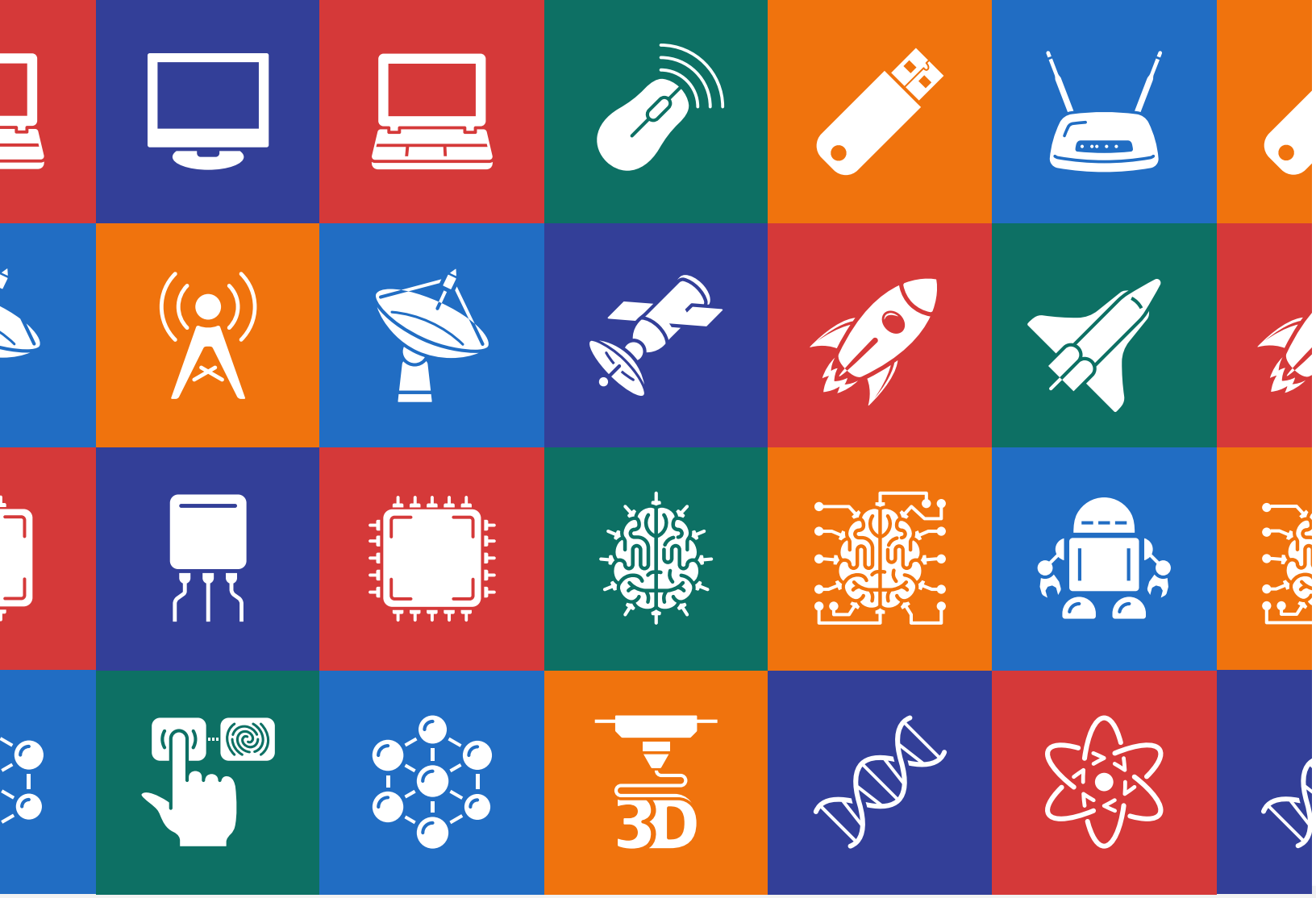

SPECIAL REPORT

Emerging Disruptive Technologies and Their Potential Threat to Strategic Stability and National Security

Christopher A. Bidwell, JD & Bruce W. MacDonald

FAS Federation of American Scientists

September 2018

About FAS

Founded in November 1945 by scientists who built the first atomic bombs, the Federation of American Scientists (FAS) is devoted to the belief that scientists, engineers, and other technically trained people have the ethical obligation to ensure that the technological fruits of their intellect and labor are applied to the benefit of humankind. The founding mission was to prevent nuclear war. While nuclear security remains a major objective of FAS today, the organization has expanded its critical work to address urgent issues at the intersection of science and security. FAS publications are produced to increase the understanding of policymakers, the public, and press about urgent issues in science and security policy.

Acknowledgements

This publication was developed under a grant awarded to FAS by the Institute for National Security Studies (INSS) at the United States Air Force Academy's (USAFA) Project on Advanced Systems and Concepts for Countering WMD No. FA7000-17-0012 contracted through the 10th Contracting Squadron (10 CONS/LGCC), with funding from the Defense Threat Reduction Agency (DTRA). It has not been formally reviewed by any of the aforementioned entities. Individual authors who may be FAS staff or acknowledged experts from outside the institution write these reports. Thus, the opinions, findings, views, conclusions or recommendations contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of FAS, USAFA, INSS, 10 CONS/LGCC, DTRA, or the U.S. government.

The authors are grateful for the opportunity to carry out this study and hope that the results will stimulate public debate among the academic, public policy, and nongovernmental communities, as well as the public in general. The U.S. government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright notation thereon.

The authors would like to express their deepest gratitude to those who participated in our workshop held on February 15, 2018 for their contributions of time and insight to help sort through a complex array of topics, as well as members of the faculty and staff at Massachusetts Institute of Technology's' Physics Department and the Belfer Center for Science and International Affairs within the John F. Kennedy School of Government at Harvard University, as well as numerous other specialists whom we consulted. Finally, we would like to thank the sponsors of this study at the U.S. Department of Defense, particularly the sponsors at INSS led by Dr. Jim Smith, whom we thank for their valuable oversight and suggestions with regard to this effort. Additionally, the authors are grateful for editing and logistical support from FAS employees Pia Ulrich and Frankie Guarini.

For more information about FAS or publications and reports, please call 202-546-3300, email fas@fas.org, or visit www.fas.org.

© 2018 Federation of American Scientists. All rights reserved.

Table of Contents

Executive Summary

This report seeks to identify and examine emerging technologies that have significant potential for substantially dangerous or disruptive effects on strategic nuclear stability in the national security arena and ways to address those impacts. Its methodology was to identify a list of candidate technologies for further examination, assess their potential to disrupt the deterrence calculus, and examine ideas, tools, and methods that could potentially ameliorate risks that use of these new technologies raises.

Before beginning the analysis, the report discusses what strategic nuclear stability means, both in terms of arms control and the broader strategic context. The report then discusses the nature of various types of threats to stability and ultimately makes recommendations for mitigating those threats.

To begin their analysis, the authors established a list of candidate technologies for consideration. While no list of this nature could ever be wholly complete, the authors established the following criteria for selecting those technologies that warranted further consideration:

- May reasonably come to fruition within 20 years
- Pose a significant challenge to one or more of the following:
  - Survivability of offensive strategic forces
  - Capability of defensive forces
  - Reliable functioning of strategic forces Command Control, Communications, Computers, and Intelligence (C4I)
  - Acceleration of crisis instability
- Not cost-prohibitive
- Potential to impose or enhance an existential threat
- Seriously enhance a nation's ability to manufacture a nuclear weapon undetected

Using these criteria, the authors identified seven separate technologies for further examination:

1. Laser isotope separation
2. Neutrino and anti-neutrino detection technology
3. High-energy lasers
4. Hypersonic strike technology
5. Artificial intelligence (AI) and big data analytics
6. Low-cost overhead persistent sensing technologies
7. Advanced cyber capabilities

After examining the impact of these technologies, the final task was to identify tools which could address the threats posed, or at least lessen their impact. Ideas such as treaties, export controls, lawfare, and norms-setting are discussed in the final section of the report. As part of this final task, certain tools are matched with appropriate new technological threats, as there is no one-size-fits-all solution to each of these potentially disruptive technologies.

Any one of these technologies appear likely to pose some challenge to strategic nuclear stability over the next 20-30 years, however it is the combination of a few of these technologies that appear to present a more demanding challenge to the strategic order than has prevailed in the nuclear realm for the last 60 years. This challenge arises from their potential to threaten the location uncertainty advantage and thus the survivability of strategic offensive nuclear forces. The ability of swarms of underwater drones to seek out submarine-launched ballistic missiles (SSBNs) and small satellites with advanced sensors to detect road-mobile intercontinental ballistic missiles (ICBMs) in a coordinated, intelligent, and remotely guided way represents a fundamentally new challenge to strategic offensive nuclear forces.

Certainly, countermeasures to this capability may be able to meet this challenge; this report claims no ironclad certainty that such a capability would be absolutely effective. As history has shown, however, just the realistic *possibility* of this capability can be enough to spur anxiety and hasty decisions that can destabilize the strategic environment. Certainly, it is better to address than to ignore such realistic prospects before they progress to the point where major powers begin to take destabilizing steps to address their concerns.

