



Emerging technologies and challenges to nuclear stability

Steve Fetter & Jaganath Sankaran

To cite this article: Steve Fetter & Jaganath Sankaran (11 Dec 2024): Emerging technologies and challenges to nuclear stability, Journal of Strategic Studies, DOI: [10.1080/01402390.2024.2433766](https://doi.org/10.1080/01402390.2024.2433766)

To link to this article: <https://doi.org/10.1080/01402390.2024.2433766>



Published online: 11 Dec 2024.



Submit your article to this journal [↗](#)



View related articles [↗](#)





View Crossmark data [↗](#)

ARTICLE



Emerging technologies and challenges to nuclear stability

Steve Fetter ^a and Jaganath Sankaran ^b

^aSchool of Public Policy, University of Maryland, College Park, MD, USA; ^bLBJ School of Public Affairs, University of Texas Austin, Austin, TX, USA

ABSTRACT

Emerging technologies are likely to have significant impacts on international security, particularly nuclear stability. A combination of these technologies could enable persistent surveillance, identification and tracking of mobile nuclear delivery platforms, such as submarines, mobile missile launchers, and bombers, weakening deterrence and catalyzing an arms race. At the same time, these technologies might enhance the survivability of nuclear arsenals, offering new ways to deceive adversaries and provide robust communication, attack warning, and navigation capabilities. To better understand the effect of emerging innovations on nuclear deterrence, we examine five technologies: small satellites, hypersonics, machine learning, cyber weapons, and quantum sensing.

ARTICLE HISTORY Received 19 November 2024; Accepted 20 November 2024

KEYWORDS Emerging technology; nuclear deterrence; space security; hypersonics; quantum sensing

Technology has long been an important factor in international security, influencing the balance between offense and defense and the strategies that states adopt to ensure their survival and security. National security, in turn, has been a driver of scientific discovery and technological innovation, and defense and intelligence are often among the first applications for new technologies. This has been particularly true in the nuclear domain, where the discovery of fission on the eve of World War II led to the development of nuclear weapons, and over subsequent decades stimulated the development of computers for weapon design, long-range jet aircraft and rockets for weapon delivery, nuclear reactors for naval propulsion, satellites to monitor adversary forces and warn of attack, and communication systems that could operate through a nuclear attack, including an early version of the Internet.

Many observers believe we have entered a new era of technological innovation – a fourth industrial revolution. Like previous industrial

CONTACT Steve Fetter  sfetter@umd.edu  School of Public Policy, University of Maryland, College Park, MD, USA

revolutions, this one is certain to have implications for international security. The first industrial revolution was powered by coal for the production of iron and the mass production of rifles and artillery; the telegraph and steam-powered railroads and ships enabled the rapid movement of information, troops, and supplies across large distances – technologies first employed on a large scale in the American Civil War. The second industrial revolution was powered by oil and electricity for the production of chemicals and steel and assembly-line production of tanks, ships, airplanes, and radios – technologies that characterized the first and second World Wars. The third industrial revolution was powered by computers, satellites, and lasers for the collection, analysis, storage, and transmission of data across worldwide networks; it produced the technologies noted above that characterized the Cold War.

The fourth industrial revolution is characterized not only by new technologies on the horizon, but also by advances in existing technologies that have produced novel applications. The foundation of this revolution is the steady advance in microelectronics. Moore's Law – the doubling of the number of transistors in an integrated circuit every two years – has resulted in a million-fold increase in the last 40 years. This has enabled even greater increases in the rate at which data are collected, analyzed, stored, and transmitted.¹ It has also produced spectacular advances in sensors, including cameras with hundreds of megapixels and hyperspectral capabilities ranging from the infrared to the ultraviolet and chip-scale GPS receivers, radar and lidar, and even atomic clocks.

An excellent illustration of the advance in microelectronics is the smart phone most people carry in their pockets. The iPhone 15, which was released in 2023, has a processing speed equal to the world's fastest supercomputer in 2001.² It also has a 12-megapixel camera that can record video at 60 frames per second, GPS receiver, three-axis gyroscope, accelerometer, magnetometer, barometer, proximity sensor, up to 512 gigabytes of memory, a 3-megapixel display, wired and wireless data transmission rates of up to a gigabit per second, and a battery that can provide a day of continuous use – all in a 6-ounce package. Because these devices are so ubiquitous, it is easy to overlook the stunning advances in technology that they represent.

These advances in microelectronics have enabled similarly consequential advances in software. Operating systems now contain tens of millions of lines

¹The fastest computer in 1982, the Cray XMP, had a peak processing speed of 800 million floating point operations per second, 128 megabytes of memory, and 38 gigabytes of storage. For comparison, the fastest computer in 2022, the Frontier Cray EX, had a processing speed of 1700 trillion operations per second, 9.2 petabytes of memory, and 750 petabytes of storage. Processing speed, memory, and storage increased by factors of 2 million, 70 million, and 20 million over this 40-year period.

²The Apple A16 processor used in the iPhone 15 can execute 17 trillion operations per second – more than the world's fastest computer in 2001. See Kyle Wiggers, "Apple unveils the A16 Bionic, its most powerful mobile chip yet," TC TechCrunch, September 7, 2022, <https://techcrunch.com/2022/09/07/apple-unveils-new-mobile-chips-including-the-a16-bionic>.

of code. The size and complexity of both hardware and software, and the fact that computers are used to control nearly all devices, from coffee makers and thermostats to automobiles and aircraft, has created opportunities to exploit vulnerabilities and remotely damage or control these devices.

Perhaps most notably, the increased power of central processing units (CPUs), particularly graphical processing units (GPUs) that are able to process large streams of data in parallel, has made possible the deep neural networks empowering modern machine learning algorithms. Deep neural networks enable handwriting, speech, and image recognition, language translation, reading comprehension, robots and autonomous vehicles, synthetic media ('deep fakes'), and virtual and augmented reality.

Other technologies that characterize the fourth industrial revolution include new materials and manufacturing techniques, including additive manufacture ('3-D printing'), nanomaterials and nanotechnologies, microfluidics and microreactors, and fiber lasers. New materials and manufacturing technologies have generated surprising gains in the performance of many weapon systems. For instance, materials derived from rare-earth metals facilitate the superior performance of modern weapon systems in extreme temperature, pressure, humidity, and other stressing conditions. Rare-earth magnets are essential for modern radars, missile guidance and control systems, lasers for mine detection, underwater mines, high-performance power generators, and various other subsystems.³ New semiconductor materials offer dramatic improvements in the performance of radars and other military systems.⁴

Advances in biotechnology and neuroscience, including low-cost genome sequencing, synthetic biology, genome editing, and human-machine interfaces will also power the fourth industrial revolution. And although we are approaching the limits of Moore's Law with conventional computer technology, we can glimpse a new generation of quantum technologies – sensors, communications, and computers – that could in theory exceed the performance of conventional technologies by many orders of magnitude.

These emerging technologies are anticipated to affect the stability of nuclear deterrence and the operational patterns of nuclear arsenals. These

³Peter Grier, 'Rare-Earth Uncertainty', Air Force Magazine, December 21, 2017, <https://www.airforcemag.com/article/rare-earth-uncertainty/>; Government Accountability Office (GAO), 'Rare Earth Materials: Developing a Comprehensive Approach Could Help DOD Better Manage National Security Risks in the Supply Chain', Feb. (Washington D.C.: Government Accountability Office (GAO) 2016), 22; Bert Chapman, 'The Geopolitics of Rare Earth Elements: Emerging Challenge for U.S. National Security and Economics', *Journal of Self-Governance and Management Economics* 6/2 (2018), 76.

⁴One example of material science driven innovation is the detection and tracking ability of the SPY-6(V)1 Air and Missile Defense Radar. The SPY-6(V)1 will use gallium nitride semiconductors and replace the vacuum-tube-based SPY-1 radars. The U.S. Navy's preliminary analysis suggested that the SPY-6(V)1 would be 40 times more sensitive, but the Navy has determined it to be '100 times more sensitive than the legacy SPY-1 radar' in field tests. See Jason Sherman, 'Navy determines SPY-6 radar three times stronger than original requirement', *Inside Defense SITREP*, 6 May 2019.

technological advances could weaken deterrence and improve the prospects for damage limitation by increasing the ability to destroy nuclear forces and command and control or by improving the prospects of an effective defense. They may also improve the survivability of nuclear forces and command and control and thereby strengthen deterrence, increase stability, and make states more willing to engage in arms control efforts. For example, advances in both satellite and sensor technology will make it possible to replace the small number of strategic communication and early-warning satellites in geosynchronous orbit with large constellations in low-earth orbit, making nuclear command and control more resilient and less vulnerable to attack.

In this article, we explore in detail five prominent emerging technologies that may affect the nuclear balance and incentives for nuclear use or arms racing over the next 10 to 20 years: small satellites, hypersonic weapons, machine learning, cyber weapons, and quantum technologies. While there are many other emerging technologies, the five listed above have received greatest attention in discussions about the future of nuclear deterrence. These technologies could be combined to amplify advances in other emerging weapon systems. For instance, autonomous vehicles navigating using real-time updates from small satellite constellations and equipped with sensors and machine-learning algorithms could, in principle, be used to identify, track, and target missile launchers. Similarly, advances in machine learning and quantum computing could accelerate disruptive innovations in nanotechnology, synthetic biology and gene-editing that could be used as weapons.⁵ We touch upon the possible outsized effects of such a combination of emerging technologies in the concluding section.

Space technology

Space is undergoing a major transformation, stimulated by substantial reductions in both satellite and launch costs. These cost reductions have shifted the primary locus of activity from governments to the commercial sector and have resulted in a dramatic increase in the rate at which satellites are placed in orbit, from an average of about 100 per year in 2000–2010 to more than 2800 in 2023.⁶ Although this expansion is motivated primarily by commercial applications, such as remote sensing and communication, it could have profound impacts on international security and nuclear deterrence.

The combination of improvements in battery and solar photovoltaic technology that have decreased the cost and mass of satellite power supplies, together with the advances in microelectronics described above, have

⁵Andrew F. Krepinevich, Jr., *The Origins of Victory: How Disruptive Military Innovation Determines the Fates of Great Power* (New Haven, CT: Yale UP, 2023), 86.

⁶United Nations Office for Outer Space Affairs, 'Online Index of Objects Launched into Outer Space', United Nations Office for Outer Space Affairs. <https://www.unoosa.org/oosa/osoindex>.

enabled substantial increases in satellite sensor, communication, and on-board processing capabilities, with corresponding decreases in mass and power requirements. These advances have made it possible to perform functions that previously required large and expensive satellites with large numbers of small and inexpensive satellites in low-Earth orbit (LEO).

One of the earliest commercial electro-optical imaging systems, the French SPOT satellites launched from 1986 to 1993, with a 6000-pixel sensor providing a ground resolution of 10 meters, weighed 1800 kilograms and cost \$200 million to build.⁷ For comparison, the SkySat satellites currently operated by Planet, with three 5.5-megapixel sensors and a ground resolution of 0.5 meter, weigh 110 kilograms and cost less than \$5 million.⁸ Not only are these smaller satellites far more capable on an individual basis, the lower mass and cost permit more satellites to be placed in orbit. Whereas two SPOT satellites could image a particular target once per day, the constellation of 21 SkySats provides an average of six revisits per day. Planet plans to expand and upgrade this constellation to provide up to 30 revisits per day with 0.3-meter resolution. Planet also operates a constellation of more than 150 shoebox-sized Dove satellites weighing 5 kilograms each, which image the entire Earth every day at 4-meter resolution.⁹

Satellite communication has traditionally been provided by small numbers of large satellites in geosynchronous orbit. Commercial communication satellites deployed in the late 1980s and early 1990s typically weighed more than a ton and cost several hundred million dollars. Iridium, an early system to provide global satellite communication for individual end-users, was a constellation of 77 satellites in LEO deployed in the late 1990s and early 2000s; each satellite had a capacity of 10 megabits per second, weighed 690 kilograms, and cost about \$50 million to build. For comparison, the Starlink satellites currently being deployed by SpaceX have a capacity of 20 gigabits per second, weigh 260 kilograms, and cost only about \$250,000 per satellite. As of April 2024, SpaceX had more than 5,800 operational Starlink satellites in orbit, with plans to deploy up to 42,000—ten times more than all satellites of

⁷Pierre Bescond, 'Public Verification: The SPOT Satellite Technology', in Dietrich Shroerer and David Hafemeister (eds.), *Nuclear Arms Technologies in the 1990s* (New York: American Institute of Physics 1988); Christopher Lavers, 'The Origin of High Resolution Civilian Satellite Imaging', in Christopher Lavers (ed.), *Recent Developments in Remote Sensing for Human Disaster Management and Mitigation* (2013); European Space Agency (ESA), 'SPOT', European Space Agency (ESA), <https://earth.esa.int/eogateway/missions/spot>

⁸European Space Agency, 'SkySat', <https://earth.esa.int/eogateway/missions/skysat>, <https://earth.esa.int/eogateway/missions/skysat>; Planet, 'Planet Imagery Product Specifications' (Dec. 2018), <https://assets.planet.com/docs/Combined-Imagery-Product-Spec-Dec-2018.pdf>; James Temple, 'Everything You Need to Know About Skybox, Google's Big Satellite Play', Vox, Jun 11, 2014, <https://www.vox.com/2014/6/11/11627878/everything-you-need-to-know-about-skybox-googles-big-satellite-play>

⁹European Space Agency (ESA), 'PlanetScope', European Space Agency (ESA), <https://earth.esa.int/eogateway/missions/planetscope>

all types in orbit at the start of 2021.¹⁰ Amazon and OneWeb also plan to deploy large constellations of communication satellites in LEO.

In addition to the increased capability and decreased cost of satellites, commercial launch services have expanded and the associated costs have decreased substantially. The Space Shuttle was the main U.S. vehicle for placing payloads in LEO in the 1980s and 1990s. At nearly \$1.8 billion per Shuttle launch, the cost to LEO was about \$65,000 per kilogram of payload.¹¹ For comparison, the SpaceX Falcon Heavy, which first carried a satellite to orbit in 2019, costs about \$95 million per launch, equal to \$1,500 per kilogram. The recovery and reuse of major parts, such as rocket engines, have been key to reducing launch costs while maintaining high reliability. The SpaceX Falcon 9, which pioneered the reuse of rocket engines, has had only two failures in 330 launches, making it the most reliable launch vehicle ever.¹² SpaceX is currently developing a fully reusable launch vehicle, Starship, able to deliver more than 100,000 kilograms to LEO.¹³ If reusability lowers the Starship launch cost to \$50 million, the cost to LEO would be only \$500 per kilogram – more than 100 times lower than for the Shuttle. The cost reduction in placing a satellite in orbit is even more dramatic when considering the decrease in satellite mass – from \$100 million for a 2000-kg satellite at \$50,000 per kilogram, to only \$100,000 for a 100-kg satellite at \$1,000 per kilogram.

Benefitting from these positive changes led by the commercial sector, major military powers, particularly the United States and China, are making significant investments in space-based capabilities to support conventional military operations. China has recently embarked on a coordinated effort to employ satellites for military surveillance and targeting, launching more than 400 satellites in the last two years.¹⁴ Similarly, the U.S. Space Development Agency has begun to implement a National Defense Space Architecture based on proliferated constellations of small satellites.¹⁵ These new capabilities, while driven by the need for more routine military functions, could cause

¹⁰Tereza Pultarova and Elizabeth Howell, 'Starlink satellites: Facts, tracking, and impact on astronomy', SPACE.com, September 27, 2024, <https://www.space.com/spacex-starlink-satellites.html>.

¹¹Thomas G. Roberts, 'Appendix 1: Implications of Low-Cost Launch', in Ian Williams, Masao Dahlgren, and Thomas G. Roberts, *Boost-Phase Missile Defense: Interrogating the Assumptions*, (Washington, DC: Center for Strategic & International Studies (CSIS) Missile Defense Project June 2022), <https://aero.space.csis.org/data/space-launch-to-low-earth-orbit-how-much-does-it-cost>, p. 36–44.

¹²SpaceX, 'FALCON 9: First Orbital Class Rocket Capable of Reflight', SpaceX, <https://www.spacex.com/vehicles/falcon-9/>

¹³SpaceX, 'STARSHIP: Service to Earth Orbit, Moon, Mars and Beyond', SpaceX, <https://www.spacex.com/vehicles/starship/>

¹⁴Audrey Decker, 'Chinese Satellites Are Breaking the US "monopoly" on Long-Range Targeting', Defense One, May 2, 2024, <https://www.defenseone.com/threats/2024/05/new-chinese-satellites-ending-us-monopoly-ability-track-and-hit-long-distance-targets/396272/>.

