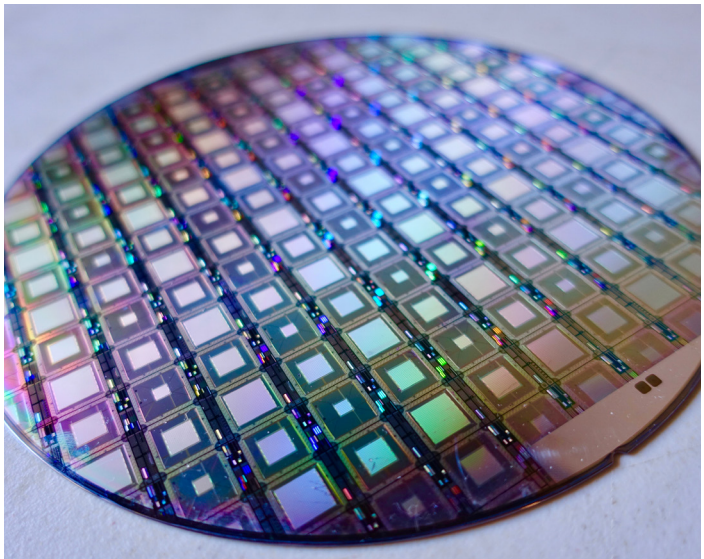
QUANTUM COMPUTING: "WHAT IF A ROBOT IS ANGRY?"

In 2020, I joined a leading quantum scientist for a meeting with representatives from the U.S. intelligence community. They were mostly concerned about when quantum computers would break encryption—the set of protocols used to safeguard everything from emails to banking records.

"It could happen within ten years," the expert somberly informed the worried audience, some of whom knew the United States wouldn't be prepared to deal with the consequences of foreign governments being able to hack our most sensitive communications.

"But you should look further out than that," the quantum whiz suggested. "Because in the 2030s, the technology we are developing could theoretically be used to give machines genuine, human-like emotions." Jaws dropped. Similar claims have been made publicly by leading experts in the field.[292]

Quantum computing is advancing quickly. By harnessing the power of physics to crunch data (rather than relying on long strings of *ones* and *zeros*) quantum computers will be able to solve previously unsolvable problems and even model nature itself. Less than two years ago, Google announced it had achieved "quantum supremacy," when its advanced computer performed a task in under two minutes that would have taken the world's fastest supercomputer 10,000 years to complete.[293] Since then, other companies have made rapid strides with their own machines.[294]



"A Wafer of the Latest D-Wave Quantum Computers" by jurvetson is licensed under CC BY 2.0

The technology's economic potential is obvious. It will help solve some of the toughest challenges in chemistry, medicine, physics, and beyond. Quantum computers will also supercharge artificial intelligence in extraordinary—and, in some cases—unforeseeable ways. Take the example above. A machine that can think independently is one thing, but one that can feel emotion is something else entirely. Such traits could hypothetically allow machines to learn about their environments more quickly, perform tasks more organically, and engage with humans more authentically.

It could also pose a serious threat. Aside from breaking encryption, a quantum computer that supercharges AI to give it human-like emotions might lead to the dystopian world futurists have long feared. What happens when a robot gets sad? What will it do if it gets angry? These are no longer sci-fi questions. They are national security concerns that raise a host of legal, ethical, and existential conundra, some of which are not yet known but must be explored before the technology is too advanced.

Time is not on our side. Quantum computers are poised to get more powerful, more quickly.[295] For every "qubit" (the basic building block of quantum information) added to a quantum machine, its processing power doubles. This means we will see steady exponential and double-exponential growth in quantum computing power in the 2020s, leading to a highly competitive and uncertain 2030s.

What does this signal for geopolitics? At the moment, nations around the world are in a digital arms race to develop fully-functioning quantum machines, recognizing the benefits it could give them, from industry to healthcare to national defense. Whichever nation has the computer with the most qubits will have an edge, able to exceed the processing power of rivals. That might mean their drones will be able to out-swarm those of rivals, or that their network defenses will be able to outsmart even the most sophisticated foreign hackers.