The specific concern would be if the United States, China, or Russia believed another among them was developing the capability to credibly localize adversary SSBN forces and/or road-mobile ICBMs (that is, to specify their location to within a small radius of a given point). This would call into question one of the country's ability to ride out an adversary's first strike. For purposes of this report the following definition for "strategic stability" will be used:

> A crisis can be defined as stable *if neither side has or perceives an incentive to use nuclear weapons first out of the fear that the other side is about to do so [emphasis in the original]* .... [and his] preferred definition of arms race instability is *the absence of perceived or actual incentives to augment a nuclear force — qualitatively or quantitatively — out of the fear that in a crisis an opponent would gain a meaningful advantage by using nuclear weapons first.*[1]

[1] James Acton, "Reclaiming Strategic Stability," in *Strategic Stability: Contending Interpretations*, eds. Elbridge A. Colby and Michael S. Gerson (U.S. Army War College Strategic Studies Institute: 2013), 117-118.

Introduction and Overview

For many years, the fundamentals of the strategic nuclear domain have remained largely constant, though with gradual, evolutionary changes over time. During the Cold War, both the United States and the Soviet Union had strategic nuclear forces consisting of ICBMs, SLBMs, and manned bombers. Each side had attained the ability to absorb a first strike and still retaliate with devastating effectiveness. Even after the fall of the Soviet Union, this condition continued to prevail. While newer technologies, such as improved missile guidance systems, stealth technology, and cruise missiles, introduced changes into the strategic equation, they did not fundamentally alter the dynamic of assured retaliation that lies at the heart of strategic stability.

Recent years have witnessed the continuing emergence of new technologies that have profoundly changed the non-military world; some of these technologies, in fact, have their roots in the defense technologies developed in previous decades, such as the integrated circuit, the internet, materials technology, and others. One important new element in this blossoming of technology is the massive amount of private investment that is taking place in these areas; the national security establishment can draw on these technologies without having to pay for more than specialized applications of them, along with some technologies unique to military. However, this also means that the military establishment has less ability to influence the development and control of these technologies. Consequently, our adversaries will have less difficulty in accessing these technologies than they may have had in the past.

It appears likely that the already prodigious level of technological innovation the world has witnessed over the last 20-40 years will continue to accelerate going forward, with the private sector playing a predominant role, and China playing a larger and more challenging role than ever before. The global race to develop, own, finance, dominate, and disseminate artificial intelligence and other emerging technologies will permeate the business competition of the future and further divide nations based on their ability to capture these gains in a competitive global landscape. Talent is critical—the United States needs to develop or attract the scientists, engineers, and creative talent to lead in this competition. China's drive to dominate these technologies of the future, including big data, quantum computing, artificial intelligence, and autonomous systems, is an economic, educational, and strategic challenge to the United States. The federal government needs to continue to be a driver of basic research, particularly as development of AI becomes a competitive race with nations such as China, which has massively increased its research funding[2] and plans to be a world leader in AI by 2030.[3]

In this brave new world that awaits us, it is possible that emerging technologies will lead to the development and deployment of new military capabilities that could undermine the strategic stability that we have taken for granted for many decades now. It is noteworthy that the Program on Advanced Systems and Concepts for Countering WMD (PASCC), identifies this issue in its most

[2] Council on Foreign Relations, "The Work Ahead," Independent Task Force Report No. 76 (2018), 63-64.
[3] Pablo Robles, "China plans to be a world leader in Artificial Intelligence by 2030," *South China Morning Post*, October 1, 2018, https://multimedia.scmp.com/news/china/article/2166148/china-2025-artificial-intelligence/index.html.

recent call for proposals, noting that such technologies could include blockchain technology development, artificial intelligence, 3D printing, human augmentation, quantum computing, synthetic biology, additive manufacturing, autonomous systems, and nanotechnology.

In light of this onrush of new technology, this report defines and describes what is meant by strategic stability and how it has evolved over the decades of the nuclear era; provides thumbnail sketches of seven new technologies, or combination of a few new technologies. that have at least some potential to disrupt strategic stability over the next 20 or so years; and finally, discuses in more detail the challenges posed to strategic stability, particularly by artificial intelligence and its related technologies, which this report sees as having potentially the greatest impact on strategic stability over the next 20 years.

Another source of instability within the next 20 years is not so much a specific technology but the growth of new capabilities in space and cyberspace already underway. Coupled with the lack of familiarity and experience with these domains, this could give our adversaries substantial incentives to strike first in a crisis with these weapons rather than holding back and trying to manage a ragged retaliation. The fact that space and cyber weapons are non-kinetic means that leaders may be tempted to believe that such moves would not be as escalatory as kinetic strikes, despite this not necessarily being true. With no space or cyber-equivalent to an assured nuclear second strike, the incentive to strike first in a crisis could be great indeed.[4] The vulnerability of both U.S. and Russian military forces to cyberattacks generate classic "first use" pressures. In other words, in the event of a crisis, knowing how vulnerable it is to a potential impending cyberattack, each side is incentivized to use its cyber-vulnerable capabilities first, or else risk losing them.

The implications of this logic are not limited to the cyber domain.[5] Nor are they limited to Russia, China being as much a concern in this regard as well. There will be strong incentives in a serious crisis for China to initiate and rapidly escalate attacks against U.S. space infrastructure. While China may not wish to initiate such attacks, it could feel compelled to strike in space before the United States does, rather than risk the far more dangerous alternative of striking second.[6] This same dynamic is pertinent in the cyber domain as well as the space domain.
In short, the world faces a new and highly dangerous pressures where, even if the dynamics of the environment are understood at a given point in time, technological change could easily upend that new understanding in a relatively short time. This report highlights just a few of the ways this could happen.

In light of these new realities the authors have set as the objectives of this study to:

a) provide, from an arms control perspective, a list and an analysis of emerging dangerous or disruptive technologies to strategic nuclear stability, with emphasis on Russian and Chinese potential adoption of these technologies;

[4] For further discussion of these issues, see: Bruce MacDonald et al., *Crisis Stability in Space*, Johns Hopkins University Foreign Policy Institute (2016), and James N. Miller and Richard Fontaine, *A New Era in U.S.-Russian Strategic Stability*, Center for a New American Security (2017).
[5] Miller and Fontaine, *op.cit.*, 30.
[6] MacDonald et al., *op.cit.*, 33.

b) analyze the adequacy of existing international regulatory regimes or arms control frameworks that would limit the technologies' use/trade/transfer; and

c) examine the adaptation of existing regulatory regimes or arms control frameworks to address their use/trade/transfer and suggest new regimes to capture their use/trade/transfer (and any foundational mechanisms required to establish such regimes).

What Is Meant by Strategic Stability?

Throughout the nuclear era, the term "strategic stability" has been often used but seldom defined. Authors mostly assume that their readers, particularly when the audience is a specialized one, inherently know what is meant by the term. Sometimes it is used strictly in reference to strategic nuclear weapons, sometimes in a larger strategic reference to overall nuclear and non-nuclear stability. During the 1960s, '70s, and '80s, analysts often considered strategic stability as consisting of crisis and arms race stability. Strategic stability was recognized even earlier by the mid-50s (in the United States at least)—that there was stability through mutual deterrence. Central to this concept was the idea that such stability depended upon the ability of a nuclear force posture to absorb a first strike and still be capable of retaliating with overwhelming force. In this way, a potential attacker would be dissuaded if that attacker also perceives such a counter capability. Such stability based on mutual deterrence is now what often passes for a definition of strategic stability, and while it is a fair approximation, it is still an incomplete one.

As James Acton, a British academic and scientist at the Carnegie Endowment for International Peace [7] notes: "strategic stability is—and always has been—a widely used concept without a common understanding." This has led, if anything, to an even less uniform understanding of the term. What is more, the bipolar world of the Cold War era is now about a quarter-century in the past, and today's multipolar world is more complicated. However, some facets of strategic stability appear to be enduring. An important dimension of strategic stability is what is now widely referred to as "crisis stability." This refers to that ability to absorb a first strike by an adversary and still be capable of retaliating with a highly destructive retaliatory strike, such that neither side would have any net incentive to initiate such an attack, even in a crisis. Often, this "crisis stability" concept is used interchangeably with strategic stability, but this does not capture other dimensions of the concept.[8]

Another dimension of strategic stability is the concept of what has been termed "arms race stability." In this concept, there is an absence of perceived or actual incentives to augment a nuclear force—qualitatively or quantitatively—out of the fear that in a crisis an opponent would gain a meaningful advantage by using nuclear weapons first.[9] When an offsetting weapon itself poses a sufficiently compelling threat to one country, it could well stimulate that country to deploy another offsetting weapon, and so on in a repeating action-reaction cycle that can be both expensive and destabilizing to all countries involved.

In this multipolar era, the impact of weapons posture and doctrine on multiple countries needs to be considered, including countries that may not have been the intended "targets" of such deployments, in what professor Greg Koblentz of George Mason University terms a "security trilemma": In what he calls this second nuclear age, "most nuclear weapon states face threats from two or more potential adversaries […] This gives rise to a security trilemma where actions taken by a state to defend against another state have the effect of making a third state feel insecure."[10]

---

[7] James Acton, "Reclaiming Strategic Stability," 117-118.

[8] See, for example, respected arms control author John Newhouse's discussion of stability: John Newhouse, *Cold Dawn: The Story of SALT*, Holt Rinehart Winston (1973), 20.