¹⁵Space Development Agency (SDA), 'Broad Agency Announcement-National Defense Space Architecture, Systems, Technologies, and Emerging Capabilities (STEC)', Space Development Agency (SDA), January 12, 2022, <https://www.sda.mil/national-defense-space-architecture-nds-a-systems-technologies-and-emerging-capabilities-stec>.

adversaries to become concerned about the survivability of their nuclear forces.

These new capabilities enabled by advances in satellite technology and sensor microelectronics could have important consequences for nuclear operations. Nuclear forces rely on space-based sensors for a number of key missions:

- **Attack warning.** Satellites equipped with short-wave infrared (SWIR) sensors can detect the hot exhaust of ballistic missiles during their boost phase. In the United States, this includes the Defense Support Program (DSP) and Space-Based Infrared System (SBIRS) in geosynchronous and highly elliptical orbits. These satellites can detect and track ballistic missile launches and provide an assessment of an enemy attack. This capability is essential to provide the option to disperse or launch nuclear forces under attack, before enemy warheads detonate on missile, submarine, and bomber bases. Attack warning is also an essential element of national and regional missile defenses.
- **Communication.** Satellites provide reliable communication with mobile and dispersed nuclear forces, such as ballistic missile submarines and mobile command and control assets. In the United States, this includes the 1990s-era Milstar and the new Advanced Extremely High Frequency (AEHF) satellite systems in geosynchronous orbit. The ability to communicate orders to nuclear forces during and after a nuclear attack is essential for deterrence.
- **Navigation.** Satellites provide accurate position, navigation, and time (PNT) information to mobile missile launchers, ships, submarines, aircraft, and mobile command posts. Missiles that use inertial navigation in flight may rely on satellites to determine their initial position. In the United States, navigation services are provided by the constellation of Navstar Global Positioning System satellites in semi-synchronous orbit, at an altitude of about 20,000 kilometers.
- **Nuclear burst detection.** Space-based sensors can detect and determine the location and yield of nuclear explosions near the Earth's surface, in the atmosphere, or in space. The United States has nuclear-burst sensor packages on GPS satellites, as well as satellites in geosynchronous orbit. These systems can be used to assess enemy attacks as well as the effectiveness of U.S. counterattacks.
- **Intelligence, Surveillance, and Reconnaissance.** Electro-optical, radar, and electronic intelligence satellites are used to detect, identify, and track nuclear forces and command and control assets. These are used to assess adversary nuclear forces, both for attack planning and to monitor compliance with arms control agreements.

Emerging space and sensor technologies can contribute to these missions in various ways, with both positive and negative effects on nuclear deterrence. Perhaps most importantly, replacing a small number of large satellites in geosynchronous orbit with a large number of small satellites in LEO can make a satellite constellation far more resilient to disruption or attack. A major U.S. concern has been the development of antisatellite weapons by Russia or China, combined with indications that both countries plan to use such weapons early in a conflict.¹⁶ Russian and Chinese analysts have described plans to degrade the ability of the United States to use precision conventional weapons and ballistic missile defenses, identify and track mobile targets, and communicate with U.S. forces overseas.¹⁷ There is a concern that such attacks might extend to satellite systems that have dual conventional and nuclear missions, such as communication satellites. There is also concern that Russia or China might attempt to degrade U.S. nuclear command and control through attacks on early warning and strategic communication satellites, if they believed nuclear war was imminent. This has led to proposals for keep-out zones around certain satellites and other defensive measures.¹⁸

The commercial communication satellite constellations being deployed by SpaceX, OneWeb, and Amazon could provide a basis for an extremely resilient backup or replacement for the U.S. Department of Defense Milstar and AEHF satellites. Starlink uses jam-proof high-bandwidth laser crosslinks between satellites and provides higher data rates than Milstar and AEHF at similar extremely high frequencies. It should be possible to add advanced anti-jamming, anti-intercept, and anti-intrusion technologies to uplinks and downlinks and to give DOD priority access to bandwidth upon demand. Alternatively, the U.S. government could build and deploy its own large constellation of Starlink-like communication satellites in LEO.

Large constellations of satellites in LEO would be resilient to antisatellite attack. With a constellation of 30,000 Starlink satellites, two dozen satellites would be high above the horizon of any point on Earth. Attempts to degrade the constellation through attrition could be countered with launches to replenish the constellation. SpaceX currently places 60 Starlink satellites into an orbital plane in a single Falcon 9 launch – a number that is planned to increase to 400 per launch with Starship.

¹⁶See Jaganath Sankaran, 'Russia's Anti-Satellite Weapons: A Hedging and Offsetting Strategy to Deter Western Aerospace Forces', *Contemporary Security Policy* 43, no. 3 (June 2022): 436–63; Jaganath Sankaran, 'Limits of the Chinese Antisatellite Threat to the United States', *Strategic Studies Quarterly* 8, no. 4 (Winter 2014): 19–46.

¹⁷Sankaran, 'Russia's Anti-Satellite Weapons'.

¹⁸James M. Acton Thomas D. MacDonald Pranay Vaddi, 'Protecting the Valuables: Establishing Keep-Out Zones Around High-Altitude Satellites', Chapter 6 in *Reimagining Nuclear Arms Control: A Comprehensive Approach* (Washington, DC: Carnegie Endowment for International Peace, 2021).

Communication satellites such as Starlink could also provide extremely robust and accurate navigation services.¹⁹ Starlink and other communication satellites have GPS receivers to precisely determine their orbit. This location and time information can be encoded into Starlink messages, in a method known as ‘fused LEO navigation’. This could provide accuracies about 10 times greater for ground users than GPS, and a signal about a thousand times stronger than GPS, which would be much more difficult to jam. Such a system would, however, rely on the GPS satellite constellation. As an alternative, one could deploy a dedicated constellation of small navigation satellites in LEO using chip-scale atomic clock technology. In fact, Xona Space plans to deploy more than 300 Pulsar navigation cubesats, providing 0.1-meter accuracy and a signal 1000 times stronger than GPS, operating independently of GPS and other satellite navigation systems.²⁰

The use of large constellations of small satellites in low orbits could be extended to missions for which there is little or no commercial market, such as attack warning and nuclear burst detection. This could be done using small payloads hosted on commercial satellites, such as Starlink, or dedicated platforms. Satellites in LEO could, for example, be equipped with SWIR sensors to detect and track missile launches and other hot objects, such as hypersonic glide vehicles. Earth observation satellites have been equipped with SWIR sensors for many years to monitor forest fires, volcanic activity, soil moisture, and greenhouse gas concentrations. In recent years, this has included micro-satellites that use SWIR cameras with indium-gallium-arsenide sensors, which do not require cryogenic cooling, and have demonstrated the ability to detect rocket plumes.²¹ The U.S. Department of Defense plans to deploy long-wave infrared sensors on a network of commercial satellites to assess the effectiveness of ballistic missile defenses that rely on hit-to-kill interceptors for mid-course intercept of enemy warheads.²²

The technological developments described above generally improve nuclear deterrence, because they have the potential to make nuclear operations that depend on space assets, such as attack warning, communication, and navigation, more survivable and resistant to adversary attack. But the

¹⁹Mark Harris, ‘SpaceX’s Starlink satellites could make US Army navigation hard to jam’, *Technology Review*, September 28, 2020, <https://www.technologyreview.com/2020/09/28/1008972/us-army-spacex-musk-starlink-satellites-gps-unjammable-navigation/>

²⁰Jason Rainbow, ‘Xona to test GPS-alternative demo satellite with customer’, *Space News*, June 7, 2022, <https://spacenews.com/xona-to-test-gps-alternative-demo-satellite-with-customer/>.

²¹Dee W. Pack, Brian S. Hardy, John R. Santiago, David Pietrowski, Jon C. Mauerhan, Paul F. Zittel, Darren W. Rowen, Cameron R. Purcell, Pradeep Thiyaratnam, Lynette J. Gelinias, Paul K. Su, Joel Gussy, and Joseph M. Santiago ‘Flight Operations of Two Rapidly Assembled CubeSats with Commercial Infrared Cameras: The Rogue-Alpha, Beta Program’, Paper presented at the 35th Annual Small Satellite Conference, August 2021, <https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=5023&context=smallsat>; European Space Agency (ESA), ‘GHGSat’, European Space Agency (ESA), <https://earth.esa.int/eogateway/missions/ghgsat>.

²²Mike Gruss, ‘MDA Kill Assessment Sensors Would Be Commercially Hosted’, *Space News*, March 20, 2015, <https://spacenews.com/mda-kill-assessment-sensors-would-be-commercially-hosted/>

impact of emerging technology on intelligence, surveillance, and reconnaissance is less clear. On the one hand, increased Earth observation capabilities will make it easier to monitor the development of nuclear weapon systems, the number and status of operational nuclear forces, and compliance with arms control agreements, making nuclear postures more predictable and surprise less likely. This could decrease the potential for worst-case assessments that might spiral into an arms race.

On the other hand, persistent surveillance can undermine systems that depend on location uncertainty for their survival. Of particular concern are mobile ICBM launchers, but this also applies to strategic bombers, which may be dispersed to other airfields during a crisis; ballistic missile submarines, which may be flushed from port; and mobile command posts. Even if these mobile systems cannot be tracked continuously in near-real-time, the ability to detect preparations to place forces on alert and move them from their bases could create perceived windows of opportunity for preemptive attack, to destroy mobile forces and command posts before they are dispersed. This could create incentives for preemptive strikes if the parties believed war was imminent.

Electro-optical systems, such as SkySat, can monitor objects on the Earth's surface only during daylight and in the absence of significant cloud cover. On average, that amounts to about 30% of all hours over land, but this can be much lower for some locations and seasons. It is highly unlikely that all or even most nuclear bases in a large country would be simultaneously observable. For example, hourly data for two submarine bases (Bangor and Kings Bay) and two bomber bases (Minot and Whiteman) in the United States indicate that all four would be simultaneously observable less than 1% of the year, and three of four would be simultaneously observable less than 10% of the year.²³ For these reasons, even continuous electro-optical satellite imagery should not pose a significant threat to nuclear deterrent forces.

Persistent imagery and reliable identification and tracking of mobile systems requires radar, which can operate at night and in all weather conditions, including heavy cloud cover and precipitation. Radar includes both synthetic aperture radar (SAR), which uses the motion of the radar to simulate an antenna large enough to produce high-resolution images of the ground, and ground moving target indication (GMTI) radar, which uses the difference in Doppler shift between radar pulses reflected off moving objects and the ground to detect moving objects. A radar can be designed to be used in both

²³See Visual Crossing, "Weather Data & API: Global Forecast & History Data," Visual Crossing, <https://www.visualcrossing.com/>. Hourly weather data for 2021 was obtained for Silverdale, WA (Bangor Naval Station), St. Mary's, GA (King's Bay Naval Station), Minot, ND (Minot Air Force Base), and Knob Noster, MO (Whiteman Air Force Base). Cloud cover was less than 25% (a generally accepted maximum for usable imagery) and solar radiation was greater than zero in all four locations only 64 of 8760 hours, or 0.7% of all hours.

SAR and GMTI modes, and SAR can be used to scan large areas at low resolutions (strip-map and scan modes) or to produce high-resolution images by steering the radar beam to keep it focused on a particular target (spotlight mode).

Military SAR and GMTI radars have been based primarily on aircraft. The U.S. Joint Surveillance Target Attack Radar System (JSTARS) was first deployed in 1991 to provide SAR imagery and to detect and track moving targets in a regional theater of operations. SAR and GMTI radar also have been deployed on uncrewed aerial vehicles, such as Predator and Global Hawk. But airborne systems cannot operate over adversary territory in peacetime and are vulnerable to air defenses during a conflict.

Space-based radar is immune from overflight restrictions and air defenses, but the much larger distances from the radar to ground require corresponding increases in radar power or antenna size. In addition, the enormous data processing requirements of SAR and GMTI require either a very large bandwidth for ground processing or very large on-board computational capabilities. GMTI is particularly challenging for space-based radar because the difference in Doppler shift between moving targets and the ground is a tiny fraction of the shift resulting from the very high velocity of the satellite.

The first SAR satellite was SEASAT, which was launched in 1978 and produced images with 25-meter resolution. Canada's RADARSAT-1, launched in 1995, weighed 2750 kilograms and cost about \$840 million to build (2022 US dollars), and produced images with up to 8-meter resolution. The follow-on RADARSAT-2, launched in 2009, provided 3-meter SAR resolution and used novel algorithms to demonstrate a GMTI capability, able to detect passenger vehicles with speeds as low as 8 kilometers per hour.²⁴

A 2007 Congressional Budget Office report examined various alternatives for a military space-based radar system able to detect and track mobile missile launchers.²⁵ The most capable alternative consisted of 21 satellites, with an estimated cost of \$33-46 billion to design and build and another \$33-49 billion to operate over a 20-year period. In SAR mode, the system would be able to image a given area 20-40% of the time at 1-meter resolution, with an average response time of 7 minutes; in GMTI mode, the system could observe relatively fast-moving targets 40-67% of the time under the most optimistic assumptions, with an average response time of 2.5-6.5 minutes. Achieving more persistent coverage at lower resolutions and against slow-moving targets would require larger constellations and/or satellites with larger

²⁴Charles E. Livingstone, RADARSAT-2 GMTI Demonstration Project (Ottawa: Defense Research and Development Canada, February 2012), https://cradpdf.drdc-rddc.gc.ca/PDFS/unc237/p804305_A1b.pdf

²⁵Joseph A. Post and Michael J. Bennett, *Alternatives for Military Space Radar* (Washington, DC: Congressional Budget Office, January 2007), <https://www.cbo.gov/sites/default/files/110th-congress-2007-2008/reports/01-03-spaceradar.pdf>

antennas. For example, an average SAR coverage of 75% would require 88 satellites for 1-meter resolution and 300 satellites for 0.1-meter resolution. With an estimated marginal cost of about \$1 billion per satellite, the cost of such large constellations would have been prohibitive. Such cost concerns led the U.S. Congress to cancel an early DOD program to develop a space-based radar system to provide near-continuous global coverage.²⁶

Recent advances in microelectronics and satellite technology have resulted in the development of a new generation of small and much less expensive SAR satellites for commercial missions. For example, the Finnish company ICEYE has built and launched a constellation of 18 SAR satellites, weighing 85 kilograms and costing \$5-10 million each, with resolution of up to 0.25 meters.²⁷ At least four other companies have announced plans to deploy constellations of small SAR satellites, with estimated costs of less than \$15 million per satellite.²⁸ These small radars have surveillance rates (the area that can be imaged per orbit) that are roughly 10 times smaller than RADARSAT-2 and 100 times smaller than the notional radars in the CBO study.²⁹ Nevertheless, constellations of hundreds or thousands of small radar satellites could provide persistent coverage of the Earth's surface.

It is sometimes claimed that advances in SAR technology may make possible the detection and tracking of submarines through the surface waves they generate. A shallow and fast-moving submarine generates surface waves with amplitudes of 0.1–0.2 meters, which might be detectable by SAR satellites operating in spotlight mode, but that would be possible only if the submarine location is already known.³⁰ SAR resolution when scanning large areas is an order of magnitude worse, making the detection of even shallow and fast-moving submarines in the open ocean extremely challenging. Surface wave amplitude decreases rapidly with increasing submarine depth and decreasing speed; a submarine with a speed of 5 knots at a depth of 100 meters would produce no detectable surface waves.

Recent advances in satellite technology have also been applied to signals intelligence (SIGINT), resulting in constellations of small satellites to collect and analyze electromagnetic signals for various commercial purposes, such as

²⁶House Committee on Appropriations, Report of the Committee on Appropriations, Department of Defense Appropriations Bill, 2005, House Report 108–553, pp. 312–314, <https://www.congress.gov/congressional-report/108th-congress/house-report/553>

²⁷European Space Agency (ESA), 'ICEYE, the World's First SAR New Space Constellation', European Space Agency (ESA), 20 Dec. 2021, <https://earth.esa.int/eogateway/news/iceye-the-world-s-first-sar-new-space-constellation?text=SAR>

²⁸Umbra, <https://umbra.space/>; EOS, <https://eossar.com/>; Capella Space, <https://www.capellaspace.com/>; Synspec, <https://synspec.com/>

²⁹The wide-area surveillance rate for GMTI is proportional to a radar's transmit power multiplied by the antenna aperture. RADARSAT-2 has a peak transmit power of 2.3 kW and an antenna area of 20 m², for a power-aperture product of 46 kWm²; the CBO and ICEYE radars have power-aperture products of 400 and 4.1 kWm², respectively.

³⁰Tom Stefanick, *Strategic Antisubmarine Warfare and Naval Strategy* (Institute for Defense and Disarmament Studies, 1987), pp. 188–197.

monitoring spectrum use and tracking maritime vessels.³¹ Constellations of satellites can use triangulation to pinpoint the location of a radio transmitter or other source of electromagnetic radiation. If mobile nuclear forces and command posts have distinctive radio frequency emissions, satellites might be used to locate and track them.

