Statement before the

Senate Homeland Security and Governmental Affairs

Subcommittee on Emerging Threats and Spending Oversight

"Advanced Technology: Examining Threats to National Security"

A Testimony by:

Gregory C. Allen

Director, Wadhwani Center for AI and Advanced Technologies, CSIS

Tuesday, September 19, 2023

562 Dirksen Senate Office Building

Chair Hassan, Ranking Member Romney, and distinguished members of the Subcommittee, thank you for inviting me to testify today. The Center for Strategic and International Studies (CSIS) does not take policy positions, so the views represented in this testimony are my own and should not be taken as representing those of my current or former employers.

I currently serve as the director of the Wadhwani Center for AI and Advanced Technologies at CSIS, where I lead a team conducting policy research at the intersection of technology, economics, and national security. Prior to CSIS, I spent three years working at the U.S. Department of Defense Joint Artificial Intelligence Center, where I most recently served as the director for strategy and policy.

For my testimony today, I hope to offer a perspective regarding the national security threats of artificial intelligence (AI) and other emerging technologies that is informed by my experience serving in government as well as my research work since leaving government.

An Overarching Trend: Reduced Cost and Complexity

To begin, let me say that there is a broad technological trend across many fields where the cost and complexity of many technological capabilities and activities have come down significantly. In many cases, it takes less money and fewer highly trained expert staff to perform the same activity.

As a result, certain types of activities that used to be only within the reach of large governments or military organizations can now be performed by individual corporations or even individual people. Take, as just one illustrative example, orbital space launch. Prior to SpaceX's successful launch of the Falcon 1, developing a new orbital space launch vehicle typically cost billions of dollars and required thousands or tens of thousands of employees. SpaceX developed the Falcon 1, which successfully launched in 2008 for only $90 million dollars. At the time of the launch, SpaceX had a staff of only around 500 people.[1]

In general, the falling cost and complexity of technologies and the activities they enable is good news for the global economy and society. This trend should be celebrated. However, it also poses genuine challenges for U.S. national security in areas where high cost and complexity have historically presented a barrier to dangerous activities. It is good that, for example, developing nuclear weapons is expensive and complicated. The United States would be significantly less safe if building a functional nuclear weapon was cheap and simple.

While nuclear weapons remain expensive and complicated, there are a number of areas where the cost and complexity of developing, acquiring, and employing national security-relevant technologies is declining. In some important areas, this includes placing certain dangerous

[1] NASA, *Commercial Market Assessment for Crew and Cargo Systems* (Washington, DC: April 2011), https://www.nasa.gov/sites/default/files/files/Section403(b)CommercialMarketAssessmentReportFinal.pdf.

capabilities within the reach of non-state actors that will seek to use those capabilities to threaten the United States. I will focus on three in particular today.

1) Reduced Cost and Complexity of Weaponizing Autonomous Drones

To provide a simple example, the vast majority of non-state terrorist groups and insurgents throughout history have not had access to military air power for either airborne reconnaissance or long-range precision strike unless they are being directly supported with military aid from a foreign government.[2] Otherwise, aircraft are typically too expensive and difficult to maintain.

The rise of commercial drone aircraft, however, has changed this story significantly. During the Battle of Mosul in 2016, the Islamic State flew more than 300 drone missions in a single month, with roughly 100 of those used for delivering explosives.[3] The U.S. Air Force described this as the first time that U.S. ground forces had come under attack from enemy aircraft since the Korean War. The typical drone used by the Islamic State during this period was a commercial model purchased for roughly $650 and then modified to carry explosives.

The trend of commercial drones being adapted for military applications now extends to both sides in the war in Ukraine, where Ukrainian forces have used commercial drones to drop explosives on Russian tanks, destroying Russian vehicles costing hundreds of thousands or millions of dollars for the price of a $100 grenade and a $1,000 drone.[4]

The drones being used in the war in Ukraine are generally remotely piloted and travel relatively short distances, but this may change as improved technology becomes more widely available. Russian forces have already used kamikaze drone weapons in Ukraine with autonomous navigation capability,[5] and in early 2023, the leader of a Russian private military corporation stated the group's intention to test an AI-enabled autonomous tank weapons system in active combat, though this may have been an exaggeration to attract attention.[6]