[9] *Ibid.*

[10] Greg Koblentz, *Strategic Stability in the Second Nuclear Age*, Council on Foreign Relations, Council Special Report No. 71 (November 2014).

U.S. homeland ballistic missile defense (BMD) is a prime example of the "security trilemma." U.S. defenses are designed against "limited" regional threats (e.g., Iran, North Korea), but Russia and China see BMD as a potential threat to their strategic deterrents. Thus, a fundamental problem for U.S. policy exists: How does the United States reassure both Russia and China about U.S. BMD intentions while meeting its important and legitimate strategic BMD needs? Strategic offense can play an analogous role, where offenses deployed to address one threat affect the deployment and strategic and other calculations of another country or countries.

Ted Warner, a former Assistant Secretary of Defense for Strategy and Requirements and well-known expert on nuclear arms control, deterrence, and other security-related topics, succinctly described strategic stability as being defined in three broad ways:

1. "Most narrowly, strategic stability describes the absence of incentives to use nuclear weapons first [this is the classic definition of crisis stability] … and the absence of incentives to build up a nuclear force (arms race stability)
2. More broadly, it describes the absence of armed conflict between nuclear armed states;
3. Most broadly, it describes a regional or global security environment in which states enjoy peaceful and harmonious relations."[11]

Warner's first definition is closest to what was the accepted definition of strategic stability during the Cold War. Acton goes on to modestly modify Warner's first definition of crisis stability and arms race stability—the narrowest of Warner's three definitions—in the following manner:

> A crisis can be defined as stable if neither side has or perceives an incentive to use nuclear weapons first out of the fear that the other side is about to do so [emphasis in the original] …. [and his] preferred definition of arms race instability is the absence of perceived or actual incentives to augment a nuclear force—qualitatively or quantitatively—out of the fear that in a crisis an opponent would gain a meaningful advantage by using nuclear weapons first.[12]

Acton's modification of the Warner definition is more precise and so will be the one this report will adopt as the primary definition of strategic stability.

As if this state of affairs was not already complex enough, new technologies with important strategic implications are further complicating our understanding of strategic stability. The relatively rapid emergence of the military's space and cyber capabilities add important new and complicating dimensions to our understanding of strategic stability. Even newer technologies such as artificial intelligence, big data analytics, swarm technology, and more continue to blur the distinctions between nuclear and non-nuclear strategic capabilities, further complicating our understanding of strategic stability and how it is affected in a crisis.

[11] James Acton, *op. cit.*
[12] James Acton, "Reclaiming Strategic Stability, 121.

What Are the Various Classes of "Threats" to Strategic Stability?

Inevitably, the quest for the next disruptive technology that will give one an upper hand against their adversaries is built into the fabric of conflict and war; it is unlikely to be abated. Yet, not all disruptive technologies should be characterized in a one-dimensional framework. In thinking about disruptive technologies in the context of strategic stability, it is helpful to distinguish among direct threats, indirect threats, unforeseen threats, intangible threats, and emerging threats to stability. All of these categories of threats, and their associated technologies, should be thought about differently if one is to deal with and mitigate their effects.

Direct threats are the easiest to conceptually see, understand, and anticipate. Consequently, they are susceptible to traditional strategic stability tools such as numerical limitations, capability governors, or range limitations that are established and maintained through treaties and agreements. An example of this would be limits on forward deployed missile ranges, such as those found in the Intermediate Nuclear Forces (INF) treaty. Another example would be the Strategic Arms Reduction Treaties (START) which parties, realizing that the race to acquire more warheads and delivery vehicles eventually drives up cost for all adversaries, made a conscientious decision to cap growth while maintaining and adequate number of weapons for their respective defense postures.

Indirect threats are asymmetric in nature and may be countered by theoretical concepts such as mutually assured destruction (MAD). In dealing with these kinds of threat, such as cyber warfare, it is necessary for nations to lay out clear redlines for potential adversaries and outline in clear language that state-disabling cyberattacks could be grounds for use of retaliatory nuclear forces (retaliatory policy).

Unforeseen threats are those that are not fully seen and understood, or whose significance is not fully appreciated. This makes them highly dangerous. An example of this kind of threat is al-Qaeda's use of airliners as cruise missile equivalents on 9/11. The abruptness and game-changing nature of these kinds of threats require highly adaptive responses. These are the threats that can overturn entrenched preconceptions, strategies, and doctrines. The issue with these threats is not simply a failure of imagination as some have posited.[13] Rather, there are so many possible combinations of potential unforeseen threats that it is impossible to allocate resources to deal with all of the potential outlier cases. The best defense against these types of threats is to have flexibility to respond built into one's defense posture and not have assets tied to or locked into preconceived notions of the threat environment.

Intangible threats are those that are not physical or readily identifiable but can strongly affect human thought and decision-making. While propaganda is not a new phenomenon, its effects are now enabled and multiplied by the internet and other forms of mass communication. Its power to conduct warfare in the adversary's head and freeze decision-making is monumental. The solution to this threat is to be counter aggressive and get into the adversary's decision-making process. Yet, at this time, U.S. information warfare is but a small fraction of the overall defense budget.

[13] "9/11 Commission Report," National Commission on Terrorist Attacks Upon the United States (July 2004), https://www.9-11commission.gov/report/911Report.pdf.

Emerging threats are those which are known or suspected, but not fully developed. An example of these types of threats could be seen in recent history. In the 1960s, it was apparent that the outer space domain would a ripe area for military use. Unfortunately, it was also apparent that the use of space for offensive and defensive military uses would be expensive. This led adversaries (notably led by the United States and the Soviet Union) to conclude treaties limiting the militarization of the space domain. These treaties were timely in that they addressed potential issues before any country had made significant investments in weapons or defenses that would lead them to want to protect the advantage gained through those investments. Furthermore, it is often hard to regulate use or pare back a system when there are potential career attachments and systematic bureaucratic equities related to those technologies have already incurred significant sunk economic costs.

Distinguishing Between a Disruptive and a Non-Disruptive Technology

All new technologies that come into use in warfare can be called "disruptive." In fact, the whole purpose of fielding a new technology is to change the status quo, whether in business, warfare, or any other societal endeavor. Under this standard, all new technologies could be considered "disruptive." The fundamental difference between disruptive and non-disruptive technologies is primarily a matter of degree (i.e., Does the new technology cross a line between evolutionary or revolutionary change to the status quo?).

For example, in World War II the concept of at-sea warfare was upended as naval battles were no longer confined to line-of-sight engagements. Furthermore, what were once considered invulnerable bases, such as Honolulu, Hawaii, could now be attacked from hundreds of miles away. The later development of jet engines and nuclear propulsion were improvements to carrier-based naval aviation but did not significantly change the new paradigm for naval conflict established during World War II. In this report, the authors have endeavored to discuss only developments that they see as revolutionary versus merely evolutionary, though in many cases this is a judgment call.

Another consideration is the fact that two or three technologies that improve tactical performance can combine to produce a revolutionary result that disrupts the strategic balance. An example of this emerging technologies phenomenon is the development of strategic bombing concepts during World War II. The initial conceived use of airplanes for military purposes was for observation and movement of enemy ground troops. In the early 20th century, the idea that an airplane could carry and drop bombs was tested and deployed in the later years of World War I; these were tactical improvements to fighting capabilities. However, a third technology, the Norden bombsight, came along, allowing for the strategic targeting of an adversary's industrial capability to manufacture weapons of war versus force-on-force engagements. This led to a new military strategy, as a much more precise and devastating use of daylight bombing on manufacturing capability was developed by the Allied Forces during World War II.

Entirely new and unforeseen technologies are certain to emerge over the next two decades that will further shape the strategic environment in ways we cannot foresee, perhaps requiring unforeseeable new control methodologies and regimes. The process is likely to be endless, but it is important to look ahead nonetheless and try to divine where we will be from a strategic stability standpoint and how best to manage or control the technologies involved to promote stability. What follows is a description of seven candidate technologies reviewed by the report's authors:

Laser Isotope Separation

Background

One of the toughest scientific challenges has been to effectively—and inexpensively—separate a desired isotope, such as uranium-235 (U-235), of a chemical element from its remaining isotopes for nuclear weapons use. Traditionally, isotope separation has been performed through the techniques of gaseous diffusion and gas centrifuge. Over the past two decades, scientists have developed a different, more efficient technique called laser isotope separation (LIS). The technique is based on the fact that different isotopes of the same element, while chemically identical, absorb different colors of laser light. Therefore, a laser can be precisely tuned to ionize only atoms of the desired isotope, which are then drawn to electrically charged collector plates. This is shown schematically in Figure 1.