Collection of EO and SAR imagery and GMTI or SIGINT data is only a first step. The enormous quantities of data collected by satellite constellations must be analyzed to correctly identify objects of interest. This may be done with machine learning and other algorithms, and those algorithms must be highly accurate and robust not only to changes in the observation environment (e.g., viewing angle), but also to adversary attempts to deny detection, identification, and tracking. This could include decoys, camouflage, deception, and signature variation against EO sensors; the use of jammers and radar-absorbing materials and other stealth technologies against radars; and the use of burst transmissions, frequency or time hopping, land lines, and laser communication to counter SIGINT.

Anti-simulation can be a particularly effective countermeasure to identification and tracking of mobile targets. Rather than deploy realistic decoys, road-mobile missile launchers and command posts could be made to resemble common vehicles. During the 1980s, the Soviet Union had a program to develop a mobile ICBM and erector-launcher in a vehicle that was outwardly identical to a common semi-truck.³² The total weight of the mobile missile was about the same as a loaded commercial vehicle. It would have been impossible to distinguish these mobile missile trucks from the hundreds of thousands of other semi-trucks on Soviet highways using the highest-resolution satellite imagery. In the case of SIGINT, generative artificial intelligence opens up the possibility of creating large numbers of decoy transmissions that would be difficult to distinguish from authentic transmissions. It would be relatively simple and inexpensive to deploy hundreds of decoy transmitters for each authentic transmitter.

Adversaries may not conduct realistic exercises with the full suite of countermeasures in peacetime, which would make it difficult to have confidence that identification and tracking algorithms would work well during a war. Although learning and adaptation may be possible in a protracted conventional conflict or a series of conflicts, this is unlikely to be possible in the run up to a nuclear war.

³¹Cortney Weinbaum, Steven Berner, and Bruce McClintock, 'SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain', RAND, 2017, https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE273/RAND_PE273.pdf; <https://www.he360.com/>; <https://alen.space/small-satellites-for-surveillance/>

³²<https://en.topwar.ru/68819-proekt-podvizhnogo-gruntovogo-raketnogo-kompleksa-kurer.html>; <https://en.topwar.ru/168580-jevoljucija-jadernoj-triady-perspektivy-razvitija-nazemnogo-komponenta-sjas-rf.html>

Finally, even if near-continuous observation and robust identification and tracking of mobile nuclear targets is possible, there also would have to be some means of reliably attacking and destroying these targets. Intercontinental and submarine-launched ballistic missiles have flight times of 20 to 40 minutes, depending on range and trajectory; air- and submarine-launched cruise missiles would take hours to reach strategic nuclear targets inside Russia or China. Mobile targets could be attacked with a barrage of nuclear warheads, to destroy the target wherever it could have moved during the flight of the attacking missiles. But barrage attacks would require at least several and up to a dozen nuclear warheads per mobile target if the targets are constrained to a single road, and at least several dozen nuclear warheads if the mobile target is able to access multiple roads or go off road after receiving warning of an attack.³³ Alternatively, updated target location information could be transmitted to the missiles or warheads while they are in flight. But this opens up the possibility that adversaries could employ countermeasures to prevent or interfere with in-flight retargeting, perhaps even diverting the warhead. Concern about the possibility of such countermeasures has prevented the United States from equipping its nuclear-armed ballistic and cruise missiles to receive information after launch. In addition, ballistic missile warheads currently have no capability to maneuver after they are released from the post-boost vehicle, about 10 minutes after launch. Thus, using the tracking information provided by space-based systems to attack mobile nuclear targets would require either a large force for a barrage attack or the development and large-scale deployment of new long-range missile systems.

In summary, emerging advances in small satellites and related sensor capabilities provide the means to strengthen several functions such as early warning and reliable command and control that are stabilizing. However, these advances also provide the means for persistent surveillance of an adversary's nuclear operations, threatening the survivability of second-strike forces. A capable adversary should be able to counter persistent surveillance and tracking through camouflage, concealment, and deception, but it is unclear whether such offsetting measures will be deemed sufficient without a buildup in offensive nuclear armaments.

Hypersonic weapons

The United States, Russia, and China are developing a new generation of hypersonic weapons – weapons that travel long distances through the atmosphere at speeds greater than five times the speed of sound (Mach 5).

³³See, for example, Charles L. Glaser and Steve Fetter, 'Should the United States Reject MAD?' *International Security* 41/1, 66.

Weapons under development include both cruise missiles and glide vehicles that are launched by ballistic missiles. Here we focus on hypersonic boost-glide vehicles (BGVs), which are launched by missiles into space but return to the atmosphere shortly after the end of the boost phase, using lift forces to sustain flight at high velocities and altitudes. Although the United States is focused on the delivery of conventional weapons over short to medium ranges, Russia and China are developing dual-capable systems that can deliver nuclear weapons, including over intercontinental ranges.

Many observers have reacted to the development of hypersonic weapons with alarm. In testimony before the U.S. Senate Armed Services Committee, Gen. Robert Ashley, Director of the Defense Intelligence Agency, stated, 'Developments in hypersonic propulsion will revolutionize warfare by providing the ability to strike targets more quickly, at greater distances, and with greater firepower'. Gen. Mark Milley, Chairman of the U.S. Joint Chiefs of Staff, referred to a Chinese test of a hypersonic weapon as 'very concerning' and said, 'I don't know if it's quite a Sputnik moment, but I think it's very close to that'.³⁴ Vice Chairman Gen. John Hyten raised the prospect that such weapons could provide the basis for a surprise nuclear first strike on the United States. Concerns have focused on four attributes of BGVs: speed of delivery; ability to maneuver; detection and tracking; and ability to evade missile defenses.

Speed

The term 'hypersonic' gives the impression that such weapons are faster than traditional delivery vehicles. While it is true that long-range bombers and cruise missiles have generally been subsonic or low supersonic (less than Mach 1.5), traditional ICBMs and SLBMs achieve speeds up to Mach 20. Although Gen. Hyten asserted that BGVs could reach targets faster than ballistic missiles,³⁵ the advantage is modest at best. A BGV can reach targets at long ranges 3 to 6 minutes faster than a reentry vehicle (RV) delivered by a ballistic missile on a minimum-energy trajectory (19 min v. 25 min at 6000

³⁴Sara Sorcher and Karoun Demirjian, 'Top U.S. general calls China's hypersonic weapon test very close to a "Sputnik moment"', *Washington Post*, 27 Oct. 2021.

³⁵In response to Sen. Shaheen, who asked 'how much time we have from the point at which those weapons might be launched until when they might land in the United States', Gen. Hyten replied, 'it is a shorter period of time. The ballistic missile is roughly 30 minutes. A hypersonic weapon, depending on the design, could be half of that, depending on where it is launched from, the platform. It could be even less than that'. U.S. Senate, Committee on Armed Services, 'Hearing to Receive Testimony on United States Strategic Command and United States Northern Command in Review of the Defense Authorization Request for Fiscal Year 2020 and the Future Years Defense Program' (Washington, DC: Alderson Court Reporting 2019), 36, https://armedservices.senate.gov/imo/media/doc/19-14_02-26-19.pdf.

km range; 28 min v. 31 min at 8500 km).³⁶ But nuclear states have long had to consider the possibility that adversaries might launch ballistic missiles on depressed trajectories, with faster arrival times. In fact, an ICBM RV delivered on a depressed trajectory would arrive 2 to 4 minutes *faster* than a BGV.³⁷ Thus, BGVs provide no new or unique capability for increased speed or decreased delivery time compared to the ballistic missiles that have been deployed for the last 60 years.

Maneuver

Traditional ICBM and SLBM RVs travel on predictable ballistic paths after being released from the final stage of the ballistic missile. In contrast, BGVs use aerodynamic forces to change direction over the long duration of their flight in the atmosphere. The ability to maneuver could be used for five possible purposes: to achieve higher accuracies in attacks against fixed targets; to attack targets that have changed position after the launch of the glide vehicle; to evade air and missile defense interceptors; to prevent target prediction; or to avoid over-flight.

It is important to note that maneuver capability has long been possible using maneuvering reentry vehicles (MaRVs), which use aerodynamic forces to maneuver during reentry. MaRVs were originally developed by the United States in the 1970s as a countermeasure to missile defenses but were not deployed because they were determined to be unnecessary to penetrate Soviet defenses. A MaRV was first deployed in the mid-1980s on the intermediate-range Pershing-II missile to achieve higher accuracies that would allow the use of a lower-yield warhead; that missile was eliminated as part of the Intermediate-range Nuclear Forces Treaty. A MaRV capability also was developed in the mid-2000 for the Conventional Trident Modification, to achieve the high accuracies necessary for the delivery of non-nuclear payloads against fixed targets; this was abandoned due to concerns that a Trident armed with conventional warheads might be mistaken for a nuclear attack. Although MaRVs have not been deployed on ICBMs and SLBMs, the important point is that maneuver capability sufficient for the first four of the purposes listed above has long been available and is not unique to BGVs. Furthermore, recent analysis by the Congressional Budget Office (CBO) notes that hypersonic weapons could cost one-third more than MaRVs of the same range deployed by ballistic missiles.³⁸

³⁶Cameron L. Tracy and David Wright, 'Modeling the Performance of Hypersonic Boost-Glide Missiles', *Science and Global Security* 28/3 (2020), 14.

³⁷Tracy and Wright, 'Modeling the Performance of Hypersonic Boost-Glide Missiles', 14.

³⁸Congressional Budget Office, *U.S. Hypersonic Weapons and Alternatives* (Washington, D.C.: Congressional Budget Office Jan. 2023), 2, <https://www.cbo.gov/system/files/2023-01/58255-hypersonic.pdf>.

Although MaRVs can execute maneuvers that change course by hundreds of kilometers, they do so only in the last minute of flight, after the RV has reentered the atmosphere. Because BGVs reenter the atmosphere much earlier, they can execute earlier and larger maneuvers. The capability to execute earlier and larger maneuvers may provide certain advantages. For instance, whereas a ballistic missile RV or MaRV launched from the continental United States against North Korea would necessarily overfly Russia, a BGV might avoid such overflight. But ballistic missile overflight could be avoided through the positioning of the launch platform (e.g., SSBN), and the dangers of overflight could be managed through notifications, so it is not clear that the large maneuvers made possible by BGVs would provide an important advantage.

Whereas the targets of traditional RVs can be predicted with reasonable accuracy 10 to 20 minutes before arrival, BGVs can create uncertainty about the intended target of an attack. A country facing a limited BGV attack may incorrectly believe the attack was directed against more valuable and strategic important targets that are within the maneuver footprint of a BGV. For example, a limited attack against an isolated industrial target intended to signal resolve might be misinterpreted as a possible decapitation attack against a key command and control facility or an attack against a nearby city. While this had led some observers to conclude that BGVs could be destabilizing because they might prompt a mistaken and unnecessarily escalatory response, the effect of target uncertainty is unclear. The dangers of target uncertainty emerge only if a country launches a retaliatory response on warning of attack, before the intended targets are known. This requires very rapid decisionmaking even if the targets are precisely known, giving rise to concerns about unwise or mistaken retaliation. To the extent that target uncertainty gives additional incentive to delay a retaliatory response, it could be a stabilizing factor. It also is worth noting that target uncertainty is not unique to BGVs; MaRVs would create similar uncertainty (albeit over a smaller footprint), as would cruise missiles and bombers (albeit over long flight times).

Detection and tracking

One difference between BGVs and traditional RVs is in detection and tracking. Both involve the launch of a ballistic missile, which can be detected and tracked by early warning satellites. RVs are released on predictable ballistic trajectories at high altitudes in space, where they can be detected and tracked at long distances by ground-based radars. By contrast, BGVs reenter the atmosphere soon after the boost phase and use lift forces to glide through the atmosphere to their targets. Although the much lower altitude path delays detection of BGVs by ground-based radar, friction with air heats the BGV to temperatures that are readily detectable by space-based infrared

sensors.³⁹ Although this is possible with current infrared sensors, the United States is developing new detection and tracking systems, including the Hypersonic and Ballistic Tracking Space Sensor (HBTSS).⁴⁰ BGVs would not avoid attack warning and tracking and therefore should not raise concerns about surprise attack or reduced warning time.

There is an important caveat. The United States maintains the option of launching its silo-based ICBMs on confirmed warning of an attack, before the ICBMs are destroyed by incoming warheads. This prevents an adversary from being confident that they could preemptively destroy U.S. ICBMs. Confirmation of attack is provided by radar detection of the incoming warheads, which confirms the warning provided earlier by satellites that detect the infrared signal from the missile launches. The requirement that an attack be confirmed by independent systems using different physical principles is known as ‘dual phenomenology.’ Under current U.S. doctrine, the launch-under-attack option for ICBMs can be exercised only if the attack is detected with both early-warning satellites and early-warning radars. It is assumed that Russia also maintains the option to launch its missiles on warning of an attack, but it is not known whether radar confirmation of satellite warning is required.⁴¹

As noted above, a BGV attack will be detected not only by the launch of the missile, but also by the infrared emissions of the BGV as it travels through the atmosphere towards its target. In both cases, detection and tracking are provided by satellites with infrared detectors. But radar detection of the BGV will occur much later. Even in the most favorable case for radar detection – a missile launched from the Russian ICBM base at Dombarovsky against the U.S. ICBM base at Minot, which almost directly overflies the U.S. early-warning radar at Thule – radar detection of the BGV will occur 9 minutes later than an RV on a minimum-energy trajectory.⁴² Because the BGV will arrive on the target 3 minutes earlier than the RV, the time available for a decision to launch U.S. ICBMs before impact by the Russian BGV is reduced by a total of 12 minutes. In order to ensure that all ICBMs can be launched before they are destroyed, the President must issue a decision to launch at least 9 minutes before the attacking warhead arrives. This leaves little time available for

³⁹Congressional Budget Office, *U.S. Hypersonic Weapons and Alternatives*, 2.

⁴⁰Jon Harper, ‘New SDA, MDA Missile-Tracking Satellites Launched into Space’, *DefenseScoop*, 14 Feb. 2024, <https://defensescoop.com/2024/02/14/sda-mda-missile-tracking-satellites-hbtss/>.

⁴¹Russian President Putin recently noted that “... Russia’s nuclear doctrine is based on the ‘launch on warning’ concept, which envisions nuclear weapons’ use in the face of an imminent nuclear attack spotted by its early warning systems. ‘When the early warning system receives a signal about a missile attack, we launch hundreds of missiles that are impossible to stop...’” See Amer Madhani and Tara Copp, ‘Putin Says Russia Could Adopt Us Preemptive Strike Concept’, *Associated Press*, 9 Dec. 2022, <https://apnews.com/article/putin-moscow-strikes-united-states-government-russia-95f1436d23b94fcbc05f1c2242472d5c>

⁴²Note that the RS-28 Sarmat could launch either RVs or BGVs against the United States via the Southern hemisphere, avoiding detection by north-facing early-warning radars.

a decision after radar confirmation: only 2 minutes for a BGV attack compared to 14 minutes for a ballistic RV on a minimum-energy trajectory.⁴³ This is the most favorable case for radar confirmation of a BGV attack; other trajectories would result in later radar detection, with less time remaining the BGV arrives on target.

The importance of the delayed radar confirmation is unclear. In order for this to be a serious concern, Russia (or perhaps China) would have to deploy hundreds of intercontinental-range BGVs in order to threaten most or all of the 400 U.S. ICBM silos. If this occurs, the United States might respond relaxing the requirement for radar confirmation to exercise the launch-under-attack option. It might instead require detection of both the missile launch and the BGV trajectories through the atmosphere. Although both would be based on detection by infrared sensors on satellites, the infrared signals would be very distinct and could be detected by different satellite systems, which might be considered adequate to confirm an attack with sufficient confidence to permit launch-under-attack.

Evading missile defense

Perhaps the most significant difference between BGVs and RVs is their vulnerability to interception by missile defenses, which probably is the primary motivation for the development of long-range nuclear BGVs by Russia and China. RVs on ballistic trajectories travel for most of their flight at high altitudes in space, where they can be engaged by midcourse missile defense interceptors that use infrared sensors to locate and home on the RV. But the midcourse missile defense systems that have been deployed by the United States to defend large areas cannot engage targets below 100 kilometers, because the heat generated at lower altitudes would blind the infrared sensors used to locate and home on the target warhead. Because BGVs have glide altitudes of 40 to 50 kilometers, they cannot not be engaged by the interceptors deployed as part of the U.S. Ground-based Midcourse Defense or the Aegis Sea-based Midcourse Defense systems.⁴⁴

BGVs might be vulnerable to terminal-phase interceptors that are designed to operate at lower altitudes, such as the Patriot Advanced Capability-3 system, particularly after the BGV has slowed to speeds that are lower than the interceptor. But the areas that could be defended by a terminal-phase system are relatively small. Although that might be adequate for the defense of high-value point targets, such as an airfield or aircraft carrier, it would not provide a basis for a regional or national missile defense against BGVs.