The basic trend of increasingly capable, increasingly autonomous drones that deliver military-relevant capabilities at a fraction of the cost of traditional military systems is highly likely to

[2] John G. Bunnell, "From the Underground to the High Ground: The Insurgent Use of Air Power," Air War College, Air University, February 16, 2011, https://apps.dtic.mil/sti/pdfs/AD1018700.pdf.
[3] Mark Pomerleau, "How $650 drones are creating problems in Iraq and Syria," C4ISRNET, January 5, 2018, https://www.c4isrnet.com/unmanned/uas/2018/01/05/how-650-drones-are-creating-problems-in-iraq-and-syria/.
[4] Gregory C. Allen, "Across Drones, AI, and Space, Commercial Tech Is Flexing Military Muscle in Ukraine," CSIS, *Commentary*, May 13, 2022, https://www.csis.org/analysis/across-drones-ai-and-space-commercial-tech-flexing-military-muscle-ukraine.
[5] Gregory C. Allen, "Russia Probably Has Not Used AI-Enabled Weapons in Ukraine, but That Could Change," CSIS, *Commentary*, May 26, 2022, https://www.csis.org/analysis/russia-probably-has-not-used-ai-enabled-weapons-ukraine-could-change.
[6] Samuel Bendett, "Bureaucrat's Gambit: Why Is Dmitry Rogozin Sending Russian Uncrewed Ground Vehicles to Ukraine—And Does It Matter?," Modern War Institute at West Point, February 10, 2023, https://mwi.usma.edu/bureaucrats-gambit-why-is-dmitry-rogozin-sending-russian-uncrewed-ground-vehicles-to-ukraine-and-does-it-matter/.

continue. At present, the United States does not have a significant challenge with drone-based terrorist attacks, whether AI-enabled or not. However, the relevant technological pieces are in place for such a threat to emerge. In the past, some types of malicious activity, such as ransomware, were technologically viable for a long period of time before they became a widespread cybercrime tactic.[7]

2) Reduced Cost and Complexity of Developing Biological Pathogens

Biotechnology is a clear case where the cost and complexity of dangerous activities have been declining for decades. The American bioweapons program during World War II employed roughly 4,000 people, of whom more than 500 were technical experts. Its multi-year budget totaled roughly $40 million ($690 million in 2023).[8] This was assessed at the time to be roughly the minimum viable program size for a bioweapons research and development effort.[9]

Decades later, in the 1990s, the Aum Shinrikyo terrorist organization in Japan attempted multiple times to develop and deploy biological weapons using botulinum and anthrax. Thankfully, Aum Shinrikyo's bioweapons efforts failed. However, the group successfully executed many steps of developing and delivering bioweapons despite having only a handful of technical expert staff and a much smaller research and development budget than any nation state.[10] Of special note, Aum Shinrikyo had members with education from and ties to legitimate academic research organizations working in biology and medicine.

Today, the development of advanced genetic engineering technologies such as CRISPR has radically reduced the cost and complexity of gene editing to the point where even amateurs can modify the genes of viruses.[11] Some research organizations have previously published genetic information related to highly lethal (but not highly contagious) pathogens such as bird flu.[12] Terrorists and terrorist organizations following in the footsteps of Aum Shinrikyo may be able to create genetically modified pathogens that are both highly contagious and highly lethal. The U.S.

[7] "History of Ransomware," Crowdstrike, October 10, 2022, https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/.
[8] Lt. Comdr. William B. Sarles, "Report of Meeting, 28 December 1944" (Washington, DC, December 28, 1944), RG 160, NM-25 12, Box 77, National Archives at College Park, MD.
[9] William F. Vogel, "'The Mighty Microbe Can Go to War': Scientists, Secrecy, and American Biological Weapons Research, 1941–1969," (PhD dissertation, University of Minnesota, November 2021), https://conservancy.umn.edu/bitstream/handle/11299/226425/Vogel_umn_0130E_22969.pdf.
[10] Richard Danzig et al., *Aum Shinrikyo: Insights into How Terrorists Develop Biological and Chemical Weapons* (Washington, DC: Center for a New American Security, December 2012), https://s3.us-east-1.amazonaws.com/files.cnas.org/hero/documents/CNAS_AumShinrikyo_SecondEdition_English.pdf.
[11] Heidi Ledford, "Biohackers gear up for genome editing," *Nature* 524 (2015): 398–399, https://www.nature.com/articles/524398a.
[12] Nell Greenfieldboyce, "Scientists Publish Recipe For Making Bird Flu More Contagious," NPR, April 10, 2014, https://www.npr.org/sections/health-shots/2014/04/10/301432633/scientists-publish-recipe-for-making-bird-flu-more-contagious.