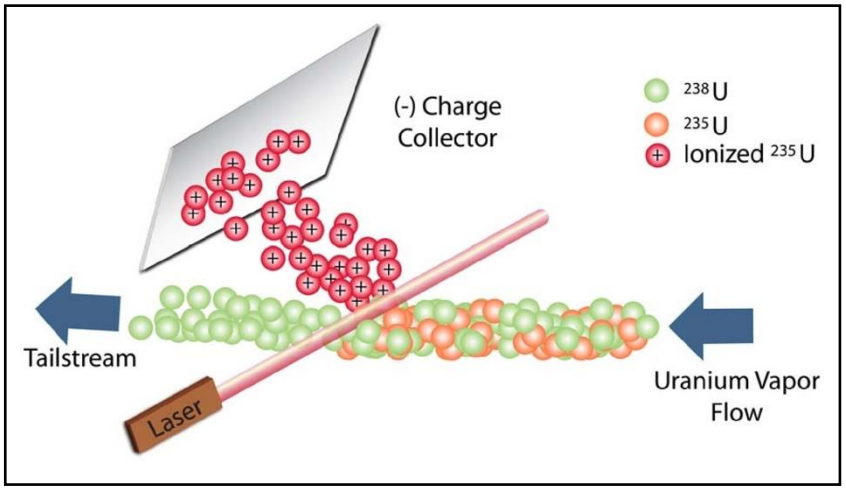

Figure 1. Conceptual configuration of Laser Isotope Separation. (Image/Nuclear Regulatory Commission)

LIS was originally developed in the 1970s as a cost-effective, environmentally-friendly technology to supply enriched uranium for nuclear power plants and special nuclear materials for national security needs. These same commercially appealing features also carry with them the potential for increasing nuclear proliferation. In the years since its early development, LIS has been refined and improved, though, at the same time, the cost of low-enriched uranium fuel has declined as well, seriously diminishing its economic prospects. GE Hitachi announced its intention to exit from a full-scale demonstration project two years ago,[14] which also has dampened its near-term prospects. The sale of its ownership share in Global Laser Enrichment, the vehicle for developing the technology, to an Australian company (Silex Systems) was abandoned in mid-2018 saying there were too many risks associated with the business case for the sale,[15] and significant economic and other issues remain.

Implications

The challenges of laser isotope separation are best put by the International Atomic Energy Agency (IAEA) in a report that calls out the rapid development of laser technologies in detecting

[14] World Nuclear News, 19 April 2016
[15] World Nuclear News, June 13, 2018

and safeguarding LIS facilities. The diffusion of knowledge about advanced laser technologies and optics, the development of new and improved laser systems and nonlinear optics, and the rapidly expanding market for these technologies make tracking LIS-related developments increasingly difficult. At the same time, detailed knowledge of LIS-related technologies remains relatively limited and may be decreasing over time as funding for declared LIS research is reduced. To maintain and develop its ability to detect, identify, and safeguard LIS-related activities, the IAEA must acquire and analyze a wide range of information, as well as conduct safeguards activities in a focused and information-driven manner. The comparatively small scale and relative absence of external indicators makes the remote detection of LIS-related activities difficult.[16]

For comparison with current technology, a proliferation-scale centrifuge facility can be housed in a Costco-size warehouse and run from a diesel generator. According to General Electric, an equivalent laser isotope enrichment facility would be one quarter of the size, use an unspecified lesser amount of energy and require fewer steps to produce highly enriched uranium. There would be no distinctive chemical or thermal emissions—making it difficult to detect a clandestine operation. To date, the Nuclear Regulatory Commission (NRC) has not performed a proliferation assessment of the technology, though the American Physical Society has called upon the NRC to perform such a review. An environmental impact statement has been performed but the NRC website does not list or indicate completion of a proliferation assessment.

It is estimated that with some laser enrichment and cascade designs, the efficiency could be five or more times greater, and possibly even higher, making even more difficult the possible detection of a clandestine laser enrichment facility based on size or energy use. The space required by a laser enrichment plant capable of producing about 30 kilograms per year of 90 percent enriched uranium (sufficient for more than one weapon a year) is estimated to be about 300 square meters. This estimate is almost certainly generous. Satellite surveillance intended to distinguish a building hosting such an activity among other buildings this size should not be expected to provide useful information.[17] Research on the relevant laser systems is also currently ongoing in Russia, China, and India.

Preliminary Assessment of Strategic Disruption

While this technology has troubling implications going forward, it does not appear to cross the threshold from troublesome to dangerous and disruptive.

Regulatory Control Regime Options

It would appear that regulatory control for LIS could be at least partially accomplished through either tight regulation of relevant users—a difficult proposition given the many different laser applications that exist. Under the Additional Protocol's more intrusive inspections regime, the additional access and information, according to IAEA, "allow a more complete and thorough investigation at the state level." However, obstacles remain; in particular:

[16] Denys Rousseau and John Lepingwell, "Isotopic separation by laser-based technologies: safeguards related aspects," International Atomic Energy Agency Paper Number: IAEA-CN-184/262 (2010).
[17] *Ibid.*

> [R]esearch programs on lasers relevant to third generation uranium enrichment may also be used for other applications that complicate identifying the intended purpose of equipment and programs. Attention needs to be focused on laser systems capable of enriching uranium to weapon-grade levels which may come to pose proliferation concerns comparable to if not greater than gas centrifuge development or plutonium reprocessing today.[18]

[18] Ryan Snyder, "A Proliferation Assessment of Third Generation Laser Uranium Enrichment Technology," *Science & Global Security* 24, no. 2 (June 2016), https://www.tandfonline.com/doi/full/10.1080/08929882.2016.1184528.

Antineutrino Detection Technology

Background

Operating nuclear reactors emit vast quantities of antineutrinos as a byproduct of nuclear fission, on the order of 10^26 per day.[19] Antineutrinos were previously undetectable and, even today, their detection is quite challenging. The ones emitted from plutonium fission have a lower average energy than from uranium, meaning that antineutrinos carry with them signature information about the amount and type of fissile material in the reactor core. So, by observing the spectrum, it is possible to determine the relative fraction of fissions that arise from plutonium, and this in turn can be used to work out the amount of plutonium that is in the core. However, detector sensitivities are still limited, and the entire energy distribution of the antineutrino spectrum from a reactor is unclear.[20]

Implications

Given that antineutrinos can travel unaffected through thousands of miles of lead, shielding their emission is not an option. This raises the possibility of detection of nuclear-powered submarines if some major technical hurdles could be overcome, chief among them being shrinking the size of the detectors while also allowing them to operate at some distance from the detector—both extraordinarily difficult tasks. Relatively recently, the coherent elastic scattering of neutrinos off nuclei has been effectively demonstrated at Oak Ridge National Laboratory, leading to a welcome miniaturization of detector size.[21] This coherent elastic neutrino-nucleus scattering (CENNS) occurs at a significantly higher rate than previously observed neutrino interactions—this scattering being observable. So, the idea is that CENNS might be used to track submarines using detectors that are much smaller than previous neutrino detectors.

In the very long run, there is some potential here for strategic disruption, but this is highly unlikely over the next 20 years. CENNS rates are, at most, a few thousand times higher than the rate of more conventional neutrino interactions (the exact enhancement factor depends on the CENNS detector material and the energy threshold of the detector). This is just not large enough to be a technological game-changer. At present, research suggests that the breakthroughs necessary to enable such a capability are nowhere near fruition, but it certainly seems possible that at least incremental improvements are likely.

The conventional interaction used to detect neutrinos from nuclear reactors is inverse beta decay, which could be seen in a water-based detector. The WATCHMAN experiment[22] is aiming to demonstrate that technique in the next few years. Antineutrinos rarely interact with anything, making them very difficult to detect, but it also means there is no known way to shield a reactor and prevent antineutrinos from flying out. With a 1-kiloton water detector, WATCHMAN expects to see about 5 neutrinos per day from a 4-megawatt reactor that is about 10 km away. Thus,

[19] Tushna Commissariat, "Using Antineutrinos to Monitor Nuclear Reactors," *Physics World*, August 12, 2014, https://physicsworld.com/a/using-antineutrinos-to-monitor-nuclear-reactors.
[20] *Ibid.*
[21] Dmitry Akimov, et al., "Observation of Coherent Elastic Neutrino-Nucleus Scattering, *Science*, August 3, 2017, http://science.sciencemag.org/content/early/2017/08/02/science.aao0990.
[22] "WATCHMAN," UC Davis Neutrino Group, accessed October 3, 2018, http://svoboda.ucdavis.edu/experiments/watchman.

if a CENNS detector has about 1,000 times the interaction rate, a 1-ton CENNS could see 5 neutrinos per day from a 4,000-MW reactor at 10 km. A submarine reactor is more like 400 MW, so one would need a 10-ton CENNS detector to see a few neutrinos per day from a submarine that is 10 km away.

Furthermore, ambient background radioactivity at the energy levels for reactor neutrinos vice the CENNS demonstration is much worse, making detection more difficult. Other background radiation rejection issues make this even more difficult.[23]

A 10-ton CENNS detector would be extremely difficult and expensive to build. In addition, there are many more background events that can mimic a CENNS signal, such as natural radioactivity in the detector materials and surroundings, cosmic rays, and neutrinos from the sun. The requirement to pick the submarine signal out from this large background would further increase the size demands on a CENNS detector, plus the movement of the submarine.

These considerations are likely sufficient to rule out CENNS as a revolutionary pathway for tracking submarines. One may still wonder if there is some other undiscovered neutrino interaction with an even higher rate than CENNS—perhaps some "macro-coherent" interaction in which the neutrino scatters coherently off an object larger than an atomic nucleus. However, an extensive literature search and discussions with physicists did not turn up any promising suggestions.[24]

Preliminary Assessment for Strategic Disruption

Highly unlikely though not impossible through 2040. Even the small possibility of a major breakthrough would have profound implications for stability given the central role that SSBNs play in strategic deterrence for the United States, United Kingdom, France, and, to some extent, Russia. Nonetheless, the technology should be pursued because of its direct relevance to monitoring nuclear reactors at close range for nonproliferation purposes.