For years we have talked about defense in terms of "qualitative" or "quantitative military edge" (QME)—the marginal additional military power one country has over another. In the quantum future, we will be talking about the "qubit military advantage" (QMA)—the marginal additional processing power one armed force is able to bring to bear against another. Unfortunately, the federal government has done only limited policy planning for this inevitable future, leaving the United States unable to anticipate and defend against the dangers of the quantum future.

A NATION UNPREPARED

Whether it is the dynamic dangers posed by autonomous drones, advanced artificial intelligence, or quantum computing, I can say confidently that the United States is unprepared for the future—a future we will be less equipped to predict than we were in the original Roaring Twenties, an ominous sign for what could happen in national security and international conflict in the years to come. In short, the one *certainty* of the New Roaring Twenties is *uncertainty*, as tech developments will set the stage for a highly variable and dynamic threat landscape in the 2030s and beyond.

What can we do about it? We cannot get ahead of the problem. It is already too late. These technologies are going "live" at this very moment, outstripping the typically laborious national-security policymaking process and leaving us little time to "plan" for the future. Instead, the United States should prioritize two vital missions. First, we need to remain the world's leader in each of these fields in order to *preserve our advantage*. Second, we must adapt our policy posture to *react at machine speed* to new tech developments.

On the first point, we have a great deal of work ahead of us. Yes, the United States has developed sophisticated drone, AI, and quantum capabilities, among other emerging tech. But our rivals are nipping at our heels and, in some cases, are poised to surpass U.S. dominance.

This will allow them to better understand the offensive potential of such technologies and develop the defense mechanisms to protect themselves sooner than we will, making us more vulnerable.

One option is a "Space Act" for the modern age. Just as the United States catalyzed unprecedented research and development in the space race through public-private partnership, America must urgently undertake massive investment in emerging tech areas with dual purpose: to develop the technology to our economic benefit and to pursue advanced research into its nefarious uses and how to thwart them.

The concept is especially salient in quantum computing, where nation-state competitors are funding the technology themselves, recognizing it is not yet profitable enough for private entities to do so at the necessary scale to develop a high-functioning machine. If America doesn't do the same, we'll risk a "quantum winter," a period in which capital dries up and the United States falls suddenly behind in the spring toward next-generation computing capabilities.

Second, in addition to "staying in the lead," we must also account for the possibility—if not the certainty—of strategic surprise. Machines that can "think" for themselves will allow nation states to mature their defensive and offensive capabilities in ways unforeseen. Officials should anticipate that an adversary will develop breakout systems that catch us off guard and instantly make our own defenses obsolete. Sadly, many U.S. departments and agencies are woefully behind in developing serious strategic planning to account for this looming future and are ill-equipped to respond quickly.

Autocratic governments have an edge when it comes to rapid reaction. They centralize power and, therefore, centralize decision-making authority, allowing them to pivot quickly in the face of a changing international security climate. Even still, autocracies suffer from structures that disincentivize truth and objective analysis, as subordinates feed leaders information they want to hear rather than what they need to hear.

This is where America could develop an upper hand. We can react more quickly to the future of free-thinking machines by better "crowd-sourcing" our response; that means short-circuiting the bureaucratic decision-making process to get leaders real-time insights while also allowing them to more quickly delegate authorities to the frontlines to respond to new threats. Such reforms should begin at the grass tops, with the National Security Council undertaking a full-scale reexamination of America's defense posture, how it is coordinated, and what can be done to reduce reaction times, while also enlisting private sector support without the thick red tape of archaic procurement processes. Various respectable commissions have recently issued actionable recommendations in this regard, and it would be wise for the Biden Administration to heed them.[296]

We must be clear-eyed about forthcoming technology security unknowns. And we must be dead set on winning the global technology race. Nothing less than our lives, our livelihoods, and our way of life depend on it. It may be hyperbolic to suggest that machines have achieved consciousness and that the Internet is trying to kill us—for now, at least. Then again, I sourced, wrote, and edited this piece entirely online, with the web looking over my shoulder.