⁴³ Author's calculations.

⁴⁴ David Wright and Cameron Tracy, 'Hypersonic Weapons: Vulnerability to Missile Defenses and Comparison to MaRVs', *Science and Global Security* 31/3 (2023).

However, because BGVs are launched by ballistic missiles, they would be vulnerable to defensive systems that destroy missiles in their boost phase. Boost-phase defense is extremely challenging because the boost-phase is short (3–5 minutes) and takes place deep within an adversary's territory (for an ICBM) or over the open ocean (for an SLBM). This makes it difficult to position interceptors close enough to engage the missile during the boost phase. Although it might be possible to mount an effective boost-phase defense against missiles launched by a geographically small country, such as North Korea, no workable concept has been proposed that would permit a boost-phase defense against missiles launched from deep within Russia or China.⁴⁵

In summary, the deployment of hypersonic weapons should not negatively affect the survivability of nuclear forces and should not increase incentives for nuclear use or weaken nuclear deterrence. On the contrary, to the extent that BGVs can penetrate national missile defenses more effectively and reliably than traditional RVs and their associated countermeasures, they should strengthen deterrence and improve stability by providing additional confidence in second-strike retaliatory capabilities. This should, in turn, reduce the potential for arms racing and build-ups of offensive forces to offset missile defenses.

Machine learning

Recent advances in machine learning algorithms have fostered expectations of technologically-advanced weapon systems and warfare concepts capable of major impacts on international security. The Interim National Security Strategic Guidance issued by President Biden in March 2021 argued that 'the world's leading powers are racing to develop and deploy emerging technologies, such as artificial intelligence ... that could shape ... [the] military balance among states.'⁴⁶

Neural networks are one of the most promising and successful types of machine learning algorithms.⁴⁷ Neural networks are not a new concept; the first attempts date to the late 1950s. But early computers were not powerful enough to implement the large multi-layer networks needed to produce useful applications, and interest in the concept died out. This changed in the late 1990s, when multi-layer neural networks demonstrated the ability to recognize handwriting, such as postal addresses. Continuing improvements in GPUs made possible deep neural networks (DNN). A watershed moment was the 2016 demonstration of an algorithm that could defeat the human

⁴⁵Jaganath Sankaran and Steve Fetter, 'Defending the United States: Revisiting National Missile Defense against North Korea', *International Security* 46/3 (2022), 75–84.

⁴⁶President Joseph R. Biden Jr., 'Interim National Security Strategic Guidance', Mar. (Washington, D.C.: The White House 2021), 8, <https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf>.

⁴⁷Christian Szegedy et al., 'Intriguing Properties of Neural Networks', 19 Feb. 2014, 1, <https://arxiv.org/abs/1312.6199>; Nicolas Papernot et al., 'The Limitations of Deep Learning in Adversarial Settings', 2016 *IEEE European Symposium on Security and Privacy (EuroS&P)*, 2016, ...

champion in the game of Go – a feat that previously was thought to be decades in the future.⁴⁸ DNNs now exceed human performance in many tasks in benchmark tests.⁴⁹ Although DNNs often exhibit failures and vulnerabilities in real-world applications, many observers expect that these limitations will be overcome with time and experience.

The fundamental computing unit of DNNs are artificial neurons, that use several inputs to produce a single output.⁵⁰ A DNN comprises many neuron layers. In the learning or training phase, the DNN trains on very large quantities of labeled data to perform the desired classification task. For instance, a DNN attempting to classify cars, trucks, and boats would be trained on an extensive collection of image datasets of the three. Each node in the DNN is initialized with a random weight and then refined by repeatedly exposing the DNN to images of cars, trucks, or boats. The weights are adjusted via back-propagation and supervised learning until the output nodes generate an accurate classification of the inputs. It is expected that rigorous training will enable a DNN to ‘generalize the features underlying’ the object and correctly classify an image ‘not encountered during training.’⁵¹

Classification tasks are one of the most technologically mature functions performed by machine learning algorithms. A typical classification machine learning algorithm processes an array of information associated with several inputs and then sort these inputs into pre-designated classification categories.⁵² For instance, an email spam filter classifies emails as ‘spam’ or ‘not spam’ using the words in the email. In the case of mobile missile launchers, a classifier algorithm is expected to receive inputs of images of potential missile launcher-like vehicles spread across a wide geographical area to pinpoint the few actual nuclear missile launchers.

DNN algorithms have achieved high levels of performance in image and speech classification tasks powered by technological advances in GPU architectures.⁵³ AlexNet – an advanced DNN – is trained on 1.28 million

⁴⁸David Silver et al., ‘Mastering the Game of Go With Deep Neural Networks and Tree Search’, *Nature* 529, (27 Jan. 2016), 484–9.

⁴⁹Matthew Hutson, ‘Taught to the Test’, *Science* 376/6593 (6 May 2022), 570–3.

⁵⁰Shawn Recker and Christiaan Gribble, ‘Real-Time In Situ Intelligent Video Analytics: Harnessing the Power of GPUs for Deep Learning Applications’, *DSIAC Journal* 4/1 (Winter 2017), 36.

⁵¹Recker and Gribble, ‘Real-Time In Situ Intelligent Video Analytics: Harnessing the Power of GPUs for Deep Learning Applications’, 37.

⁵²Pedro Domingos, ‘A Few Useful Things to Know About Machine Learning’, *Communications of the ACM* 55/10 (Oct. 2012), 89.

⁵³On recent advances of Deep Neural Networks (DNN) in images and speech recognition, see Alex Krizhevsky, Ilya Sutskever, and Geoff Hinton, ‘Imagenet Classification with Deep Convolutional Neural Network’, *Advances in Neural Information Processing Systems* 25 (2012), 1106–14; Geoffrey E. Hinton et al., ‘Deep Neural Networks for Acoustic Modeling in Speech Recognition: The Shared Views of Four Research Groups’, *IEEE Signal Processing Magazine* 29/6 (2012), 82–97. For details on advances made in GPUs, see Recker and Gribble, ‘Real-Time In Situ Intelligent Video Analytics: Harnessing the Power of GPUs for Deep Learning Applications’.

images iteratively for 90 cycles within 2 hours.⁵⁴ If attempted with earlier computational architectures, the task would require at least six days.⁵⁵ More recently, other DNN such as VGGNet, ResNet, Inception, and DenseNet have demonstrated better capabilities in certain operational parameters.⁵⁶ As advances in GPUs have continued, progress in DNN and other machine learning efforts has been remarkable.⁵⁷

Machine learning algorithms and counterforce operations

The advances in GPUs and DNN algorithms have also impacted the national security operations of technologically advanced nation-states. The United States is leading efforts to apply AI and machine learning techniques to various military missions. The mission of tracking and targeting time-critical targets in a crisis has received significant attention. Project Maven, launched in 2017, used algorithms to analyze military drone footage to quickly identify targets in military operations in Iraq and Syria.⁵⁸ The NORTHCOM-led Global Information Dominance Experiments (GIDE) have tested AI and machine learning tools to recognize patterns across a variety of indicators to provide geostrategic warnings, such as the early detection of invasion troops assembling at a border region.⁵⁹ More recently, the U.S. military is embarking on a research effort to use machine learning techniques to anticipate the launch of a nuclear missiles by North Korea and other adversaries and track and target them in a crisis.⁶⁰ The research effort is directed at training algorithms to scour large amounts of satellite imagery and other data ‘with a speed and accuracy beyond the capability of humans’ to ferret out signs of missile launch preparation.⁶¹

⁵⁴Recker and Gribble, ‘Real-Time In Situ Intelligent Video Analytics: Harnessing the Power of GPUs for Deep Learning Applications’, 39. See also Alex Krizhevsky, Ilya Sutskever, and Geoffrey E. Hinton, ‘ImageNet Classification with Deep Convolutional Neural Networks’, *NeurIPS Proceedings*, 2012, <https://papers.nips.cc/paper/2012/hash/c399862d3b9d6b76c8436e924a68c45b-Abstract.html>.

⁵⁵Recker and Gribble, ‘Real-Time In Situ Intelligent Video Analytics: Harnessing the Power of GPUs for Deep Learning Applications’, 39.

⁵⁶Khush Patel, ‘Architecture comparison of AlexNet, VGGNet, ResNet, Inception, DenseNet’, *Inside AI*, March 8, 2020, <https://towardsdatascience.com/architecture-comparison-of-alexnet-vggnet-resnet-inception-densenet-beb8b116866d>; Siddharth Das, ‘CNN Architectures: LeNet, AlexNet, VGG, GoogleNet, ResNet and more ...’, *Medium*, 16 Nov. 2017, <https://medium.com/analytics-vidhya/cnns-architectures-lenet-alexnet-vgg-googlenet-resnet-and-more-666091488df5>

⁵⁷Mohit Pandey et al., ‘The Transformational Role of GPU Computing and Deep Learning in Drug Discovery’, *Nature Machine Intelligence* 4 (2022): 211–21, <https://doi.org/10.1038/s42256-022-00463-x>.

⁵⁸Cheryl Pellerin, ‘Project Maven to Deploy Computer Algorithms to War Zone by Year’s End’, U.S. Department of Defense 21 July 2017, <https://www.defense.gov/News/News-Stories/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/>.

⁵⁹Amy Hudson, ‘Revamping Homeland Defense’, *Airforce Magazine*, 2 Dec. 2021, <https://www.airforce-mag.com/article/revamping-homeland-defense/>.

⁶⁰Phil Stewart, ‘Deep in the Pentagon, a Secret AI Program to Find Hidden Nuclear Missiles’, *Reuters*, 5 June 2018, <https://www.reuters.com/article/us-usa-pentagon-missiles-ai-insight/deep-in-the-pentagon-a-secret-ai-program-to-find-hidden-nuclear-missiles-idUSKCN1J114J>.

⁶¹Stewart, ‘Deep in the Pentagon, a Secret AI Program to Find Hidden Nuclear Missiles’.

However, recent counterforce experiments in tracking missile launchers have also raised worrying red flags. A U.S. Air Force experimental AI target recognition program initially trained using data from a sensor that looked for a single surface-to-surface missile at an oblique angle. The target recognition program was performing well 'when all of the conditions were perfect, but a subtle tweak sent its performance into a dramatic nosedive'.⁶² The 'subtle tweak' was testing the program with data from a sensor tracking multiple missiles at a near-vertical angle. Even more problematic was the false confidence offered by the target recognition program. While the program was accurate 25% of the time, it claimed a 90% success rate.⁶³

Such false confidence in a real-world crisis with a nuclear-armed adversary would be highly problematic for decision-makers. Can machine learning algorithms be made highly accurate and robust when used against a capable adversary?

Machine learning algorithms and adversarial examples

DNN algorithms have been observed to possess intrinsic blind spots, particularly instability to small imperceptible 'adversarial' input perturbations.⁶⁴ These adversarial perturbations are often tested using computer-generated inputs that, in principle, could be mapped to the physical world. In some cases, researchers have also demonstrated adversarial physical systems, such as altered stop signs designed to fool automated cars.⁶⁵ Machine learning

⁶²Patrick Tucker, 'This Air Force Targeting AI Thought It Had a 90% Success Rate. It Was More Like 25%', *Defense One*, 9 Dec. 2021, <https://www.defenseone.com/technology/2021/12/air-force-targeting-ai-thought-it-had-90-success-rate-it-was-more-25/187437/>.

⁶³Tucker, 'This Air Force Targeting AI Thought It Had a 90% Success Rate'.

⁶⁴Szegedy et al., 'Intriguing Properties of Neural Networks', 2. For a brief technical discussion on what constitutes 'small' and 'imperceptible' in an adversarial perturbation, see Ali Shafahi et al., 'Are Adversarial Examples Inevitable?', February 3, 2020, 1, <https://arxiv.org/abs/1809.02104>.

⁶⁵For a survey of research on adversarial physical systems, see: Alexey Kurakin, Ian J. Goodfellow, and Samy Bengio, 'Adversarial Examples in the Physical World', ICLR 2017, <https://arxiv.org/abs/1607.02533>; Kevin Eykholt et al., 'Robust Physical-World Attacks on Deep Learning Visual Classification', 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, <https://ieeexplore.ieee.org/document/8578273>; Simon Thys, Wiebe Van Ranst, 'Fooling Automated Surveillance Cameras: Adversarial Patches to Attack Person Detection', 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, <https://www.computer.org/csdl/proceedings-article/cvprw/2019/250600a049/1iTvixAH5qo>; Jucheng Li, Frank Schmidt, and Zico Kolter, 'Adversarial camera stickers: A physical camera-based attack on deep learning systems', Proceedings of the 36th International Conference on Machine Learning, <https://proceedings.mlr.press/v97/li19j.html>; Yulong Cao et al., 'Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving', ACM Conference on Computer and communications Security (CCS), 2019, <https://arxiv.org/abs/1907.06826>; Daniel F. Smith, Arnold Wiliem, and Brian C. Lovell, 'Face Recognition on Consumer Devices: Reflections on Replay Attacks', *IEEE Transactions on Information Forensics and Security*, Vol. 10, No. 4, April 2005, <https://ieeexplore.ieee.org/document/7029643>; Huali Ren and Teng Huang, 'Adversarial Example Attacks in the Physical World', Machine Learning for Cyber Security, Third International Conference, ML4CS 2020, Guangzhou, China, October 8–10, 2020, <https://link.springer.com/conference/ml4cs>

experts have shown that by introducing adversarial examples, i.e., images with ‘imperceptible non-random perturbation’, they were able to alter a DNN machine learning algorithms prediction, forcing it to misclassify.⁶⁶ More importantly, the adversarial examples remain surprisingly robust and transfer across independently developed neural networks with differing characteristics.⁶⁷ Adversarial examples built using DNN machine learning algorithms transfer effectively not only to other DNN algorithms but also to other types of machine learning algorithms such as logistic regression, support vector machines, decision trees, nearest neighbors, and ensembles.⁶⁸ In other words, adversarial inputs demonstrate the ability to operationally generalize across a spectrum of machine learning algorithms.⁶⁹ These vulnerabilities of DNN algorithms should not come as a surprise. Misclassification errors by machine learning algorithms, including neural net classifiers, were a norm, not the exception, until a few years ago.⁷⁰

In addition to the observed *transferability* of adversarial attacks, recent research on machine learning algorithms has demonstrated that an adversarial input can be generated in a *black box* environment without access to the internal working of the algorithm or its training data.⁷¹ In a *black box* environment, adversaries can develop a substitute machine learning algorithm that solves the same classification task, test it using a synthetic dataset, and repurpose it to develop an adversarial example.⁷² In essence, the properties of *transferability* and a *black box* capacity to generate adversarial examples suggest that machine learning algorithms can, in principle, be fooled with very little direct information about the algorithm.⁷³ In other words, a technologically sophisticated adversary might be able to develop ways to defeat machine learning algorithms employed in counterforce operations without having a complete knowledge of the algorithm’s inner logic.

⁶⁶Szegedy et al., ‘Intriguing Properties of Neural Networks’, 2. Erica Klarreich suggests that adversaries can also systematically poison a machine learning algorithm during its training period. See Erica Klarreich, ‘Learning Securely: Because It Is Easy to Fool, Machine Learning Must Be Taught How to Handle Adversarial Inputs’, *Communications of the ACM* 59/11 (Nov. 2016), 12.

⁶⁷Szegedy et al., ‘Intriguing Properties of Neural Networks’, 2.

⁶⁸Nicolas Papernot, Patrick McDaniel, and Ian Goodfellow, ‘Transferability in Machine Learning: From Phenomena to Black-Box Attacks Using Adversarial Samples’, 24 May 2016, <https://arxiv.org/abs/1605.07277>.

⁶⁹See Ian J. Goodfellow, Jonathon Shlens, and Christian Szegedy, ‘Explaining and Harnessing Adversarial Examples’, March 20, 2015, 7, <https://arxiv.org/abs/1412.6572>.

⁷⁰Klarreich, ‘Learning Securely: Because It Is Easy to Fool, Machine Learning Must Be Taught How to Handle Adversarial Inputs’, 13.

⁷¹Nicolas Papernot et al., ‘Practical Black-Box Attacks against Machine Learning’, *ASIA CCS ’17: Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, Apr. 2017, 506–19; Szegedy et al., ‘Intriguing Properties of Neural Networks’.

⁷²Papernot et al., ‘Practical Black-Box Attacks against Machine Learning’; Szegedy et al., ‘Intriguing Properties of Neural Networks’. Papernot et al. Develop Their Adversarial Examples by Observing The Assigned Labels of a Machine Learning Algorithm Without any Knowledge of its Internal Structure.