Regulatory Control Regime Options

None needed at present. The technology should be examined periodically over the long term to determine whether multi-party control is possible without compromising the technology. In the meantime, scientific and technological development in this area should be subject to high secrecy classifications.

[23] Private communication, Professor Robert Svoboda, UC/Davis, USN Submarine Service (Ret.), June 24, 2018.
[24] Private communication, Dr. Rachel Carr, Pappalardo Fellow in the MIT Physics Department, Laboratory for Nuclear Science, December 2017 to January 2018.

High-Energy Lasers

Background

High-energy (H-E) lasers have been the subject of speculation for strategic weapons applications for decades. The challenge has always been how to deliver enough energy focused on the right spot on a ballistic missile. It is noteworthy that a ballistic missile is most vulnerable—and the technical challenge relatively less demanding—during the latter part of a missile's boost phase when all the warheads are still on the boosting rocket and not dispersed; the boosting missile's prominent infrared signature makes detection and tracking straightforward, and the missile is not fully up to speed yet. While H-E lasers have been under development for many years, advances in the last few years in solid-state lasers have increased prospects for practical weapons applications. H-E lasers would offer the potential of enabling low-cost, speed-of-light multiple shots, increasing the likelihood of destroying the missile.

Implications

If lasers in the 0.5–1-MW power range can be developed, multiple weapons applications would be possible, including at the strategic level. Applications of H-E lasers for boost-phase missile defense from aerial platforms—either unmanned aerial vehicles (UAVs) or aircraft—could be a serious challenge to fixed-base, highly "MIRVed" (multiple independently targetable reentry vehicle) ICBMs, such as Russia's SS-18 or successor ICBM, the SS-X-30. The U.S. Missile Defense Agency (MDA) is following a path of developing increasingly more powerful H-E lasers capable of being deployed on UAVs and other platforms,[25] with 30-, 60-, and 100-kW lasers planned for testing over the next four years. In addition, MDA plans to test a high-altitude drone likely in the 2020s with a 140–280-kW laser.[26] The plan is to take the power of the H-E laser system up over time to 150–300 kW, and eventually 500 kW. The Navy plans a test firing of a 150-kW laser in 2018.[27]

DARPA's High-Energy Liquid Laser Area Defense System (HELLADS) program is developing a 150-kW H-E laser weapon system with a weight goal of less than 5 kg/kW, approximately 750 kg, or 1650 pounds.[28] This will enable UAVs to carry the HELLADS, significantly increasing engagement ranges to hundreds of miles. Scaling this figure up from 150 kW to a power level of 1 MW, which approaches an ICBM lethality level, would require a laser of about 11,000 lbs., which becomes feasible for a large UAV. It should be emphasized that H-E lasers at this energy level would be unlikely to be feasible if space-based: size, weight, maintenance and other issues would make it quite difficult to achieve necessary performance and reliability levels. Ground- or air-based lasers would be more feasible sooner than space-based. A UAV could get closer to the launch point of an ICBM, especially for a country like North Korea.

[25] "New Dawn," *Aviation Week and Space Technology*, January 14, 2018, 76.
[26] James Drew, "MDA Advances Missile-Hunting UAV Programs," *Aviation Week and Space Technology*, March 11 2018, 41.
[27] Tom Waldwyn, "Fielding US Navy lasers: not quite speed-of-light," Military Balance Blog, IISS, February 8, 2018, https://www.iiss.org/blogs/military-balance/2018/02/us-navy-lasers.
[28] David Shaver, "High Energy Liquid Laser Area Defense System (HELLADS) (Archived)," DARPA, accessed October 3, 2018.

Preliminary Assessment of Strategic Disruption

The progression of H-E laser development into the multi-hundreds-of-kilowatts level will begin to make missile defense applications more feasible, at least for the boost phase. While countermeasures are possible, the development and deployment of such capabilities would be a source of great uneasiness to the major nuclear powers—not so much for its actual BMD capability as for what it would portend for the future. Countries would likely be seeking countermeasures of various kinds from an early start. Were space-based H-E lasers deployed, they would be early targets from hostile ground-based or other space-based H-E lasers in a deteriorating crisis environment, a destabilizing feature of such an environment. The non-nuclear dimensions of hypersonic technology are an important military concern, but long-range tactical strike does not seem likely to lead to a destabilizing strategic situation, at least not over the next 20 years.

Regulatory Control Regime Options

Were a regulatory regime deemed desirable for this technology, there are several approaches that could be taken. One would be to ban space-based H-E lasers because of their destabilizing characteristics. Another would be to limit the numbers of such systems that could be deployed, either ground or air vehicle-based, though this would run up against U.S. BMD policy of the last 16 years of resisting limitations such as this on BMD.

Hypersonic Strike Technology

Background

Hypersonics refers to speed regimes of five times the speed of sound (Mach 5) and higher. Recent interest in hypersonic weapons technology, beyond ballistic missile re-entry vehicles and other highly specialized applications, has centered on difficult-to-intercept hypersonic air-launched strike missiles that reach their targets quickly; and missile re-entry vehicles that maneuver in the upper atmosphere to make interception much more difficult. Recent advances in the areas of materials technology, guidance, control, and propulsion systems have started to address the exceptional thermal, pressure, and other technical challenges of hypersonic weapons, and have received growing attention. Hypersonics was one of five key game-changing technologies that the 2014 Air Force Master Plan identified, the others being nanotechnology, unmanned systems, autonomy, and directed energy.[29] There are claims that Russia and China are surpassing the United States in this technology,[30] though the United States government has recently reactivated its R&D spending in this area. Such claims must be weighed against the Air Force Scientific Advisory Board's 2015 finding that "hypersonic technology is probably not mature enough to field a recoverable hypersonic surveillance and strike aircraft before the early 2030s."[31] A more recent Air Force Chief Scientist assessment states that the Air Force will likely have some initial hypersonic weapons ready by sometime in the 2020s; the 2030s could see a hypersonic drone or ISR (intelligence, surveillance, reconnaissance) vehicle.[32]

Implications

The concerns about hypersonic weapons are that they are difficult to intercept because of their speed and maneuverability. While there has always been some interest in hypersonics, the technical challenges to successful weapons application have, in the past, been too daunting. If the speed of a hypersonic weapon launched from a stand-off platform can be combined with a high-accuracy and non-nuclear warhead, it becomes possible to envision a disarming first strike against adversary missile silos and other hard targets with very little warning that does not cross the nuclear threshold. In fact, the kinetic energy alone of the hypersonic weapon would deliver an equivalent explosive yield against a target even if it carried no warhead at all.[33] This would lead to a very compressed timeline for the targeted country's leaders, a prescription for rushed, and perhaps unwise, decision-making. In addition, maneuvering re-entry vehicles would pose a major challenge to re-entry-oriented missile defenses. Hypersonic missiles also increase the expectation of a disarming attack. Whether conventionally or nuclear-armed, hypersonic weapons threats encourage hair-trigger tactics by the targeted adversary that would likely increase crisis instability.

[29] "America's Air Force: A Call to the Future," U.S. Air Force.
[30] "U.S. Playing Catch-Up in Arms Race," *Washington Post*, June 10, 2018, p. E-1.
[31] *Aviation Week and Space Technology*, September 11, 2016, 47.
[32] Kris Osborn, "U.S. Air Force Chief Scientist Says Hypersonic Weapons Ready by 2020s," *The National Interest*, November 3, 2016.
[33] Richard H. Speier, George Nacouzi, Carrie Lee, and Richard M. Moore, "Hypersonic Missile Nonproliferation," RAND Corporation (2017).

Preliminary Assessment of Strategic Disruption

The potential for strategic disruption over the next 20 years appears to be mixed. Much has been made of the assessment by Strategic Command's General Hyten:

> We don't currently have effective defenses against hypersonic weapons because of the way they fly, i.e., they're maneuverable and fly at an altitude that our current defense systems are not designed to operate at. Our whole defensive system is based on the assumption that you're going to intercept a ballistic object.[34]

However, U.S. missile defenses are not currently designed to intercept traditional ICBMs of the type Russia and China possess; U.S. defense forces are sized to deal with smaller rogue threats, such as North Korea and Iran. Thus, for this particular application there is little net difference from a strategic stability point of view between current strategic weapons and weapons with maneuverable hypersonic warheads. The ability to use hypersonic strike missiles to carry out prompt, high-accuracy global strike missions with conventionally-armed warheads raises the possibility of non-nuclear attacks against missile silos; though we assess that such applications would likely be more than 20 years in the future. Technology developments should be monitored, but strategic disruption before 2040 should not be a significant worry.