Intelligence Community specifically called out this bioweapons proliferation threat in a previous report to Congress.[13]

3) Reduced Cost and Complexity of High-Quality Forged Media

One of the most remarkable capabilities of modern AI technology is its ability to generate compelling synthetic digital media—text, photos, videos, and audio files—that can realistically imitate or depict real people in appropriate contexts. Today, many of these AI-enabled media forgery capabilities, commonly referred to as deepfakes, are realistic enough that they can routinely fool the untrained eye and ear and sometimes even the trained eye and ear. Moreover, these tools are increasingly available not only to advanced computer scientists, but to essentially anyone with a computer or smartphone.

During my time at the Department of Defense, my organization collaborated with DARPA on an effort to detect deepfake media using technical analysis. Similar efforts to develop digital forensics tools to detect AI-generated media are now widespread in the private sector and academia.[14]

However, work on such tools is not preventing deepfakes from featuring increasingly prominently in cybercrime and disinformation attacks. For example, in July 2019, Symantec reported that it was aware of three cases in which deepfake audio was used as part of a criminal operation to impersonate corporate CEOs in which company employees were tricked into transferring funds totaling millions of dollars.[15] More recently, deepfakes have been used as part of false kidnapping scams and other types of crime.[16]

Beyond criminal theft, deepfakes are also increasingly likely to feature in politically motivated disinformation efforts. In March 2022, a deepfake video—presumably created by the Russian government—depicted Ukrainian president Volodymyr Zelenskyy surrendering to Russia and instructing Ukrainian forces to stop fighting.[17] The quality of this particular deepfake was quite low, and the Ukrainian government had been warning its citizens to expect manipulated videos. As a result, few were fooled. Pro-Chinese propaganda organizations have also recently used

[13] James R. Clapper, "Worldwide Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, February 9, 2016, https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.
[14] Matthew Hutson, "Detection Stays One Step Ahead of Deepfakes—for Now: The spread of AI-generated content is keeping the tech designed to spot it on its toes," IEEE Spectrum, March 6, 2023, https://spectrum.ieee.org/deepfake.
[15] "Fake voices 'help cyber-crooks steal cash'," BBC, July 8, 2019, https://www.bbc.com/news/technology-48908736.
[16] Faith Karimi, "'Mom, these bad men have me': She believes scammers cloned her daughter's voice in a fake kidnapping," CNN, April 29, 2023, https://www.cnn.com/2023/04/29/us/ai-scam-calls-kidnapping-cec/index.html.
[17] James Pearson and Natalia Zinets, "Deepfake footage purports to show Ukrainian president capitulating," Reuters, March 17, 2022, https://www.reuters.com/world/europe/deepfake-footage-purports-show-ukrainian-president-capitulating-2022-03-16/.

deepfake media as part of an online disinformation effort.[18] This was also a low-quality effort with minimal impact.

However, these examples should not lead anyone to conclude that future deepfake disinformation campaigns will continue to be equivalently clumsy and ineffective. Many early cyberattacks were also clumsy and ineffective, but the field improved dramatically over time. Moreover, important events in recent world history have frequently hinged upon disseminating the right media at the right time. For example, the 2015 attempted coup in Turkey was prevented in part because the Turkish president conducted a live TV interview via video call in which he successfully encouraged Turkish citizens to protest the coup.[19] Had that news broadcast been coopted by a deepfake disinformation attack, perhaps the events that day might have taken a different course.

Governance of Artificial Intelligence

In 2012, a revolution in the application of deep neural networks and GPU processors to image recognition kicked off a decade of revolutionary progress in AI technology. In just the past year, a second equally extraordinary AI revolution has begun with the application of generative AI models. These two major milestones in AI over the last 15 years have considerably expanded the scale and scope of AI's applications across the global economy, civil society, and international security. Generative AI has the potential to disrupt industries, driving large gains in efficiency and quality, but will also raise difficult questions about workforce displacement, education, intellectual property rights, and responsible use. People and organizations of all sizes are already using AI to advance labor productivity and drive anti-inflationary growth, develop more sustainable products, cure diseases, feed a growing population, and address climate change. In the future, AI has the potential to transform the way societies learn, work, innovate, and address global challenges.