⁷³Papernot, McDaniel, and Goodfellow, ‘Transferability in Machine Learning: From Phenomena to Black-Box Attacks Using Adversarial Samples’.

The possibility of such viable pathways to defeat classification machine learning algorithms demands caution in utilizing them for counterforce operations, especially against technologically advanced states such as Russia and China. It is also certainly possible that North Korea or Iran could receive direct and indirect assistance from the Russians or the Chinese in developing ways to fool American machine learning efforts at identifying, tracking, and targeting their missile launchers and other mobile targets.

It should also be noted that unintended and crude adversarial inputs can lead to algorithm failures. For example, in the 1991 Gulf War, the Patriot missile defense system's tracking and intercept program failed because the incoming missiles generated unexpected debris during reentry.⁷⁴ The Patriot system was designed to counter an advanced tactical ballistic missile. Instead, it was presented with a missile that was breaking up in flight and unintentionally producing effects that confused the missile defense system.⁷⁵ Eleven software modifications had to be developed and incorporated before the Patriot missile defense system was able to function against the target missiles.⁷⁶ There is insufficient time to make such operational tweaks during a nuclear conflict. Nuclear counterforce operations require high confidence in getting it right the first time.

Future possibilities in machine learning algorithm defenses

Several forms of defenses have been proposed to make machine learning algorithms robust against adversarial manipulation. However, several proposed defenses seem to have quickly fallen victim to adaptive adversarial attacks.⁷⁷ While defensive tactics of training machine learning algorithms with adversarial samples successfully defended against more direct attacks, they could not cope against multi-stage attacks.⁷⁸ Other proposed defensive

⁷⁴General Robert H. Scales, *Certain Victory: The US Army in the Gulf War* (Fort Leavenworth, KS: U.S. Army Command and General Staff College Press 1994), 183, <https://history.army.mil/html/bookshelves/resmat/desert-storm/docs/CertainVictory.pdf>.

⁷⁵Scales, *Certain Victory: The US Army in the Gulf War*.

⁷⁶Scales, *Certain Victory: The US Army in the Gulf War*.

⁷⁷Shafahi et al., 'Are Adversarial Examples Inevitable?', 2.

⁷⁸Shafahi et al., 'Are Adversarial Examples Inevitable?', 2. Robert Geirhos et al suggest that while machine learning algorithms performed well against adversarial distortions they were trained on, there will still be a tendency to failure when the algorithm was subject to previously unseen distortions. See Robert Geirhos et al., 'Generalisation in Humans and Deep Neural Networks', 21 Aug. 2017, 9, <https://arxiv.org/abs/1708.06131>. The authors compared the robustness of human perception against convolutional deep neural networks and report that 'DNNs trained directly on distorted images consistently surpass human performance on the exact distortion types they were trained on, yet they display extremely poor generalisation abilities when tested on other distortion types ... training on salt-and-pepper noise does not imply robustness on uniform white noise and vice versa'. See Shafahi et al., 'Are Adversarial Examples Inevitable?', 1. On adversarial training of machine learning algorithms, see also Takeru Miyato, Andrew M Dai, and Ian Goodfellow, 'Adversarial Training Methods for Semi-Supervised Text Classification', 16 Nov. 2021, <https://arxiv.org/abs/1605.07725>.

strategies have also been circumvented and defeated.⁷⁹ In a 2020 conference paper, machine learning researchers successfully demonstrate adaptive adversarial attacks against 13 recently outlined defensive strategies for machine learning algorithms.⁸⁰

Interestingly, the research indicates that neither the offense nor the defense can be assured of success. They note that for every proposed attack aimed at defeating a machine learning algorithm, there is a non-robust defense and vice versa.⁸¹ A truly universal defense or a comprehensive adversarial attack strategy remains undiscovered.

The publicly available literature on civilian research shows a strong effort to develop comprehensive defense and attack strategies. However, these efforts have become resource intensive, and results may be quite slow to emerge. In a study that explored the demands on computing power in five prominent areas of deep learning, suggest that continued progress is 'economically, technically, and environmentally unsustainable'.⁸² The study argued that continued performance improvements in deep learning techniques demand, at the very least, a squaring in computational power proportional to the number of data points.⁸³ Therefore, continued technological progress in deep learning will require changes to deep learning paradigms that increase performance without a corresponding increase in computing power.⁸⁴

Even in the absence of deliberate adversarial manipulation, algorithms may have to be extraordinarily accurate in order to effectively discriminate

⁷⁹Other defensive strategies include thermometer encoding, detection using local intrinsic dimensionality, input transformations, adversarial boosting, stochastic activation pruning, randomization at inference time, deploying generative models as defense, etc. See Anish Athalye et al., 'Synthesizing Robust Adversarial Examples', 7 June 2018, <https://arxiv.org/abs/1707.07397?context=cs>; Anish Athalye, Nicholas Carlini, and David Wagner, 'Obfuscated Gradients Give a False Sense of Security: Circumventing Defenses to Adversarial Examples', 31 July 2018, <https://arxiv.org/pdf/1802.00420>; Shafahi et al., 'Are Adversarial Examples Inevitable? On adversarial boosting to harden DNNs, see Alex Kantchelian, J. D. Tygar, and Anthony D. Joseph, 'Evasion and Hardening of Tree Ensemble Classifiers', 27 May 2016, <https://arxiv.org/abs/1509.07892>.

⁸⁰Florian Tramèr et al., 'On Adaptive Attacks to Adversarial Example Defenses', *Advances in Neural Information Processing Systems* 33, 2020, <https://proceedings.neurips.cc/paper/2020/hash/11f38f8ecd71867b42433548d1078e38-Abstract.html>.

⁸¹Tramèr et al., 'On Adaptive Attacks to Adversarial Example Defenses', 9.

⁸²Neil C. Thompson et al., 'The Computational Limits of Deep Learning', MIT Initiative on the Digital Economy Research Brief, 2020, 1, <https://ide.mit.edu/wp-content/uploads/2020/09/RBN.Thompson.pdf>. The five prominent areas of deep learning studied by the authors are image classification, object detection, question answering, named entity recognition, and machine translation.

⁸³Thompson et al., 'The Computational Limits of Deep Learning'. Jamie Sevilla et al identify three eras in the demand for computing power and the progress of machine learning research. They note that before 2010, training computational needs grew in line with Moore's law doubling roughly every 20 months. With the advent of deep learning algorithms in the early 2010s, they suggest that computational demands almost doubled every six months. Finally, the emergence of large-scale machine learning models in 2015 has spawned the need for 10 to 100-fold increasing in computing requirements. See Jaime Sevilla et al., 'Compute Trends Across Three Eras of Machine Learning', 9 Mar. 2022, <https://doi.org/10.48550/arXiv.2202.05924>.

⁸⁴Ibid., 3.

between targets (e.g., mobile missile launchers) and the many similar objects (e.g., trucks, buses, and other vehicles) operating in a given area. A machine learning algorithm that mistakenly identified other vehicles as mobile missile launchers with a probability of only 0.01% could generate about 100 false targets for every true targets.⁸⁵

Machine learning algorithms deserve more study and attention to understand their effects on nuclear damage limitation. As machine learning technologies evolve, their capabilities may present new opportunities for executing damage-limitation strikes. The current state of play, however, suggests technologically mature and determined adversaries can offset any vulnerabilities to their nuclear forces.

Cyber-attack

There are several hypothetical pathways through which cyber-attack capabilities can affect nuclear deterrence.⁸⁶ Cyber-attacks can be directed at the operational nodes of each of the three legs of a nuclear force – land-based nuclear missiles, ballistic missile submarines, and bombers. Cyber vulnerabilities of nuclear platforms have existed for several decades. In the 1990s, the U.S. Department of Defense (DOD) discovered an electronic backdoor that could be hijacked by unauthorized actors to transmit launch orders to its ballistic missile submarines.⁸⁷ Such vulnerabilities have persisted. The U.S. DOD, for instance, has identified mission-critical vulnerabilities to cyber-attack in several newer weapon systems.⁸⁸ These weapon systems include the Columbia-class ballistic missile submarines and Sentinel ICBMs.⁸⁹ It is equally plausible that weapon systems in Russia or China suffer similar vulnerabilities. These vulnerabilities may be exploited to weaken the retaliatory capabilities of a nuclear adversary.

Adversaries can also conduct cyber-attacks on nuclear command, control, and communications (C3) systems.⁹⁰ The effects of such cyber-attacks tend to

⁸⁵Christopher Clary, 'Survivability in the New Era of Counterforce', Chapter 6 in Vipin Narang and Scott D. Sagan (eds.), *The Fragile Balance of Terror: Deterrence in the New Nuclear Age* (Ithaca: Cornell UP 2022); Alan J. Vick, Richard M. Moore, Bruce R. Pirnie, John Stillion, *Aerospace Operations Against Elusive Ground Targets* (Santa Monica: RAND Corporation 2001).

⁸⁶A more comprehensive listing is provided in Jon R. Lindsay, 'Cyber Operations and Nuclear Escalation: A Dangerous Gamble', in *Nuclear Command, Control, and Communications: A Primer on US Systems and Future Challenges* (Washington, DC: Georgetown UP 2022).

⁸⁷Bruce Blair, 'Could Terrorists Launch America's Nuclear Missiles?', *Time*, 11 Nov. 2010, <https://content.time.com/time/nation/article/0,8599,2030685,00.html>.

⁸⁸U.S. Government Accountability Office, 'Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities', U.S. Government Accountability Office, 9 Oct. 2018, <https://www.gao.gov/products/gao-19-128>.

⁸⁹David E. Sanger and William J. Broad, 'New U.S. Weapons Systems Are a Hackers' Bonanza, Investigators Find', *The New York Times*, 10 Oct. 2018, <https://www.nytimes.com/2018/10/10/us/politics/hackers-pentagon-weapons-systems.html>.

⁹⁰There are a few cases of cyber-attacks on targets that might technically resemble nuclear C3 systems. The 2010 Stuxnet attack on the air-gapped Natanz uranium enrichment facility, 2012 cyber-attack on Saudi Arabia's Aramco, and a 2015 attack on Ukrainian energy companies are some of the prominent

be nonlinear and unpredictable. For instance, in the prelude to the Russian invasion of Ukraine, Russia managed to successfully execute a distributed denial of service (DDoS) attack against ViaSat modems to compromise their security and install the 'Acid Rain' malware that enabled it to render the modems unusable.⁹¹ Russia had hoped to disintegrate Ukrainian command and control and its ability to mount an effective defense against Russian forces. The effort failed and the Ukrainians managed to execute a robust defense against the Russian forces. Additionally, while more than 100 cyber-attacks against satellite infrastructure has been conducted in the war between Russia and Ukraine, none of them has been as sophisticated as the ViaSat attack, instead most of them have been brute force DDoS efforts.⁹² The absence of similarly sophisticated cyber incidents suggests that cyber-attacks against technologically sophisticated systems may be single-use instruments that work best when an attack is not anticipated.

However, the ViaSat cyber-attack does illustrate the possibility of disabling a communication system through cyber-attacks. Disabling nuclear C3 may, in theory, simultaneously render all three legs of a nuclear force incapacitated or leave them in significant disarray. If successfully executed, such attacks may hypothetically afford a highly potent way to limit damage in a nuclear exchange. For these reasons, decision-makers in the United States, Russia, and China have to contend with real and perceived vulnerabilities of their nuclear C3 systems. Perceptions of vulnerability by themselves might be manipulated to coerce adversaries during a serious crisis. An adversary could demonstrate that it can disable a critical nuclear C3 or weapon system and threaten to disable other systems if its demands are not heeded.⁹³ For instance, an adversary might demonstrate its ability to suppress the functioning of core elements of the national missile defense system and claim (or bluff) that the next move would be the disabling of nuclear weapons platforms. If the confidence of decision-makers has been compromised, hypothetically such threats may be used to end a conflict in preferential terms.

Cyber-attacks could also be used as force multipliers in large-scale conventional and nuclear strike campaigns to disarm a nuclear adversary. Cyber-attacks can blind air and missile defenses and facilitate strikes on nuclear platforms and other related targets. Such attacks have been demonstrated in a few instances against relatively weak adversaries. In 1995, a secretive unit

cases. See Jon Lindsay, 'Stuxnet and the Limits of Cyber Warfare', *Security Studies* 22/3 (2013), 365–404; Andrew Futter, *Hacking the Bomb: Cyber Threats and Nuclear Weapons* (Washington, DC: Georgetown UP 2018), 82–4.

⁹¹Christian Vasquez and Elias Groll, 'Satellite Hack on Eve of Ukraine War Was a Coordinated, Multi-Pronged Assault', *CyberScoop*, 10 Aug 2023, <https://cyberscoop.com/viasat-ka-sat-hack-black-hat/>.

⁹²Clémence Poirier, 'Trawling Hacker Forums Uncovers Crucial Information on Space Cyber Attacks', *Via Satellite*, October 30, 2024, <https://interactive.satellitetoday.com/via/november-2024/trawling-hacker-forums-uncovers-crucial-information-on-space-cyber-attacks>

⁹³Herbert Lin, *Cyber Threats and Nuclear Weapons* (Stanford, CA: Stanford UP 2021), 113.

within the Pentagon, J-39, used a CIA electronic bug to intrude into and disrupt the Serbian air defense network to aid the penetration of NATO aircraft into Serbian airspace. The CIA Information Operations Center had previously installed a bug at the central station of the Serbian phone line through which the Serbian air defense system communication was routed.⁹⁴ On the few occasions when NATO aircraft were attempting low altitude flight, J-39 operators hacked into the Serbian air defense system and misdirected with it false information.⁹⁵

Several years later, on 6 September 2007, Israel reportedly used cyber-attacks and electronic warfare techniques to facilitate a strike on a Syrian nuclear reactor. By late 2006, Israel had determined that North Korea was helping Syria build a Yongbyon-like nuclear reactor for the purpose of producing plutonium for a nuclear weapon.⁹⁶ The intelligence was obtained by installing a Trojan Horse program in the computer of a senior Syrian government official visiting London.⁹⁷ Israel decided to bomb the facility. The Israeli operation, codenamed Orchard, involved four Israeli F-15 jets destroying an unfinished Syrian nuclear reactor with a barrage of missiles and laser-guided bombs.⁹⁸ Israel's Unit 8200, a secret cyber warfare unit, had hacked Syria's new Russian air defense batteries and disrupted the data link between the radars and screens of the Syrian air defense operators.⁹⁹ The hacking blinded the Syrians and facilitated the Israeli strike operation without any losses of its aircraft. The hacking was reportedly performed by an airborne electronic warfare network attack platform called *Suter*.¹⁰⁰ A similar cyber-attack against air defense systems was considered by American military planners during the 2011 air strikes on Libya and the special forces raid that killed Osama bin Laden.¹⁰¹ It is conceivable that cyber-attacks may increase the ability of future stealthy autonomous vehicles to breach the territories of well defended states.

⁹⁴Fred Kaplan, *Dark Territory* (New York, NY: Simon & Schuster, 2016), 113.

⁹⁵*Ibid.*, 114.

⁹⁶David Makovsky, 'The Silent Strike: How Israel Bombed a Syrian Nuclear Installation and Kept It Secret', *The New Yorker*, September 10, 2012, <https://www.newyorker.com/magazine/2012/09/17/the-silent-strike>.

⁹⁷Erich Follath and Holger Stark, 'The Story of "Operation Orchard": How Israel Destroyed Syria's Al Kibar Nuclear Reactor', *DER SPIEGEL*, 11 Feb. 2009, <https://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html>.

⁹⁸Follath and Stark, 'The Story of "Operation Orchard": How Israel Destroyed Syria's Al Kibar Nuclear Reactor', 160.

⁹⁹Follath and Stark, 'The Story of "Operation Orchard": How Israel Destroyed Syria's Al Kibar Nuclear Reactor', 161.

¹⁰⁰Sharon Weinberger, 'How Israel Spoofed Syria's Air Defense System', *Wired*, October 4, 2007, <https://www.wired.com/2007/10/how-israel-spoof/>.

¹⁰¹In both cases, the cyber route was shelved for traditional kinetic attacks on air defense systems. See Eric Schmitt and Thom Shanker, 'U.S. Debated Cyberwarfare Against Libya', *The New York Times*, October 17, 2011, <https://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html>.

These various pathways may provide means to limit damage in a nuclear war but can also destabilize nuclear deterrence. During a crisis, benign cyber intelligence collection efforts might be assessed as the prelude to a first strike.¹⁰² Misinformation or misinterpretation of intelligence information may lead to such assessments by decision-makers navigating a tense stand-off.¹⁰³ If decision-makers believe their nuclear C3 system and weapons platforms have been compromised, even if the reality was different, the belief can set in motion highly destabilizing countermeasures.