While it is true that an additional layer of sensors in orbit could improve U.S. ability to intercept mixed ballistic/hypersonic nuclear weapons,[35] there is more to the story than that. Knowing where a hypersonic warhead is at any given moment is useful, but a defense system would need to know where the hypersonic warhead would be a minute or two later, something that is inherently unknowable if the hypersonic missile is maneuverable. In addition, if the United States seeks to defend against such an advanced hypersonic challenge, this could send a signal that the United States seeks to undermine the credibility of Russian and Chinese nuclear deterrents. Such actions would likely trigger a range of new countermeasures designed to defeat such defenses and preserve the longstanding credibility of Russian and Chinese strategic offensive forces, just as the United States would do if our nuclear force credibility were threatened. While the strategic disruption potential does not appear to be substantial, a hypersonic strike weapon with a conventional warhead for prompt global strike purposes would have significant tactical conventional potential for countries that possess them. It should be noted, however, that such a hypersonic weapon would be quite costly and would appear to be valuable only for use against very high-value targets that could justify its cost.

Regulatory Control Regime Options

None needed for the next 20 years, though the technology should be monitored. Should the threat develop faster than expected, a multinational ban on exports of hypersonic delivery vehicles and major hypersonic missile subsystems (e.g., hypersonic fuels and flight controls, supersonic combustion ramjet engines, warheads, etc.) would be useful. Hypersonic weapons could also be added to the list of weapons restricted by the Missile Technology Control Regime, with case-by-

[34] Testimony of General John Hyten before the Senate Armed Services Committee, March 20, 2018.
[35] Sandra Erwin, "Missile-tracking satellites are part of the plan to foil Russia's hypersonic weapons," Space News, May 20, 2018, https://spacenews.com/missile-tracking-satellites-are-part-of-the-plan-to-foil-russias-hypersonic-weapons.

case export reviews on underlying technologies.[36] Given the fact that significant investments have yet to be made by any country regarding this technology, it may be ripe for an arms control treaty solution.

[36] Richard H. Speier *et al., op. cit.*

Artificial Intelligence (AI) and Big Data Analytics

Background

Commercial entities and governments are investing major resources in developing artificial intelligence (AI) applications—which include the notion of machine learning and big data analytics—for a variety of tasks. The explosive growth in the amount of electronic data available for analysis bolsters the impact of AI, making it more useful in a variety of contexts. By 2020, analysts predict that the world will produce 44 trillion gigabytes of data annually,[37] an annual rate of growth of almost 60 percent. If sustained, this would lead to an annual data production of almost 450 quadrillion gigabytes of data. The sheer volume of data growth surpasses the human brain's ability to digest and comprehend what it is learning. Unsurprisingly, analytic methods, such as use of AI, to assess such large volumes of sensing and other data have made significant advances in recent years and appear to be accelerating, particularly in the commercial sector.

In her recent testimony before the Senate Foreign Relations Committee, the Undersecretary for Arms Control and National Security, Andrea L Thompson, noted that AI was a key emerging threat to strategic stability.[38] At the recent Aspen Strategy Group, AI was described as "the biggest technological challenge" facing the United States.[39] The growth in AI development is not limited to the United States. China has identified AI as a strategic priority. Last summer, China's State Council issued an ambitious policy blueprint calling for the nation to become "the world's primary AI innovation center" by 2030, by which time, it forecast, the country's AI industry could be worth $150 billion.[40] This likely includes all spending on AI, not just defense spending. In the words of one analyst, "the digital revolution is going to be the biggest geopolitical revolution in human history […] Every other twenty-first century geopolitical trend will look piddling by comparison."[41] AI will play a prominent role in this revolution.

One indication of AI's growing significance is the decision by DOD's Defense Innovation Unit Experimental (DIUx) made when making its first investment in space technology. It chose AI and machine learning over satellites, launchers, and even ground terminals.[42] In an echo of this action, it is noteworthy that France has recently made a commitment to advanced defense technology with its recent establishment of the Agency for Defense Innovation with a budget of $1.2 billion. It is headed by Emmanuel Chiva, a specialist in artificial intelligence, emphasizing the importance that France, a nuclear power, accords to AI.[43] Finally, Russian President Vladimir Putin has somewhat extravagantly claimed that that the country that "leads in AI will get to rule the world."[44]

---

[37] Jamie Vernon, "How Will Big Data and Artificial Intelligence Change Science?," Sigma Xi Speaks (May 2018).
[38] Andrea L. Thompson, testimony before Senate Foreign Relations Committee, September 19, 2018.
[39] David Ignatius, "A Sputnik moment for our military," *Washington Post*, August 8, 2018, p. A17.
[40] Christina Larson, "China's massive investment in artificial intelligence has an insidious downside," *Science*, February 8, 2018, http://www.sciencemag.org/news/2018/02/china-s-massive-investment-artificial-intelligence-has-insidious-downside.
[41] Kevin Drum, "Welcome to the Digital Revolution," *Foreign Affairs* (July-August 2018), 46.
[42] Irene Klotz, "Small Satellites, Big Data,"Aviation Week and Space Technology, July 30-August 19, 2018, p. 49.
[43] Pierre Tran, "Artificial intelligence expert gets top job at French defense innovation agency," Defense News, September 5, 2018, https://www.defensenews.com/industry/techwatch/2018/09/05/artificial-intelligence-expert-gets-top-job-at-french-defense-innovation-agency.
[44] "The Race for AI," Defense One, February 27, 2018, 12.

Implications

With the help of AI and machine learning, analysis can be produced with greater efficiency and speed, along with significantly reduced costs. This has numerous national security implications. First is AI's impact on passive surveillance operations; sensors may no longer be looking for an object in the noise but rather AI is being used to find a hole in the noise that would indicate the presence an object. This would apply to anti-submarine warfare and anti-air warfare. Second, the introduction of AI to the intelligence process is affecting the speed of analysis. For example, electro-optical change detection (EOCD) software is the first fully automated processing capability to work with panchromatic imagery, producing reliable detections, highlighting changes, and identifying second and third order indicators, thus saving analysts time and catching those changes that the human analysts working a manual process might not even have noticed. The result is a speeding-up of the process by which intelligence is acquired, analyzed, and acted upon. Furthermore, humans are now comfortably interacting with artificial intelligence in their daily operations. According to *Aviation Week*, "more than 80% of leading executives in defense and aerospace companies expect to see artificial intelligence systems working alongside their human employees in just the next few years." Use of AI in the workplace could soon be as innocuous as the use of smartphones is today.[45] A report to the director of the Intelligence Advanced Research Project Agency notes that "AI has demonstrated significant technical progress over the last five years, much faster than previously anticipated,"[46] and is expected to continue and accelerate.

The combination of AI and big data analytics already has substantial push for applications across the board, from resource development and oilfield operations to medical imaging and mineral detection. Startups, as well as established companies, have major financial incentives to exploit this technology, which will be available for advanced applications in the near future, over and above currently available capabilities. The extension of this, in conjunction with persistent surveillance capabilities, to the detection of deployed bulky transporter-erector-launchers carrying ICBMs, is an obvious potential application. One such firm is a deep learning company that specializes in using big data analytics to review large amounts of satellite and aerial imagery to pick isolated objects, some small, based on subtle clues in the imagery—and they have competition from others seeking to do similar things.

For the national security community, AI has important implications, not only for the impact of the AI technology itself, but also for the combination of AI with other technological developments related to offensive military operations (such as underwater drones, aerial drones, mobile missile launcher locations, antisubmarine warfare, counter-C3I, and the development of swarm tactics). On the offensive side, U.S. military leaders' and policymakers' assumptions about the stealthiest of platforms may have to be re-evaluated in light of the technological advances. Adjustments to the nuclear triad may be in order. The combination of advances in big data analytics and more advanced sensors could diminish the effectiveness of the different legs of the nuclear TRIAD over time. On the intelligence side, adversaries will likely have increased capabilities to spot each other's technological developments and, more importantly, detect deployed strategic forces (e.g., mobile ICBMs) despite the best attempts to hide them. AI and machine learning have been helpful in identifying facilities' developments early in their construction by matching

[45] *Aviation Week* Newsletter, April 3, 2018.

[46] Greg Allen and Taniel Chan, "Artificial Intelligence and National Security," Harvard Kennedy School, Belfer Center, July 2017, 1.

current imagery with the plethora of available past images of facilities of concern. Finally, the growth of big data sets and AI processing set the conditions for the possible development of autonomous weapon systems, but in our judgment would be unlikely to occur within the next 20 years to any significant extent. To some extent, this was foreshadowed by the Soviet development of the Dead Hand system in the latter stages of the Cold War,[47] a system built to ensure an automatic Soviet response to a U.S. nuclear first strike.[48]

Another dimension of AI that poses important challenges to strategic nuclear stability is the potential ability of AI to assist cyber operations in the disruption of command/control/communications for strategic nuclear forces. This is a high-priority mission for all the major nuclear powers, and it is difficult to imagine that AI-augmented cyber-disruption efforts would not pose a significantly greater challenge to all the nuclear powers.

One of the unique aspects regarding the development of AI is the fact that technological growth and innovation in the commercial sector significantly outpaces that of the military/national security sector. Commercially focused entities in this space are in a proverbial arms race with each other to gain a competitive edge. This is most notable in the search for AI talent. Salaries for highly qualified AI scientists and engineers in the Silicon Valley commercial sector can often top $1 million per year.[49] The fast-moving employee compensation structure is wildly out of sync with that of the heavily bureaucratized military/national security/defense industry. The implication of this discrepancy is twofold.