Like any technology, AI presents risks. AI can be maliciously used for harm, such as the previously mentioned disinformation attacks, and can also be a source of unintentional harm through technical or managerial failures.

There is no inherent trade-off between mitigating AI risks and pursuing the benefits of increased adoption. We can pursue both goals simultaneously. AI regulation and frameworks must be well balanced, ethically designed, and part of an internationally interoperable framework.

Many uses of AI are already regulated today when AI is used in a regulated application. For example, a bank using AI as part of a consumer lending decision would still be subject to the relevant regulations, such as non-discrimination. Any use of machine learning in an aircraft would still be subject to U.S. air safety regulations.

[18] Graphika Team, "Deepfake It Till You Make It, Pro-Chinese Actors Promote AI-Generated Video of Fictitious People in Online Influence Operation," Graphika, February 2023, https://public-assets.graphika.com/reports/graphika-report-deepfake-it-till-you-make-it.pdf.
[19] Kieran Healy, "Turkey Coup: How Facetime and social media helped Erdogan foil the plot," Vox, July 16, 2016, https://www.vox.com/2016/7/16/12206304/turkey-coup-facetime.

A key challenge for regulators, however, is the fact that AI systems are becoming both increasingly powerful and increasingly generalized. Many large language models, for example, can expound on topics ranging from medical advice, to engineering assistance, to military strategy.

These models currently suffer from "hallucinations" and other reliability problems that limit the willingness of most customers to deploy them in mission- and safety-critical applications without appropriate guardrails in place. Sector-specific regulations are still useful and appropriate, but there is also an opportunity for more general regulations that would be helpful, particularly for the largest and more advanced models.

More generalized regulations in support of AI safety should take the form of a licensing regime for the most advanced AI models and a Know Your Customer requirement for cloud companies that are supporting the development and use of advanced AI models.

Artificial Intelligence and Semiconductor Export Controls

AI powered by machine learning is a general-purpose technology, analogous to electricity or digital computers. When first invented during World War II, computers had only a handful of important military applications, such as code breaking. Today, nearly every military technology involves computers to some greater or lesser extent, whether that is radio communications or missile guidance systems. Even military items that do not have any computers, such as boots or bullets, were nonetheless designed on computers.

Military AI is in a similar situation today as computers were in the 1940s and 1950s. There are a handful of applications where the use of AI is already delivering significant military benefit—such as satellite imagery analysis. Over the next several decades, AI technology will be involved in a rapidly growing share of military activities. The senior military leadership of both the United States and China believe that AI will be foundational to the future of military and economic power.

In some areas, AI will genuinely revolutionize how military operations and warfighting are conducted. The Department of Defense's Replicator Initiative, which seeks to field thousands of AI-enabled and attritable autonomous drones within the next 24 months, is one example.

AI development is not merely an issue of software. All software has to run on semiconductor chip hardware somewhere, and that hardware, and the software architectures that run on top of it, are areas in which the United States and allied countries have a significant technological edge.

On October 7, 2022, the Biden administration adopted a new export controls policy designed to severely restrict China's access to American semiconductor technology, including chips,

chipmaking equipment, chip design software, and equipment components.[20] This was a genuine landmark in the history of U.S.-China relations.[21]

The four chokepoints mentioned above are not all alike in the case of enforcement. Chipmaking equipment, which is large, expensive, and produced in limited quantities, is easiest to enforce prior to sale and—to a lesser extent—even after sale. However, from China's perspective, the most direct path to AI progress is simply continuing to use American chips. It is at this first and crucial chokepoint that China most flagrantly attempts to evade our export controls—and too often succeeds.

The Bureau of Industry and Security (BIS) at the Department of Commerce oversees most export controls. Unfortunately, BIS is increasingly challenged by worldwide smuggling and export control evasion networks, especially those that are supported by Russia and China. For example, investigators have examined the wreckage of downed Russian weapons systems in Ukraine and found that they contain U.S. and allied components, including electronics that were manufactured years after the implementation of the 2014 Russia export controls.[22]

As our geopolitical rivals pursue increasingly aggressive and better-resourced means of obtaining critical technology, BIS must use every tool available to increase capacity and productivity for effective enforcement. At a time when the need for robust U.S. export controls is more strategically critical than at any time since the end of the Cold War, BIS's enabling technology is in a poor state.