Finally, inadvertent cyber targeting of nuclear C3 systems can occur in cases of integrated conventional and nuclear C3 systems.¹⁰⁴ Such integration can result from a variety of technological, operational, and economic reasons, and may not always be apparent to adversaries. Targets that otherwise appear legitimate in a limited conflict can assume strategic importance because of these integrations. For instance, targeting of dual-capable Chinese regional ballistic missile arsenal by the United States in a Taiwan conflict may be interpreted by Chinese decision-makers as a beginning of a disarming first strike.¹⁰⁵ Similarly, Chinese targeting of space-based early-warning satellites to degrade the performance of regional missile defense systems may be interpreted by American decision-makers as an attempt to blind American strategic early-warning and tracking capabilities.

In addition to these risks of destabilizing nuclear deterrence, it may also be very difficult to reliably test the effectiveness of cyber-attack capabilities against adversary systems in peacetime. Therefore, it seems unlikely that cyber-attack capabilities would significantly increase incentives to initiate preventive nuclear first strikes. But a nation that had already decided to launch a nuclear attack during a crisis might use unproven cyber-attacks to increase the likelihood of a successful attack and to limit damage from a retaliatory strike.

Quantum technology

Of the emerging technologies examined here, quantum technologies are the least mature and their applications are speculative. However, quantum technologies may possibly be the most consequential in the longer term. Quantum technologies exploit the special phenomena that govern matter and energy at the smallest scales. These include superposition – the fact that a particle can simultaneously be in more than one state – and entanglement –

¹⁰²Lin, *Cyber Threats and Nuclear Weapons*, 106–7.

¹⁰³*Ibid.*, 113. On the impact of social media, see Lin, *Cyber Threats and Nuclear Weapons*, 114–17; Futter, *Hacking the Bomb: Cyber Threats and Nuclear Weapons*, 78.

¹⁰⁴Lin, *Cyber Threats and Nuclear Weapons*, 108–9.

¹⁰⁵In a Taiwan conflict China's regional missiles will be significant threat to the United States and allied forces. See Jaganath Sankaran, 'Missile Wars in the Asia Pacific: The Threat of Chinese Regional Missiles and U.S.-Allied Missile Defense Response', *Asian Security* 17/1 (2021), 25–45.

the fact that the state of one particle can be linked with that of other particles, so that observing the state of one particle can provide information on the states of other particles. These special properties of quantum physics make possible new and potentially transformational applications, such as quantum computing, quantum communication, and quantum sensing.¹⁰⁶

Emerging quantum technologies rely on the ability to measure and control the quantum state of individual quantum systems or ‘qubits’. Qubits may be particles, such as neutral atoms, ions, electrons, or photons. For example, an electron qubit can be spin-up or spin-down. Qubits also can be created from structures that exhibit quantum states, such as a superconducting circuit or defects in a lattice structure. For example, a superconducting circuit can run in a clockwise or counterclockwise direction. A wide range of qubit technologies are being explored for various applications.

Quantum computing has received the most attention, because of the theoretical ability of quantum computers to solve problems that are infeasible for conventional computers. Because each qubit can simultaneously represent two logical states (0 and 1), a quantum computer with n qubits is equivalent to a conventional computer with 2^n bits (e.g., 100 qubits = 2^{100} or more than a million trillion trillion bits). In principle, this would allow quantum computers to solve extremely complex problems in reasonable amounts of time, such as factoring large prime numbers and accurately modeling chemical reactions, materials, and large systems.

Qubits are highly sensitive to minor perturbations and environmental factors, and it is challenging to maintain large numbers of qubits in superposition and entangled states. Decoherence, or loss of superposition and entanglement, leads to loss of information. Substantial effort is being devoted to developing systems with longer coherence times and error correction. Although prototype quantum computers exist, they are not yet capable of tasks that cannot be accomplished by conventional computers. It is not clear whether it will be possible to develop usable, full-scale, general-purpose quantum computers – and, if it is possible, whether it will take one or several decades.¹⁰⁷ Although quantum computers are likely to have important national security applications, such as breaking conventional encryption algorithms and extending the capabilities of machine learning, they are unlikely to have important impacts on strategic stability in the next 20 years.

Quantum communication holds the promise of extremely secure communication. The use of entanglement, in which the sender and receiver

¹⁰⁶Lindsay Rand, *Quantum Technology: A Primer on National Security and Policy Implications* (July 18, 2022); Michal Krelina, ‘Quantum technology for military applications’, *EPJ Quantum Technology* 8/4 (2021), <https://epjquantumtechnology.springeropen.com/track/pdf/10.1140/epjqt/s40507-021-00113-y.pdf>.

¹⁰⁷*Quantum Computing and Communications: Status and Prospects*, Oct. (Washington, DC: General Accountability Office, GAO-22-104422 2021).

exchange information via entangled particles, can eliminate the possibility of undetected eavesdropping. Quantum communication is at a relatively early stage of development. Although there have been prototype demonstrations, there are major challenges in exchanging information over long distances and at high data rates. Quantum communication is unlikely to have any impact on strategic stability in the next 20 years, although it may have applications in command and control in the longer term.

Quantum sensing takes advantage of the sensitivity of quantum states to environmental disturbances to measure physical properties, such as electric and magnetic fields, gravity, acceleration, and time. The extreme sensitivity of qubits, which is a liability for quantum computing and communication, can be harnessed to measure changes and variations that are much too small to be detectable by conventional sensors. Quantum sensing is more advanced than quantum computing and communication, and a number of qubit technologies have been demonstrated to measure various physical properties in laboratory settings.¹⁰⁸

To illustrate both the potential and the challenges of quantum sensing, consider one of the oldest quantum sensors, the superconducting quantum interference device (SQUID). The SQUID was invented in 1964 but it remains one of the most sensitive magnetometer technologies, able to measure fields as low as 1 femtotesla (fT), or fields 50 billion times smaller than the Earth's magnetic field. Arrays of SQUID detectors are used routinely in magnetoencephalography to map brain activity by measuring the tiny magnetic fields produced by the electric currents flowing in and between neurons (albeit with heavy shielding of the Earth's and other magnetic fields).

Submarines with steel hulls become magnetized in the Earth's magnetic field and also distort the Earth's field. Magnetometers have been used since World War II to detect magnetic anomalies from ships and submarines. This triggered efforts to reduce magnetic fields through periodic degaussing, internal devices, and non-magnetic hulls. There is almost no publicly available information about the effectiveness of such 'magnetic quieting' techniques, but it is commonly assumed that the magnetic field can be reduced by 95–99%. The residual magnetic field decreases with the cube of distance from the submarine, or by a factor of 1000 when the distance increases by a factor of 10. Conventional magnetometers, which have a sensitivity of about 1 picotesla, can detect an SSBN with low residual magnetism at a distance of a few hundred meters. But a SQUID that is 1000 times more sensitive could detect the submarine's magnetic field out to a distance of a few kilometers,

¹⁰⁸C.L. Degen, F. Reinhard, and P. Cappellaro, 'Quantum sensing', *Reviews of Modern Physics* 89 (July-Sep 2017), <https://journals-aps-org.proxy-um.researchport.umd.edu/rmp/abstract/10.1103/RevModPhys.89.035002>.

and a quantum magnetometer operating at the theoretical limits of sensitivity might extend this to 10 kilometers.¹⁰⁹

The extreme sensitivity of quantum sensors raises several issues. First, there is the issue of separating the tiny signal from environmental noise. The Earth's magnetic field varies constantly in time and space due to geophysical factors and the interaction of the solar wind with the Earth's magnetic field, and these fluctuations are many orders of magnitude greater than the SQUID sensitivity. Various techniques can be used to cancel this noise, including the use of detector arrays and signal processing techniques, but it would be challenging to achieve the level of reduction required to reliably detect signals that are much smaller than the noise. Second, there are a host of issues that would need to be resolved to transition technology from the laboratory to field operations, to allow quantum sensors to operate in a range of environmental conditions for extended periods without expert attention.

But even if these problems can be solved, quantum magnetometers would not make the oceans transparent or enable wide-area search. The ocean is vast; U.S. SSBNs can patrol an area of almost 300 million km² and remain within range of targets in Russia.¹¹⁰ Suppose that a reliable quantum sensor is available with a detection range of 5 kilometers. Continuous coverage of the entire potential patrol area would require millions of floating platforms. Just scanning the potential patrol area once per day would require 10,000 continuously operating UAVs or 100,000 UUVs.¹¹¹ To give a sense of the scale of such an enterprise, these are comparable to the total number of commercial airplanes in flight and ships at sea at any moment.

An array of quantum magnetometers with a range of a few kilometers could be used to detect submarines that pass through a choke point, such as the Luzon Strait. This might be useful for the detection of very quiet submarines that could not be detected by traditional acoustic sensors. Quantum magnetometers might also be used to track a very quiet submarine after it has been located, but there are two challenges. The first is identifying a suitable tracking platform. Tracking with an underwater vehicle would require a nuclear-powered UUV, because nothing else could match the endurance and speed of an SSBN. The second challenge is countermeasures. Hundreds or thousands of cheap magnetic decoys could be released for every

¹⁰⁹Lindsay Rand, personal communication, based on methods outlined in James A. Kuzdrall, 'Magnetometer Underwater Detection Range' (Nashua, NH: INTREL Service Company 11 July 2018), http://www.intrel.com/mea/mag/mea_app_mag_rng_sum.pdf. See also David Hambling, 'China's quantum submarine detector could seal South China Sea', *New Scientist*, 22 Aug. 2017, <https://www.newscientist.com/article/2144721-chinas-quantum-submarine-detector-could-seal-south-china-sea/>.

¹¹⁰The range of the Trident D5 with five warheads is 10,000 km (John R. Harvey and Stefan Michalowski, 'Nuclear Weapon Safety: The Case of Trident', *Science and Global Security* 4 (1994), 303; at a range of 10,000 km, the submarine operating area is 296 million km² (Patrick J. Friel, 'United States and Soviet Strategic Technologies and Nuclear War Fighting', in Robert L. Pfaltzgraff, Uri Ra'anan, Warren Milberg (eds.), *Intelligence Policy and National Security* (London: MacMillan Press 1981), 117.

¹¹¹Assumes UAV and UUV velocities of 120 and 12 km/hr, respectively.

SSBN. The decoys could mimic the magnetic signature of the SSBN or have much stronger and varying fields that would make it difficult to identify the weak signal of the SSBN.

Other quantum sensors are even less promising for tracking submarines. Quantum gravimeters might be able to detect the gravitational anomaly generated by an SSBN, and countermeasures against gravity detection would be very difficult, but detection ranges are on the order of hundreds of meters at best.¹¹² Quantum radar and lidar can in theory decrease noise and increase sensitivity by using entanglement to distinguish the photons reflected from a target from background photons. But even if the practical problems can be solved, which include storing entangled photons for later comparison with reflected photons, there are inherent limitations on the power of quantum radar and lidar, which provide an advantage over conventional approaches only when the number of photons is small. Such considerations led one radar expert to conclude that ‘quantum radar will never be deployed for long-range uses, such as tracking airplanes’.¹¹³ There may be short-range applications where small numbers of photons are sufficient, but even here quantum effects provide only a modest advantage. For example, one study estimated that a quantum lidar using blue-green photons could detect an underwater target at a range 70 meters greater than a conventional lidar of the same (extremely low) power.¹¹⁴ But it is much easier to increase range and sensitivity by increasing the power of a conventional radar or lidar.

Perhaps the most promising military application of quantum sensing is inertial navigation. Although GPS and other satellite systems provide excellent navigation services, with location uncertainties of less than a meter, there are situations in which satellite signals cannot be received (e.g., submerged submarines) and applications in which reliance on satellite navigation is undesirable because the GPS signal is vulnerable to jamming or spoofing (e.g., nuclear-armed ballistic and cruise missiles). Inertial guidance systems use measurements of acceleration, rotation, and time to calculate changes in location from an initial reference point, a process known as ‘dead reckoning’. Conventional inertial navigation technologies allow submarines to navigate between GPS updates and provide long-range ballistic missiles with accuracies of about 100 meters, but the accuracy degrades rapidly with time as small errors accumulate. Quantum sensors could make possible inertial guidance systems that would match the accuracy of satellite navigation, with much lower drift rates. Laboratory-scale quantum

¹¹²Marco Lanzagorta, Jeffrey Uhlmann, Salvador E. Venegas-Andraca, ‘Quantum Sensing in the Maritime Environment’, OCEANS 2015 - MTS/IEEE Washington, 2015, pp. 1–9, <https://ieeexplore.ieee.org/document/7401973>, estimate a detection range of 200 meters for a U.S. SSN with a 100-qubit noiseless quantum gravimeter; the larger mass and length of an SSBN would increase this to 300 meters.

¹¹³Adrian Cho, ‘The short, strange life of quantum radar’, *Science* 369 (25 Sept. 2020), 1156–7.

¹¹⁴Lanzagorta, op cit.

accelerometers and gyroscopes based on cold atoms have demonstrated extreme sensitivity.¹¹⁵ The main challenge is to reduce size and power requirements and improve stability and reliability so that systems could be installed on submarines, airplanes, and even missiles. There has been significant progress in this direction, and it seems likely that quantum inertial navigation will become practical within the next 10–20 years.¹¹⁶ And unlike the search and tracking problems examined above, there are no significant environmental factors or countermeasures that can interfere with inertial guidance.

If quantum navigation becomes possible on ballistic missiles and individual warheads, it could allow targeting accuracies on the order of a few meters without reliance on GPS, if the reentry vehicle was given the capability to maneuver in the terminal phase. This would allow large reductions in warhead yield – and perhaps even the use of conventional warheads – to destroy hardened targets, such as missile silos. Increasing accuracy by a factor of 10 allows yield to be reduced by a factor of 1000 while maintaining the same probability of destroying a hard target. Thus, nuclear weapons with yields of hundreds of kilotons could be replaced by sub-kiloton weapons. Yields in the sub-kiloton range could be provided with the primary stage of current two-stage strategic nuclear weapons, with the boost gas removed. The use of unboosted primaries would eliminate concerns about the reliability of nuclear weapons because most uncertainties are about the boost process and achieving a boosted primary yield sufficient to drive the secondary.

A 1000-fold reduction in yield would greatly reduce casualties from an attack. The area affected by blast would be 100 times smaller and the area receiving a lethal dose of radiation is more than 200 times smaller, for a 0.3-kiloton surface burst compared to a 300-kiloton surface burst.¹¹⁷ Whereas an attack against U.S. ICBM silos with current warheads might result in 1–7 million deaths (mostly from fallout),¹¹⁸ an attack against the same

¹¹⁵Donghui Feng, 'Review of quantum navigation', *IOP Conference Series: Earth Environmental Science* 237 (Febr. 2019).

¹¹⁶See, for example, 'This Device Could Usher in GPS-Free Navigation', *Sandia Labs News Release*, 26 October 2021, https://newsreleases.sandia.gov/quantum_navigation; Lee, J., Ding, R., Christensen, J. et al. 'A compact Cold-atom Interferometer With a High Data-rate Grating Magneto-optical Trap and a Photonic-integrated-circuit-compatible Laser System', *Nature Communication* 13/5131 (2022), <https://doi.org/10.1038/s41467-022-31410-4>; Bethany J. Little, Gregory W. Hoth, Justin Christensen, Chuck Walker, Dennis J. De Smet, Grant W. Biedermann, Jongmin Lee, and Peter D. D. Schwindt, 'A Passively Pumped Vacuum Package Sustaining Cold Atoms for more than 200 days', *AVS Quantum Science* 3/035001 (2021), <https://doi.org/10.1116/5.0053885>.

¹¹⁷Author's calculations based on methods outlined in Samuel Glasstone and Philip J. Dolan, *Effects of Nuclear Weapons* (Washington, DC: U.S. Department of Defense 1977), assuming 50% fission yield for 300-kt and 100% fission yield for a 0.3-kt surface burst.

¹¹⁸William Daugherty, Barbara Levi and Frank Von Hippel, 'The Consequences of "Limited" Nuclear Attacks on the United States', *International Security* 10/4 (Spring, 1986), 3–45 estimated 4–14 million early deaths and 1–8 cancer deaths from fallout resulting from a Soviet attack on targets; of this, 2–15 million deaths result from attacks on missile silos. Reductions in the number of targets would reduce the early deaths to 2–6 million, and total deaths from attacks on missile silos to 1–6 million. Reducing blast and fire deaths by a factor of 100 and radiation deaths by a factor of 230 would reduce total deaths from attacks on missile silos to 10,000 – 40,000.

targets with sub-kiloton weapons might result in only 10,000 to 40,000. This could have an effect on strategic stability by making certain large-scale counterforce attacks less apocalyptic and therefore more plausible. Attacks on area and deeply buried targets, such as bomber bases and command posts, would still require high-yield warheads, so a comprehensive counterforce attack would still result in several million deaths. The risk of escalation to attacks on cities with high-yield weapons would remain a powerful deterrent to counterforce attacks.