First, the government will likely lose the battle for top talent. Second, AI technology will be funded and developed primarily for commercial applications and uses. National security uses will be a secondary objective for businesses in the AI sector. Attempts to secure or restrict sales of emerging AI technologies on national security grounds will likely be met with great resistance from the commercial sector, especially from those companies that have made significant R&D investments in expectation of high monetary returns. Furthermore, there is cultural resistance from many of those technologists working in Silicon Valley to performing work for the US government in the intelligence and defense sectors. One recent example of this involves Google's decision to stop working on the DOD's Project Maven due to pressure and resistance from its employees.[50] The major financial incentive to develop big data analytics is from the commercial sector, so restrictions will be difficult to impose, much less to enforce. It is noteworthy that when a number of Google personnel objected to Google's contract with DOD under Project Maven, a controversial collaboration between U.S. military and private companies to train algorithms to analyze drone footage and identify targets of interest, Google withdrew from further work on the project. It is not unreasonable to conclude that Google had more to gain in balance from refusing to work on the military project than from maintaining that business.

[47] Nicholas Thompson, "Inside the Apocalyptic Soviet Doomsday Machine," *Wired*, September 21, 2009, https://www.wired.com/2009/09/mf-deadhand.
[48] See, for example, David Hoffman, *The Dead Hand*, Random House (2009).
[49] Cade Metz, "Tech Giants Are Paying Huge Salaries for Scarce A.I. Talent," *New York Times*, October 22, 2017, https://www.nytimes.com/2017/10/22/technology/artificial-intelligence-experts-salaries.html.
[50] Andrew Ross Sorkin, "Silicon Valley Doesn't Like Trump. It Can Still Work With the Government.," September 3, 2018, https://www.nytimes.com/2018/09/03/business/silicon-valley-trump-government.html.

Strategic Disruption

On the operational search side, an improved ability to locate stealthy platforms means the loss of a tactical advantage in the conventional realm. In the context of nuclear platforms, the loss could create a major strategic disadvantage and add to worries about strategic force survivability, especially during a crisis. Given the stakes, this will likely result in heightened competition in both military and commercial big data analytics, and in artificial intelligence more generally. On the intelligence side, the implication is that the use of big data analytics will drive down costs considerably as one analyst processing intelligence through AI can process analyze and develop strategic and tactical intelligence facts that may have taken hundreds of analysts and days' worth of time just 10 years ago. Big data analytics may also be more adept than humans at understanding cyberattacks and threats and even perhaps attributing the source of such attacks which can have positive impact on deterrence strategies related to cyber warfare.

Traditionally, strategic stability has involved offensive assets that are either hidden (e.g., SSBNs or stealthy cruise missiles) or protected (e.g., ICBMs contained in once-sufficient hardened silos). To the extent that confidence in this dynamic is diminished, major nuclear powers are thrust back into a "use or lose" world where they may feel major pressure to use their vulnerable nuclear forces first rather than have them destroyed by an adversary, vulnerable or not, that used its weapons first. The combination of artificial intelligence, persistent surveillance in the form of underwater drone sensors and constellations of imaging satellites, and big data analytics could represent a potent combination over the next 10-20 years.

A major validation of the importance of AI to DOD can be seen in the department's establishment of the Joint Artificial Intelligence Center (JAIC) with a specific mandate to explore and develop the agency's use of the "profoundly significant" technology that is artificial intelligence. [51]

Regulatory Control Regime Options

This is a case where the commercial sector is driving technological advances for business purposes and is moving faster than laws and regulations. This may be a case where regulation may emerge from the commercial sector's structure for preserving sensitive information and technologies versus the government's traditional classification and security paradigms. (See the final chapter of this report for discussion on the ways to control technologies in the commercial environment.)

[51] Tajha Chappellet-Lanier, "Pentagon's Joint AI Center is 'established,' but there's much more to figure out," *FedScoop*, July 20, 2018, https://www.fedscoop.com/dod-joint-ai-center-established.

Low-Cost Overhead Persistent Sensing Technologies

Background

Sixty years ago, the first overhead satellites were launched into space solely through government sponsorship (mostly the United States and Soviet Union). Initially, they could only produce low-resolution images that were rarely released to the public. Today, and into the foreseeable future, a significant number of satellites in orbit are owned and controlled by private entities and are producing data from various overhead sensor devices, including optical and multi-spectral. Satellite imaging is booming thanks to greater capacity in orbit, and improved image processing on the ground, and [all] for smaller investments to boot, with image quality rapidly improving. Excluding a growing number of satellites weighing less than 110 pounds, more than 600 observation satellites are expected to be launched by 2026.[52] The sheer number of commercial satellites in orbit (thousands) now ensures 360-degree pole-to-pole coverage and allows for some points on the planet to now receive nearly continuous coverage. Unlike legacy aerospace firms that focused on national security clients, these newer private firms are financially incentivized to sell their products to as many customers as they can, including foreign governments and NGOs. Furthermore, these newer enterprises are now fusing satellite imagery data with other data sources, such as social media and news feeds, allowing users to search for themes (e.g., geopolitical conflicts, energy resources, natural disasters) or obtain data feeds curated by location (e.g., ports, pipelines, borders). The result of all this growth the last few years has served to significantly lower the cost and volume of high-resolution imagery. This means that individuals or small groups can purchase images and order up new images for a few hundred dollars.

In addition to greater availability and lower costs, these advances in sensor technology, coupled with big data analytics, small satellite and drone technology, improved inter-satellite coordination, and other relevant technologies advance the prospect of maintaining a continuous monitoring capability over strategic targets of interest. This is in sharp contrast to the situation that existed over 20 years ago, where overhead imagery of important sites could only be taken every few days, if that. While such a capability would be of limited interest against silo-based ICBMs, SSBN bases, and strategic bombers, it could provide the basis for a more substantial capability to maintain a track of mobile ICBM launchers, even when they are flushed from their bases. Both Russia and China have turned to mobile ICBMs as an important means to ensure the survivability of their ICBM forces, given the vulnerability of fixed-base ICBMs to highly accurate ICBM and SLBM forces of the United States. In addition, the advent of technology enabling cooperating swarms of usually smaller vehicles designed to seek out targets holds the potential to change, even disrupt, submarine operations, including SSBNs. An important facet of this potential disruption is the combination of several new technologies, including artificial intelligence, new sensors, and big data analytics, the last being important to manage and process all the data that such swarms would provide. This could make submarine detection substantially less difficult than is currently the case. China has shown interest in swarm technology, though at present this appears to be limited to tactical applications.[53]

[52] "Argus Eyes," *Aviation Wee & Space Technology*, November 26, 2017, 29.
[53] *Aviation Week & Space Technology*, May 6, 2018, 46

Implications

The implications of these advancements are twofold, affecting both the policy community and military deterrence operations. On the policy side, the implications of having widely available, cheap, and high-quality imagery is that amateurs, NGOs, and small governments are now able to piece together plausible stories about world events (with varying degrees of accuracy) utilizing such advanced imagery. Subsequently, those narratives, supported by compelling imagery, are easily broadcast throughout the internet and can reach ever-growing audiences. Consequently, any significant events around the world can quickly generate multiple competing narratives for which policymakers must sift through and contend with in ways that can paralyze decision-making.

The effect of this growth on the deterrence calculation is even more significant. To date, mobile ICBMs have been seen as a somewhat cumbersome but effective way to maintain the deterrent credibility of ICBM forces in an era of high ballistic missile accuracy. Integrated persistent real-time surveillance would pose a serious challenge to this assumption. If the technologies involved can be effectively integrated—which is no small order but not impossibly difficult—it should be possible at some point in the future, perhaps within 20 years, to maintain an out-of-garrison tracking capability of adversary mobile ICBMs. Coupled with offensive forces, such a persistent surveillance capability would enable offensive strikes against mobile ICBMs, especially given that, when deployed out of garrison, mobile ICBMs are much softer targets to strike than silo-based ICBMs. This could bring into question the credible survivability of Russian and Chinese nuclear retaliatory capabilities, given the substantial dependence both countries have on their ICBM forces for nuclear deterrence. China has recently been reported to be exploring air-launched ballistic missiles, a substantially costlier basing mode, but one that would provide a degree of ICBM survivability against a first strike and would be much less vulnerable to persistent surveillance capabilities.

Of potentially greater impact on the United States would be a coordinated fleet of underwater ASW drones that could seek out adversary SSBNs. The long-time invulnerability of SSBNs, representing an assured second-strike capability, could be called into question at some point if technological trends continue. While countermeasures are conceivable, they appear unlikely to be able to completely offset the new threat to SSBN survivability. SSBNs and the nuclear-armed missiles they carry lie at the heart of U.S. strategic deterrent capabilities. Depending on the countermeasures that may be possible, confidence in the credibility of U.S. deterrent nuclear forces could be weakened in the years ahead. Key will be the operating ranges of the sensors on the drones. While significant obstacles exist, a number of scientists interviewed expressed serious concern about this threat.

Preliminary Assessment of Strategic Disruption

The strategic disruption to the policy community is creation of a trust deficit as decision makers are paralyzed by the sheer volume of conflicting information that must be analyzed. The competing narratives make it hard to develop consensus about events or threats and limit the ability to build broad coalitions to address those threats. This effectively degrades the strategic stability calculus as leaders become unsure about what is true or not true and therefore may be more likely to initiate aggressive action out of fear.