---

[278]James R. Fitzsimonds and Jan M. Van Tol, "Revolutions in Military Affairs," *Joint Force Quarterly* (Spring 1994): 24-31, <https://apps.dtic.mil/dtic/tr/fulltext/u2/a360252.pdf>.
[279]Secretary of Defense Donald Rumsfeld, "Defense Department Briefing," broadcast on CSPAN, February 12, 2002, <https://www.c-span.org/video/?168646-1/defense-department-briefing/>.
[280]Nick Paton Walsh, Natalie Gallón, et al, "Inside the August plot to kill Maduro with drones," CNN, June 21, 2019, <https://www.cnn.com/2019/03/14/americas/venezuela-drone-maduro-intl>.
[281]David Miller, "Swarm Warning: The Future of Unmanned Aerial Systems," U.S. Army, September 21, 2020, <https://www.army.mil/article/239210/swarm_warning_the_future_of_unmanned_aerial_systems>.
[282]Ryan Hilton, "The FAA's New Digital License Plate Requirement for Drones," JDSupra, January 26, 2021, <https://www.jdsupra.com/legalnews/the-faa-s-new-digital-license-plate-5236373/>.
[283]Department of Homeland Security, Press Release, October 4, 2018, "Secretary Kirstjen M. Nielsen Statement on Passage of Legislation to Counter Dangerous Unmanned Systems," < https://www.dhs.gov/news/2018/10/04/secretary-kirstjen-m-nielsen-statement-passage-legislation-counter-dangerous>.
[284]Steve Paulson, "The Nature of Consciousness: How the Internet Could Learn to Feel," *The Atlantic*, August 22, 2012, <https://www.theatlantic.com/health/archive/2012/08/the-nature-of-consciousness-how-the-internet-could-learn-to-feel/261397/>.
[285]Ibid.
[286]Meghan O'Gieblyn, "Is the Internet Conscious? If It Were, How Would We Know?" *Wired*, September 16, 2020, <https://www.wired.com/story/is-the-internet-conscious-if-it-were-how-would-we-know/>.
[287]*Zach Dorfman*, "China Used Stolen Data to Expose CIA Operatives in Africa and Europe," Foreign Policy, December 21, 2020, <https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks/>.
[288]Karla Lant, "China, Russia and the US Are in An Artificial Intelligence Arms Race," *Futurism*, September 12, 2017, <https://futurism.com/china-russia-and-the-us-are-in-an-artificial-intelligence-arms-race>.
[289]*National Security Commission on Artificial Intelligence*, Final Report, U.S. Government Document, March 2021, < https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf>, pp. 1; 7.
[290]Department of Defense, Press Release, February 25, 2020, "DOD Adopts 5 Principles of Artificial Intelligence Ethics," <https://www.defense.gov/Explore/News/Article/Article/2094085/dod-adopts-5-principles-of-artificial-intelligence-ethics/>; Russell T. Vought, *Memorandum for the Heads of Executive Departments and Agencies*, U.S. Government Document, January 7, 2019, < https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf>.
[291]*National Security Commission on Artificial Intelligence*, Final Report, p. 7.
[292]"American Innovation in the Quantum Future," Center for Strategic and International Studies, January 29, 2020, <https://www.csis.org/events/american-innovation-quantum-future>.
[293]Elizabeth Gibney, "Hello quantum world! Google publishes landmark quantum supremacy claim," *Nature*, October 23, 2019, <https://www.nature.com/articles/d41586-019-03213-z>.
[294]Elizabeth Gibney, "Quantum computer race intensifies as alternative technology gains steam," *Nature*, November 17, 2020, <https://www.nature.com/articles/d41586-020-03237-w>.
[295]"Former Google National Security Chief Miles Taylor Discusses Quantum Computing—and How It May Soon Revolutionize Our Lives," Accesswire, March 25, 2021, <https://www.accesswire.com/637513/Former-Google-National-Security-Chief-Miles-Taylor-Discusses-Quantum-Computingand-How-It-May-Soon-Revolutionize-Our-Lives>.
[296]See *National Security Commission on Artificial Intelligence, Final Report.*

Miles Taylor is a national security expert and former CNN contributor. A New York Times bestselling author, Taylor served as chief of staff of the U.S. Department of Homeland Security and later as the head of advanced technology and security strategy at Google. He is a Senior Fellow at the McCrary Center for Cyber and Critical Infrastructure Security.