The strategic consequences of emerging technologies

Since the dawn of the nuclear age, emerging technological capabilities have affected the stability of nuclear deterrence. During the Cold War, fears that emerging technologies might offer the possibility of damage limitation or first-strike advantages catalyzed costly efforts to offset real and perceived vulnerabilities, triggered arms races, and in some cases motivated arms control agreements. As we enter a new era of strategic competition, the emerging technologies detailed above have reanimated questions about the stability of nuclear deterrence. Wisely managing the effects of these emerging technologies requires an understanding of their potential impacts. We reviewed five prominent emerging technologies – small satellites, hypersonic weapons, machine learning, cyber weapons, and quantum technologies – to understand their separate and combined effects on damage limitation and nuclear balance.

These five emerging technological capabilities, alone or in various combinations, will have mixed effects on nuclear deterrence. Small satellite constellations can create redundancies to vital nuclear C3 functions and eliminate critical vulnerabilities, strengthening strategic stability. Small satellites can also offer increased transparency to facilitate arms control verification and significantly reduce military surprises. However, persistent satellite surveillance, combined with autonomous vehicles equipped with sensors powered by machine learning algorithms to track and track targets, could make mobile missiles and bombers vulnerable to attack. Cyber-attacks could further enable the penetration of autonomous uncrewed combat aerial vehicles (UCAVs) into adversary territory by suppressing radars and air defense units.

Several next-generation UCAVs are being developed to obtain deep penetration capabilities. Lockheed Martin's Skunk Works is testing a new uncrewed aircraft system, Speed Racer, that is expected to operate in dense air defense systems environments.¹¹⁹ DARPA is exploring a new program called LongShot, envisioned as a drone that carries air-to-air weapons and

¹¹⁹Steve Trimble, 'Secretive New Skunk Works UAS Set For Ground Testing Soon', *Aviation Week Network*, 11 Feb. 2021, <https://aviationweek.com/defense-space/aircraft-propulsion/secretive-new-skunk-works-uas-set-ground-testing-soon>.

can be deployed from a manned platform from a standoff distance, thereby 'extending the range from which the military can defeat adversary defenses while protecting piloted vehicle at a safe distance'.¹²⁰ The design concept for LongShot envisions a plane launching the 'LongShot mothership' from a safe operating distance, and when the LongShot UCAV reaches near a target it in turn launches missiles at targets.¹²¹ However, these UCAVs are technologically still in an early experimental stage.¹²²

Similarly, underwater autonomous vehicles combined with other emerging technologies might facilitate the identification and tracking of ballistic missile submarines. DARPA's Submarine Hold at Risk (SHARK) project is one example of a UUV project that is intended to augment submarine tracking.¹²³ Similarly, DARPA's 'long-duration, long-range' Manta Ray UUV could, in the future, engage in submarine tracking.¹²⁴ It is conceivable that these UUVs when combined with quantum sensors and machine-learning algorithms would significantly augment U.S. capabilities in submarine tracking. Another example is a US Navy project that has tested small quadcopter that can be dropped from planes or helicopters, float on the ocean surface with sonar and other sensors, and then fly to track a ballistic missile submarine.¹²⁵ However, the operational use of these capabilities remains to be proven.

Cyber capabilities can offer new intelligence gathering opportunities that may provide transparency and have stabilizing characteristics but might also be employed to attack and disable nuclear platforms and C3 systems. Precision weapons and hypersonic missiles, which might one day use quantum sensors for ultra-precise inertial navigation, might make effective conventional or very-low-yield nuclear attacks possible against strategic nuclear targets, such as hardened missile silos. Such precision capabilities can have destabilizing effects. Advances in microelectronics, satellite sensors, and autonomous space vehicles might significantly improve missile defense,

¹²⁰Sara Sirota, 'DARPA Aims for LongShot Air-Launched Drone Flight Test in FY-24', *Inside Defense*, 23 Feb. 2021.

¹²¹Lee Ferran, 'DARPA's Aerial Turducken, the LongShot, Still Cooking towards 2022 Milestone', *Breaking Defense*, 24 Nov. 2021, <https://breakingdefense.com/2021/11/darpas-aerial-turducken-the-longshot-still-cooking-towards-2022-milestone/>.

¹²²Furthermore, the political, ethical, and legal ramifications of employing UCAVs and other autonomous weapons are still being explored. While these issues have been explored for automatic engagement of certain pre-selected narrowly defined targets under human supervision, completely autonomous engagement of a broad range of targets, including nuclear weapons related targets, poses severe legal and ethical complexities and escalation risks. See Jürgen Altmann and Frank Sauer, 'Autonomous Weapon Systems and Strategic Stability', *Survival* 59/5 (2017).

¹²³Andrew Reddie and Bethany Goldblum, 'Unmanned Underwater Vehicle (UUV) Systems for Submarine Detection', *CSIS: On the Radar*, 29 July 2019, <https://ontheradar.csis.org/issue-briefs/unmanned-underwater-vehicle-uuv-systems-for-submarine-detection-a-technology-primer/>.

¹²⁴Manta Ray UUV Prototype Completes In-Water Testing', DARPA: Defense Advanced Research Projects Agency, 1 May 2024, <https://www.darpa.mil/news-events/2024-05-01>.

¹²⁵David Hambling, 'Submarine-hunting drones take off and land on water vertically', *New Scientist*, 6 Apr. 2016, <https://www.newscientist.com/article/2083345-submarine-hunting-drones-take-off-and-land-on-water-vertically/>

which could be destabilizing if deployed by a revisionist power seeking first-strike advantages. Other technologies such as additive manufacturing, nano-technology, synthetic biology, and CRISPR gene-editing could interact with the five technologies discussed in the article and produce a diverging range of effects on strategic stability depending on the circumstances.¹²⁶

In a strategic competition among technologically advanced adversaries, it is unlikely that one state will be able to attain lasting advantages in damage limitation. Even if a state lags in one technological sphere, it will compete and seek out technological capabilities in other areas to offset its vulnerabilities. The scale of the technological competition and its effect on strategic stability will be accentuated by the nature of prevailing geopolitics and the collective ability to manage disagreements.¹²⁷ The 2022 U.S. National Defense Strategy observes that the United States and its allies ‘will increasingly face the challenge of deterring two major powers with modern and diverse nuclear capabilities – the PRC and Russia – creating new stresses on strategic stability’.¹²⁸ The concerns over deterring two near-peer adversaries could trigger the search for technological offsets that can offer the United States ways to preserve its nuclear deterrent against both rivals without having to increase its nuclear arsenal to maintain nuclear parity. Such efforts, however, may compromise strategic stability in the eyes of the Russia and China. Russia and China, in a 2022 joint statement, denounced ‘U.S. plans to develop global missile defence ... combined with the capacity building of high-precision non-nuclear weapons for disarming strikes and other strategic objectives’.¹²⁹ Renewed American efforts to gain substantial technological advantages will appear as an intolerable threat to Russia and China, both of whom are likely to believe that maintaining strategic parity with the United States is vital to their national security. If the emerging technology competition is to be wisely managed, it is necessary prudently to manage the emerging geopolitical differences and limit the role of the nuclear deterrent in resolving these differences.

Disclosure statement

No potential conflict of interest was reported by the author(s).

¹²⁶Krepinevich, *The Origins of Victory*, 86–87.

¹²⁷Krepinevich, *The Origins of Victory*, 145.

¹²⁸U.S. Department of Defense, ‘2022 National Defense Strategy of the United States of America. Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review’, Oct. (Washington, DC: U.S. Department of Defense 2022), 4, <https://www.defense.gov/News/News-Stories/Article/Article/3202438/dod-releases-national-defense-strategy-missile-defense-nuclear-posture-reviews/>.

¹²⁹In Their Own Words: Joint Statement of the Russian Federation and the People’s Republic of China on the International Relations Entering a New Era and the Global Sustainable Development, 4 Feb. 2022’, China Aerospace Studies Institute, Feb. 2022, <https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2022-02-04%20China%20Russia%20joint%20statement%20International%20Relations%20Entering%20a%20New%20Era.pdf>.

Funding

This work was funded through the Carnegie Corporation of New York.

Notes on contributors

Steve Fetter is a professor in the School of Public Policy at the University of Maryland.

Jaganath Sankaran is an assistant professor in the LBJ School of Public Policy at the University of Texas.

ORCID

Steve Fetter  <http://orcid.org/0000-0002-6589-2586>

Jaganath Sankaran  <http://orcid.org/0000-0002-9685-2595>

Bibliography

- Acton, James M., Thomas D. MacDonald, and Pranay Vaddi, 'Protecting the Valuables: Establishing Keep-Out Zones Around High-Altitude Satellites', in *Reimagining Nuclear Arms Control: A Comprehensive Approach* (Washington, DC: Carnegie Endowment for International Peace 2021), 61–70.
- Altmann, Jürgen and Frank Sauer, 'Autonomous Weapon Systems and Strategic Stability', *Survival* 59/5 (2017), 117–42. [10.1080/00396338.2017.1375263](https://doi.org/10.1080/00396338.2017.1375263)
- Athalye, Anish, Logan Engstrom, Andrew Ilyas, and Kevin Kwok, 'Synthesizing Robust Adversarial Examples', 7 June 2018. [10.48550/arXiv.1707.07397](https://arxiv.org/abs/10.48550/arXiv.1707.07397)
- Athalye, Anish, Engstrom Logan, Ilyas Andrew, and Kevin Kwok, 'Synthesizing Robust Adversarial Examples', Proceedings of the 35th International Conference on Machine Learning, June 2018, Stockholm, Sweden, 2018.
- Bescond, Pierre, 'Public Verification: The SPOT Satellite Technology', in Dietrich Shroerer and David Hafemeister (eds.), *Nuclear Arms Technologies in the 1990s* (New York: American Institute of Physics 1988), 149–164
- Biden, Joseph R., Jr., 'Interim National Security Strategic Guidance', Mar. (Washington, DC: The White House 2021).
- Blair, Bruce, 'Could Terrorists Launch America's Nuclear Missiles?' Time 11 Nov. 2010.
- Cao, Yulong, Chaowei Xiao, Benjamin Cyr, Yimeng Zhou, Won Park, Sara Rampazzi, Qi Alfred Chen, Kevin Fu, and Z. Morley Mao, 'Adversarial Sensor Attack on LiDAR-Based Perception in Autonomous Driving', *ACM Conference on Computer and Communications Security*, London, UK, 2019.
- Chapman, Bert, 'The Geopolitics of Rare Earth Elements: Emerging Challenge for U.S. National Security and Economics', *Journal of Self-Governance and Management Economics* 6/2 (2018), 76–77.
- Cho, Adrian, 'The Short, Strange Life of Quantum Radar', *Science* 369/6511 (25 Sep. 2020), 1156–57. [10.1126/science.369.6511.1156](https://doi.org/10.1126/science.369.6511.1156)
- Clary, Christopher, 'Survivability in the New Era of Counterforce,' Chapter 6', in Vipin Narang and Scott D. Sagan (eds.), *The Fragile Balance of Terror: Deterrence in the New Nuclear Age* (Ithaca: Cornell UP 2022), 171–173.

- Das, Siddharth, 'CNN Architectures: LeNet, AlexNet, VGG, GoogLenet, ResNet and More . . .', *Analytics Vidhya*, 16 Nov. 2017.
- Daugherty, William, Barbara Levi, and Frank Von Hippel, 'The Consequences of "Limited" Nuclear Attacks on the United States', *International Security* 10/4 (Spring 1986), 3–45. [10.2307/2538949](https://doi.org/10.2307/2538949)
- Decker, Audrey, 'Chinese Satellites are Breaking the US 'Monopoly' on Long-Range Targeting', *Defense One*, 2 May 2024.
- Degen, C. L., F. Reinhard, and P. Cappellaro, 'Quantum Sensing', *Reviews of Modern Physics* 89/3 (July-Sep. 2017). [10.1103/RevModPhys.89.035002](https://doi.org/10.1103/RevModPhys.89.035002)
- Domingos, Pedro, 'A Few Useful Things to Know About Machine Learning', *Communications of the ACM* 55/10 (Oct. 2012), 78–87. [10.1145/2347736.2347755](https://doi.org/10.1145/2347736.2347755)
- European Space Agency, 'ICEYE, the World's First SAR New Space Constellation' 20 Dec. 2021.
- Eykholt, Kevin, Ivan Evtimov, Earlene Fernandes, Bo Li, Amir Rahmati, and Chaowei Xiao, 'Robust Physical-World Attacks on Deep Learning Visual Classification', *IEEE/CVF Conference on Computer Vision and Pattern Recognition*, Salt Lake City, UT, 2018.
- Feng, Donghui, 'Review of Quantum Navigation', *IOP Conference Series: Earth Environmental Science*, Utah, USA, 237, Feb. 2019.
- Ferran, Lee, 'DARPA's Aerial Turducken, the LongShot, Still Cooking Towards 2022 Milestone', *Breaking Defense*, 24 Nov. 2021.
- Follath, Erich and Holger Stark, 'The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor', *Der Spiegel*, 11 Feb. 2009.
- Friel, Patrick J., 'United States and Soviet Strategic Technologies and Nuclear War Fighting', in Robert L. Pfaltzgraff, Uri Ra'anana, Warren Milberg (eds.), *Intelligence Policy and National Security* (London: MacMillan Press 1981), 98–128.
- Futter, Andrew, *Hacking the Bomb: Cyber Threats and Nuclear Weapons* (Washington, D. C.: Georgetown UP 2018), 82–84.
- Geirhos, Robert, Carlos R. Medina Temme, Jonas Rauber, Heiko H. Schütt, Matthias Bethge, and Felix A. Wichmann, 'Generalisation in Humans and Deep Neural Networks', *Proceedings of the 32nd International Conference on Neural Information Processing Systems*, Montreal, Canada, 21 Aug. 2017, 7549–61.
- Glaser, Charles L. and Steve Fetter, 'Should the United States Reject MAD?' *International Security* 41/1 (Summer 2016), 66.
- Glasstone, Samuel and Philip J. Dolan, *Effects of Nuclear Weapons* (Washington, DC: U.S. Department of Defense 1977).
- Goodfellow, Ian J., Jonathon Shlens, and Christian Szegedy, 'Explaining and Harnessing Adversarial Examples', 20 Mar. 2015. [10.48550/arXiv.1412.6572](https://doi.org/10.48550/arXiv.1412.6572)
- Grier, Peter, 'Rare-Earth Uncertainty', *Air Force Magazine*, 21 Dec. 2017.
- Gruss, Mike, 'MDA Kill Assessment Sensors Would Be Commercially Hosted', *Space News*, 20 Mar. 2015.
- Hambling, David, 'Submarine-Hunting Drones Take off and Land on Water Vertically', *New Scientist*, 6 Apr. 2016.
- Hambling, David, 'China's Quantum Submarine Detector Could Seal South China Sea', *New Scientist*, 22 Aug. 2017.
- Harper, Jon, 'New SDA, MDA Missile-Tracking Satellites Launched into Space', *DefenseScoop*, 14 Febr. 2024.
- Harris, Mark, 'SpaceX's Starlink Satellites Could Make US Army Navigation Hard to Jam', *Technology Review*, 28 Sep. 2020.