The cause is simple: decades of underinvestment. Current and former BIS staff have told CSIS in interviews that the major government databases that they use to monitor trade flows and identify suspicious activity can perform only a fraction of the needed functionality and crash routinely. Instead of knowledge graph databases and machine learning—capabilities that have revolutionized both the private sector and other federal agencies with similar missions—BIS analysts often perform their work primarily using Google searches and Microsoft Excel.

Modern, data-driven digital technologies utilizing AI and machine learning can and should play an integral role in enhancing BIS export control enforcement capabilities. Relatively modest investments could lead to significant improvements in analyst productivity. Despite the increasingly pressing need to invest in these new enforcement capabilities, the budget of BIS has not increased commensurate with the increased number of export-controlled items, the evolving threat landscape, and the growing pressure from an increasingly sophisticated evasion regime.

---

[20] Gregory C. Allen, *Choking off China's Access to the Future of AI* (Washington, DC: CSIS, October 2022), https://www.csis.org/analysis/choking-chinas-access-future-ai.
[21] Gregory C. Allen, *China's New Strategy for Waging the Microchip Tech War* (Washington, DC: CSIS, May 2023), https://www.csis.org/analysis/chinas-new-strategy-waging-microchip-tech-war.
[22] Jeanne Stars and Stripes, June 16, 2022, https://www.stripes.com/theaters/us/2022-06-15/us-electronic-chips-russian-military-6356609.html.

The current international momentum behind U.S.-led export controls presents a unique opportunity both to help solve a pressing problem—responding to Russia's invasion of Ukraine—and to advance the adoption of digital technology by U.S. government agencies for mission impact. A changed geopolitical landscape demands reinvigorated U.S. government export controls capacity, and this cannot be done without additional resources. CSIS analysis of relevant, comparable data-driven digital technology modernization efforts by other U.S. government agencies with similar mission requirements suggests that this could be accomplished with an additional appropriation for technology modernization at BIS of roughly $25 million annually for five years.

This funding would allow BIS to better ingest, connect, and analyze hundreds of billions of records from both government and open-source data. By applying modern data science and machine learning techniques, BIS could increase productivity across all its processes, such as automatically detecting that a purported Eastern European "tractor manufacturer" has the same phone number as a supplier of engines to the Russian military. This figure accounts for opportunities at BIS to improve collaboration with other U.S. government agencies and the need to prevent unnecessary duplication of effort.

However, a more productive enforcement analysis community will identify more entities as likely shell companies engaging in illicit transactions. This will in turn increase the need for enforcement agents to conduct site inspections or criminal investigations of these identified entities. Despite the severe current technological limitations on the efficacy of the analytic community, its work is already identifying enough candidate entities for inspection to more than fully consume the capacity of the current staff. Therefore, in addition to the $25 million annual increase for five years to support new technology and staff for BIS analytical capabilities, BIS will also require an additional $18.4 million and 48 positions annually for the Export Enforcement organization as well as another $1.2 million for additional classified facility space for these individuals to support the classified aspects of their work. Thus, the total size of the recommended additional BIS budget appropriation is $44.6 million annually.

In terms of return on investment, this increase in BIS's budget by $44.6 million annually is likely to be one of the best opportunities available anywhere in U.S. national security. The U.S. government is currently spending tens of billions to assist Ukraine in destroying the weapons of Russia's military, which too often are powered by U.S. technology. Providing a few tens of millions of dollars annually to BIS to modernize the technology that enables export controls enforcement and increase their staff would go a long way toward ensuring that far fewer Russian and Chinese weapons using U.S. technology are built in the future.

Conclusion

AI and biotechnology, together with other emerging technologies, are among the most exciting developments occurring anywhere in the global economy. While I have focused my testimony on the risks and challenges that these technologies present for U.S. national security, I want to emphasize again that emerging technologies have enormous positive potential. The United States

government should pursue accelerated adoption of these technologies in areas where they have the potential to make a positive impact, while also pursuing regulatory and other mechanisms that can improve the safety and security of the United States.

Thank you for the opportunity to testify today, and I look forward to your questions.