- Harvey, John R. and Stefan Michalowski, 'Nuclear Weapon Safety: The Case of Trident', *Science and Global Security* 4/3 (1994), 261–337. [10.1080/08929889408426405](https://doi.org/10.1080/08929889408426405)
- Hinton, Geoffrey, Li Deng, Dong Yu, George E. Dahl, Abdel-rahman Mohamed, and Navdeep Jaitly, 'Deep Neural Networks for Acoustic Modeling in Speech Recognition: The Shared Views of Four Research Groups', *IEEE Signal Processing Magazine* 29/6 (2012), 82–97. [10.1109/MSP.2012.2205597](https://doi.org/10.1109/MSP.2012.2205597)
- House Committee on Appropriations, 'Report of the Committee on Appropriations, Department of Defense Appropriations Bill', House Report 108-553, 2005.
- Hudson, Amy, 'Revamping Homeland Defense', *Air Force Magazine*, 2 Dec. 2021.
- Hutson, Matthew, 'Taught to the Test', *Science* 376/6593 (6 May 2022), 570–73. [10.1126/science.abq7833](https://doi.org/10.1126/science.abq7833)
- Ilyas, Andrew, Shibani Santurkar, Dimitris Tsipras, Logan Engstrom, Brandon Tran, and Aleksander Mądry, 'Adversarial Examples are Not Bugs, They are Features', *Proceedings of the 33rd International Conference on Neural Information Processing Systems*, Vancouver, Canada, Dec. 2019, 125–36.
- 'Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development, February 4, 2022', China Aerospace Studies Institute, Feb. 2022.
- Kantchelian, Alex, J. D. Tygar, and Anthony D. Joseph, 'Evasion and Hardening of Tree Ensemble Classifiers', *Proceedings of the 33rd International Conference on Machine Learning*, New York, NY, 48, 27 May 2016.
- Kaplan, Fred, *Dark Territory* (New York, NY: Simon & Schuster 2016).
- Klarreich, Erica, 'Learning Securely: Because it is Easy to Fool, Machine Learning Must Be Taught How to Handle Adversarial Inputs', *Communications of the ACM* 59/11 (Nov. 2016), 12–14. [10.1145/2994577](https://doi.org/10.1145/2994577)
- Krelina, Michal, 'Quantum Technology for Military Applications', *EPJ Quantum Technology* 8/1 (2021). [10.1140/epjqt/s40507-021-00113-y](https://doi.org/10.1140/epjqt/s40507-021-00113-y)
- Krepinevich, Andrew F., Jr., *The Origins of Victory: How Disruptive Military Innovation Determines the Fates of Great Power* (New Haven: Yale UP 2023).
- Krizhevsky, Alex, Ilya Sutskever, and Geoff Hinton, 'Imagenet Classification with Deep Convolutional Neural Network', *Advances in Neural Information Processing Systems* 25 (2012), 1106–14.
- Kurakin, Alexey, Ian J. Goodfellow, and Samy Bengio, 'Adversarial Examples in the Physical World', ICLR 2017. [10.48550/arXiv.1607.02533](https://arxiv.org/abs/1607.02533)
- Kuzdrall, James A., 'Magnetometer Underwater Detection Range', 11 July (Nashua, NH: INTREL Service Company 2018).
- Lanzagorta, Marco, Jeffrey Uhlmann, and Salvador E. Venegas-Andraca, 'Quantum Sensing in the Maritime Environment', OCEANS 2015 - MTS/IEEE (Washington, 2015), 1–9.
- Lavers, Christopher, 'The Origin of High Resolution Civilian Satellite Imaging, Chapter 1', in Christopher Lavers (ed.), *Recent Developments in Remote Sensing for Human Disaster Management and Mitigation* (Morrisville, NC: Lulu 2013), 1–5.
- Lee, J., R. Ding, and J. Christensen, 'A Compact Cold-Atom Interferometer with a High Data-Rate Grating Magneto-Optical Trap and a Photonic-Integrated-Circuit-Compatible Laser System', *Nature Communication* 13/1 (2022). [10.1038/s41467-022-31410-4](https://doi.org/10.1038/s41467-022-31410-4)
- Li, Jucheng, Frank Schmidt, and Zico Kolter, 'Adversarial Camera Stickers: A Physical Camera-Based Attack on Deep Learning Systems', *Proceedings of the 36th International Conference on Machine Learning*, Long Beach, CA, 2019.
- Lin, Herbert, *Cyber Threats and Nuclear Weapons* (Stanford, CA: Stanford UP 2021), 113.

- Lindsay, Jon, 'Stuxnet and the Limits of Cyber Warfare', *Security Studies* 22/3 (2013), 365–404. [10.1080/09636412.2013.816122](https://doi.org/10.1080/09636412.2013.816122)
- Lindsay, Jon R., 'Cyber Operations and Nuclear Escalation: A Dangerous Gamble', in James J. Wirtz and Jeffrey A. Larsen (eds.), *Nuclear Command, Control, and Communications: A Primer on US Systems and Future Challenges* (Washington, D.C: Georgetown UP 2022), 121–144
- Little, Bethany J., Gregory W. Hoth, Justin Christensen, Chuck Walker, Dennis J. De Smet, Grant W. Biedermann, Jongmin Lee, and Peter D. D. Schwindt, 'A Passively Pumped Vacuum Package Sustaining Cold Atoms for More Than 200 Days', *AVS Quantum Science* 3/3 (2021). [10.1116/5.0053885](https://doi.org/10.1116/5.0053885)
- Livingstone, Charles E., *RADARSAT-2 GMTI Demonstration Project* (Ottawa: Defense Research and Development Canada 2012).
- Madhani, Aamer and Tara Copp, 'Putin Says Russia Could Adopt US Preemptive Strike Concept', Associated Press, 9 Dec. 2022.
- Makovsky, David, 'The Silent Strike: How Israel Bombed a Syrian Nuclear Installation and Kept it Secret', *The New Yorker*, 10 Sep. 2012.
- 'Manta Ray UUV Prototype Completes In-Water Testing', DARPA: Defense Advanced Research Projects Agency, 1 May 2024.
- Miyato, Takeru, Andrew M. Dai, and Ian Goodfellow, 'Adversarial Training Methods for Semi-Supervised Text Classification', *International Conference on Learning Representations 2017*, Toulon, France, 16 Nov. 2021
- National Defense Space Architecture, Systems, 'Technologies, and Emerging Capabilities, Space Development Agency, Broad Agency Announcement', 13 Jan. 2022.
- Pack, Dee W., Brian S. Hardy, John R. Santiago, David Pietrowski, Jon C. Mauerhan, Paul F. Zittel, Darren W. Rowen, Cameron R. Purcell, Pradeep Thiyanaratnam, Lynette J. Gelinis, Paul K. Su, Joel Gussy, and Joseph M. Santiago, 'Flight Operations of Two Rapidly Assembled CubeSats with Commercial Infrared Cameras: The Rogue-Alpha, Beta Program', *35th Annual Small Satellite Conference*, Aug. 2021.
- Pandey, Mohit, Michael Fernandez, Francesco Gentile, Olexandr Isayev, Alexander Tropsha, Abraham C. Stern, and Artem Cherkasov, 'The Transformational Role of GPU Computing and Deep Learning in Drug Discovery', *Nature Machine Intelligence* 4/3 (2022), 211–21. [10.1038/s42256-022-00463-x](https://doi.org/10.1038/s42256-022-00463-x)
- Papernot, Nicolas, Patrick McDaniel, and Ian Goodfellow, 'Transferability in Machine Learning: From Phenomena to Black-Box Attacks Using Adversarial Samples', 24 May 2016. [10.48550/arXiv.1605.07277](https://arxiv.org/abs/1605.07277)
- Papernot, Nicolas, Patrick McDaniel, Ian Goodfellow, Z. Berkay Celik Somesh Jha, and Ananthram Swami, 'Practical Black-Box Attacks Against Machine Learning', *ASIA CCS '17: Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, Abu Dhabi, UAE, Apr. 2017, 506–19.
- Papernot, Nicolas, Patrick McDaniel, Somesh Jha, Z. Berkay Celik Matt Fredrikson, and Ananthram Swami, 'The Limitations of Deep Learning in Adversarial Settings', *2016 IEEE European Symposium on Security and Privacy*, Saarbrücken, Germany, 2016, 373.
- Patel, Khush, 'Architecture Comparison of AlexNet, VGGNet, ResNet, Inception, DenseNet', *Inside AI*, 8 Mar. 2020.
- Pellerin, Cheryl, *Project Maven to Deploy Computer Algorithms to War Zone by Year's End* July 2017. <https://www.defense.gov/News/News-Stories/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/>
- Planet, 'Planet Imagery Product Specifications', Dec. 2018. <https://assets.planet.com/docs/Combined-Imagery-Product-Spec-Dec-2018.pdf>

- Poirier, Clémence, 'Trawling Hacker Forums Uncovers Crucial Information on Space Cyber Attacks', *Via Satellite*, 30 Oct. 2024.
- Post, Joseph A. and Michael J. Bennett, *Alternatives for Military Space Radar* (Washington, DC: Congressional Budget Office 2007).
- Rainbow, Jason, 'Xona to Test GPS-Alternative Demo Satellite with Customer', *Space News*, 7 June 2022.
- Rand, Lindsay, 'Quantum Technology: A Primer on National Security and Policy Implications', 18 July (Livermore, CA: Lawrence Livermore National Laboratory 2022).
- Recker, Shawn and Christiaan Gribble, 'Real-Time in situ Intelligent Video Analytics: Harnessing the Power of GPUs for Deep Learning Applications', *DSIAC Journal* 4/1 (Winter 2017), 35–43.
- Reddie, Andrew and Bethany Goldblum, 'Unmanned Underwater Vehicle (UUV) Systems for Submarine Detection', CSIS: On the Radar, 29 July 2019.
- Ren, Huali and Teng Huang, 'Adversarial Example Attacks in the Physical World', Machine Learning for Cyber Security, Third International Conference, ML4CS 2020, Guangzhou, China, Oct. 8–10, 2020.
- Sanger, David E. and William J. Broad, 'New U.S. Weapons Systems are a Hackers' Bonanza, Investigators Find', *The New York Times*, 10 Oct. 2018.
- Sankaran, Jaganath, 'Limits of the Chinese Antisatellite Threat to the United States', *Strategic Studies Quarterly* 8/4 (Winter 2014), 20–47
- Sankaran, Jaganath, 'Missile Wars in the Asia Pacific: The Threat of Chinese Regional Missiles and U.S.-Allied Missile Defense Response', *Asian Security* 17/1 (2021), 25–45. [10.1080/14799855.2020.1769069](https://doi.org/10.1080/14799855.2020.1769069)
- Sankaran, Jaganath, 'Russia's Anti-Satellite Weapons: A Hedging and Offsetting Strategy to Deter Western Aerospace Forces', *Contemporary Security Policy* 43/3 (June 2022). [10.1080/13523260.2022.2090070](https://doi.org/10.1080/13523260.2022.2090070)
- Sankaran, Jaganath and Steve Fetter, 'Defending the United States: Revisiting National Missile Defense Against North Korea', *International Security* 46/3 (2022), 51–86. [10.1162/isec_a_00426](https://doi.org/10.1162/isec_a_00426)
- Scales, Robert H., *Certain Victory: The US Army in the Gulf War* (Fort Leavenworth, KS: U.S. Army Command and General Staff College Press 1994).
- Schmitt, Eric and Thom Shanker, 'U.S. Debated Cyberwarfare Against Libya', *The New York Times*, 17 Oct. 2011.
- Sevilla, Jaime, Lennart Heim, Anson Ho, Tamay Besiroglu, Marius Hobbhahn, and Pablo Villalobos, 'Compute Trends Across Three Eras of Machine Learning', 2022 *International Joint Conference on Neural Networks*, Padua, Italy, 9 Mar. 2022).
- Shafahi, Ali, Ronny Huang, Christoph Studer, Soheil Feizi, and Tom Goldstein, 'Are Adversarial Examples Inevitable?' 3 Feb. 2020. [10.48550/arXiv.1809.02104](https://arxiv.org/abs/1809.02104)
- Sherman, Jason, 'Navy Determines SPY-6 Radar Three Times Stronger Than Original Requirement', *Inside Defense SITREP*, 6 May 2019.
- Silver, David, Aja Huang, Chris J. Maddison, Arthur Guez, Laurent Sifre, George van den Driessche, Julian Schrittwieser, Ioannis Antonoglou, Veda Panneershelvam, Marc Lanctot, Sander Dieleman, Dominik Grewe, John Nham, Nal Kalchbrenner, Ilya Sutskever, Timothy Lillicrap, Madeleine Leach, and Koray Kavukcuoglu, 'Thore Graepel and Demis Hassabiset, "Mastering the Game of Go with Deep Neural Networks and Tree Search', *Nature* 529/7587 (27 Jan. 2016), 484–89. [10.1038/nature16961](https://doi.org/10.1038/nature16961)
- Sirota, Sara, 'DARPA Aims for LongShot Air-Launched Drone Flight Test in FY-24', *Inside Defense*, 23 Feb. 2021.

- Smith, Daniel F., Arnold Wiliem, and Brian C. Lovell, 'Face Recognition on Consumer Devices: Reflections on Replay Attacks', *IEEE Transactions on Information Forensics and Security* 10/4 (Apr. 2005), 736–45. [10.1109/TIFS.2015.2398819](https://doi.org/10.1109/TIFS.2015.2398819)
- Sorcher, Sara and Karoun Demirjian, 'Top U.S. General Calls China's Hypersonic Weapon Test Very Close to a 'Sputnik moment'', *Washington Post*, 27 Oct. 2021.
- Stefanick, Tom, *Strategic Antisubmarine Warfare and Naval Strategy* (Brookline, Massachusetts: Institute for Defense and Disarmament Studies 1987).
- Stewart, Phil, 'Deep in the Pentagon, a Secret AI Program to Find Hidden Nuclear Missiles', *Reuters*, 5 June 2018.
- Szegedy, Christian, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus, 'Intriguing Properties of Neural Networks' 19 Feb. 2014, [10.48550/arXiv.1312.6199](https://arxiv.org/abs/10.48550/arXiv.1312.6199)
- Temple, James, 'Everything You Need to Know About Skybox, Google's Big Satellite Play', *Vox*, 11 June 2014.
- Tereza, Pultarova. and Howell. Elizabeth, 'Starlink Satellites: Facts, Tracking, and Impact on Astronomy', <https://www.space.com/spacex-starlink-satellites.html>
- Thompson, Neil C, Kristjan Greenewald, Keeheon Lee, and Gabriel F. Manso, 'The Computational Limits of Deep Learning', *MIT Initiative on the Digital Economy Research Brief* (2020). [10.48550/arXiv.2007.05558](https://arxiv.org/abs/10.48550/arXiv.2007.05558)
- Thys, Simon and Wiebe Van Ranst, 'Fooling Automated Surveillance Cameras: Adversarial Patches to Attack Person Detection', *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*, Long Beach, CA.
- Tracy, Cameron L. and David Wright, 'Modeling the Performance of Hypersonic Boost-Glide Missiles', *Science and Global Security* 28/3 (2020), 135–70. [10.1080/08929882.2020.1864945](https://doi.org/10.1080/08929882.2020.1864945)
- Tramer, Florian, Nicholas Carlini, Wieland Brendel, and Aleksander Madry, 'On Adaptive Attacks to Adversarial Example Defenses', *Advances in Neural Information Processing Systems* 33 (2020). [10.48550/arXiv.2002.08347](https://arxiv.org/abs/10.48550/arXiv.2002.08347)
- Trimble, Steve, 'Secretive New Skunk Works UAS Set for Ground Testing Soon', *Aviation Week Network*, 11 Feb. 2021.
- Tucker, Patrick, 'This Air Force Targeting AI Thought it Had a 90% Success Rate. It was More Like 25%', *Defense One*, 9 Dec.2021.
- United Nations Office for Outer Space Affairs, 'Online Index of Objects Launched into Outer Space'. <https://www.unoosa.org/oosa/osoindex>
- U.S. Congressional Budget Office, *U.S. Hypersonic Weapons and Alternatives* (Washington, DC: Congressional Budget Office Jan. 2023).
- U.S. Department of Defense, '2022 National Defense Strategy of the United States of America. Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review', Oct. (Washington, D.C.: U.S. Department of Defense 2022).
- U.S. Government Accountability Office, 'Rare Earth Materials: Developing a Comprehensive Approach Could Help DOD Better Manage National Security Risks in the Supply Chain', Feb. (Washington D.C: Government Accountability Office, GAO-16-161 2016).
- U.S. Government Accountability Office, 'Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities', 9 Oct. (Washington, DC: Government Accountability Office, GAO-19-128 2018).
- U.S. Government Accountability Office, 'Quantum Computing and Communications: Status and Prospects', Oct. (Washington, DC: Government Accountability Office, GAO-22-104422 2021).

- U.S. Senate, Committee on Armed Services, 'Hearing to Receive Testimony on United States Strategic Command and United States Northern Command in Review of the Defense Authorization Request for Fiscal Year 2020 and the Future Years Defense Program' (Washington, DC: Alderson Court Reporting 2019).
- Vasquez Christian and Elias Groll, 'Satellite Hack on Eve of Ukraine War was a Coordinated, Multi-Pronged Assault', *CyberScoop*, 10 Aug. 2023.
- Vick, Alan J., Richard M. Moore, Bruce R. Pirnie, and John Stillion, 'Aerospace Operations Against Elusive Ground Targets' (Santa Monica: RAND Corporation 2001).
- Weinbaum, Cortney, Steven Berner, and Bruce McClintock, 'SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain', RAND, 2017.
- Weinberger, Sharon, 'How Israel Spoofed Syria's Air Defense System', *Wired*, 4 Oct. 2007.
- Williams, Ian, Masao Dahlgren, and Thomas G. Roberts, 'Boost-Phase Missile Boost-Phase Missile Defense: Interrogating the Assumptions', 24 June (Washington, DC: Center for Strategic and International Studies 2022).
- Wright, David and Cameron Tracy, 'Hypersonic Weapons: Vulnerability to Missile Defenses and Comparison to MaRvs', *Science and Global Security* 31/3 (2023), 68–114. [10.1080/08929882.2023.2270292](https://doi.org/10.1080/08929882.2023.2270292)