From an operational perspective, both Russia and China are more heavily dependent on their ICBM forces to deter than is the United States, so there would be an asymmetric and potentially destabilizing disruption in the strategic balance from such massive expansion in the number of platforms observing them. Countermeasures against persistent surveillance technology would themselves have potential destabilizing effects. In a crisis, deployed mobile ICBMs may not provide the survivability that political leaders would want, presenting them with the same "use or lose" pressures that silo-based ICBMs have. Launch-on-warning firing doctrines could overcome such survivability threats. Both Russia and China have submarine-based nuclear forces that would still have deterrent capability but would not have nearly the robustness of their ICBM counterparts in terms of size and ability to resist U.S. anti-submarine warfare (ASW) capabilities. Furthermore, in a risk-averse world, just the credible possibility that their mobile ICBM forces could be placed at risk could be enough to create instability in a crisis, even if the United States did not believe that its counter-ICBM capabilities were sufficient to threaten their adversaries' ICBMs.

For SSBNs, what is significant for swarm technology and the technologies that enable it is that there is a major investment in these technologies already ongoing within the private sector, as well as growing DOD interest. While in the short term it seems unlikely that the stars will all align for this set of technologies to coalesce into a workable system in the next ten years, it cannot be ruled out for the latter part of our 20-year horizon. Furthermore, the feasibility shockwaves of a vigorous persistent surveillance development program would certainly be felt well in advance of its full maturity, heightening concerns about strategic force survivability and strategic stability.

A peer competitor could be driven to adopt doctrines that could reduce strategic stability, or incentives to strike first in a crisis rather than risk the loss of its retaliatory capabilities, issues that strategic analysts thought had been laid to rest several decades ago by the assumed invulnerability of SSBNs and mobile missile launchers. It would be too easy, and dangerous, to dismiss the challenge that persistent surveillance, in conjunction with AI and new sensor technologies, poses to strategic stability as just one more in a long line of new technologies that don't pan out. With the kinds of investments being made in AI in both the private sector and government, and the priority being accorded to it in China, Russia, and elsewhere, there is at least some significant potential for strategic disruption from AI combines with other advancing technologies.

Regulatory Control Regime Options

At first blush, any regulatory control regime for improved persistent surveillance technologies would be either to limit or ban their deployment or use. However, there is a significant headwind to this approach. The United States government essentially gave up trying to regulate sales of commercial satellite imagery back in 1992 when it realized that other countries and other companies based in other countries were putting more and more satellites into space and challenging the near-monopoly that U.S. based firms had enjoyed for years. By the 1990s, if one wanted to get overhead imagery that was not available through U.S. based companies, due to classification issues or political sensitivity, they could simply acquire that imagery from a non-U.S. based company. Given the ubiquity of commercial satellites covering most, if not all, of the earth it would seem that a limitation or restrictive treaty would not be enforceable from a practical point of view.

With regards to those who might use the geospatial technology in support of false or misleading narratives, the best that can be done is aggressive use of libel laws against those who publish damaging or misleading stories. Putting regulatory pressure on IT companies such as Facebook and Google may help. The European Union is currently taking steps to regulate these entities as media companies vice IT companies which may force them to monitor and police content available on the internet. Aggressive information operations may help and quick reaction by public affairs officials in responding to allegations supported by misleading commercial imagery may also help

It would be difficult to control persistent surveillance technology. If successfully developed, the technology would be of substantial benefit to conventional forces. Many tactical applications could rely upon aircraft-based sensors, which could provide one avenue for control. There are no regimes or treaties that can adequately address this new environment.

Cybersecurity Threats

Background

Cyberattacks on military and economic systems have been a known threat since at least the mid-90s. These attacks continuously evolve and mature in form: from attacks used to extract sensitive information and denial of service/access to ultimately the sabotaging of physical equipment and operating plants as demonstrated by the 2010 Stuxnet attacks on Iran's uranium enrichment facilities at Natanz. Working like a virus on a biological organism the Stuxnet virus traveled throughout the world and infected many computer systems before it was discovered. Since the Stuxnet events there have been multiple attempts to use similar cyberattack methods to disrupt physical systems, including an attempted attack by an unknown entity on Saudi Arabia's Ras Tanura oil complex in 2012.

Implications

Given that cyberattacks are very difficult to attribute to a specific country, group, or person, they are a viable weapon of choice for adversaries. Attacked parties will have very little evidence with which to make an attribution determination, and there appear to be limited political consequences for the purveyors of cyberattacks. Cyberattacks are financially cheaper to deploy than traditional WMDs, giving small countries and terrorist organizations significant strategic capability. These are the characteristics that make cyberattacks attractive to weaker adversaries. The challenge for the United States is how to respond to such attacks without causing undue escalation.

Preliminary Assessment of Strategic Disruption

Cyberattacks' abilities to affect a wide range of technologies and activities make this a multi-dimensional threat. This multi-dimensional nature makes cyberattacks—or at least the attack vectors—hard to anticipate and defend against as the various control variables are near-infinite. Cyberattacks are known to have the potential to shut down both offensive and defense systems and, perhaps more insidiously, erode public trust in institutions. That said, the offensive cyber capabilities available to the major powers, and their ability to cause major damage to their economies, even if attacked first, imposes a form of de facto deterrence against any truly major cyberattack. Cyber offense will almost certainly be a prominent feature of future warfare, but in the authors' judgment is not just yet by itself a truly disruptive feature for stability in the strategic nuclear arena, at least in the near future, though this could certainly change over time and should be very carefully monitored. In the post-2038 time period, it is difficult to believe it will not be at least somewhat disruptive.

Regulatory Control Regime Options

A convention on cybercrime and numerous authoritative legal treatises on international law, including the Tallinn Manual on International Law Applicable to Cyber Weapons, have worked to create some agreed-upon norms of behavior. Progress is challenging due to the fact that the United States, Europe, Russia, and China all have different ideas about freedom of expression issues, which naturally cross over into cyber defense issues. The main sticking point seems to be that freedom of expression, a mainstay of American culture and values, is seen as interference with state control by countries such as Russia and China. However, as much as adversaries

would like to use cyberattacks against each other, there is greater fear of having cyberattack capabilities used against them. Thus, many mutually assured destruction paradigms appear to apply to the cyber security arena, as noted above.

Mitigating the Impact of Disruptive Technologies

Common Themes

In looking at the above-listed technological advances a few themes emerged. First, there is a distinction between those emerging technologies that result in new types of offensive weapons or hardware and those softer technological developments which affect decision-making and analytics. Consequently, the tools available to address these different categories of technological advances must be differentiated. Additionally, when combined, many of these new analytical technologies have the potential to increase the speed at which mass amounts of data can be acquired and analyzed supporting decision-making regarding a current or potential adversary's actions and behaviors. This is especially true when thinking about the combination of AI and big data sets along with cheap and near persistent surveillance of potential adversaries' facilities.

While these technological developments may be a somewhat softer form of power projection, it is their insidiousness and pervasiveness that represent the challenge to our current strategic environment. They have many economically attractive civilian or commercial applications. Consequently, progress in these softer technologies is geared toward commercial sector applications. This is a sea-change from the way most technologies have come into military or national security use and makes the technologies more difficult to regulate or control.

The other difference is that these soft analytical technologies do not produce "things," such as a warheads, missiles, or launch mechanisms that can be counted and monitored if necessary. New "hard" technologies, such as high-energy lasers, antineutrino detection, and hypersonic weapons are all technologies that could lend themselves to traditional arms control tools. With traditional arms control treaties and agreements, the parties would account for, monitor, and verifiably reduce the number of "items" in each party's possession. On the other hand, technologies like AI, vast databases, sensor data, and information operations are not tangible items and thus are not easily subject to traditional solutions such as arms control treaties. In many instances, the establishment of norms of behavior, use of law enforcement, and civil litigation tools may prove to be more suitable approaches for regulating the spread of dangerous technologies.

The Impact of Softer Technologies on Trust

The increasing depth and speed of the analytical processes has several consequences for strategic stability going forward. While it might seem counterintuitive, acquiring more facts and more analysis does not always result in more knowledge. That is because each new fact, each new piece of analysis, and each new piece of imagery rarely answers 100 percent of policymakers' questions. The result may end up being a more granular mosaic that suggests more information gaps than fills. The data overload often ends up resulting in a breakdown of trust regarding the availability of data, colloquially called an "analysis paralysis." Although it is not part of many discussions surrounding strategic stability, trust in knowing what is true and not true is a highly consequential element of strategic stability.

Autonomous Weapons

One fear that some have regarding this new speedy and data-rich environment is that it will lead to the deployment of autonomous systems (i.e., taking the human out of the decision loop). The pressure to go fully autonomous may grow if it is perceived that adversaries' decision-making

processes are moving faster than one's own—and if adversaries are using autonomous weapons themselves.

Autonomous weapons may not necessarily differ in size, shape, or effects from regular weapons; they may even use the exact same platform. The only difference, therefore, may be how the decision to instigate the use of the weapon is made, i.e., the machine making the decision to fire without human control. While there may be an inherent reluctance to use an autonomous weapon that takes a human out of the firing decision loop, the fact that an adversary has gained information superiority may tip the scales in favor of the weaker adversary going autonomous. Thus, an escalation in the use of autonomous weapons inevitably leads to an even more unstable environment and the erosion of strategic stability. The merging of AI and big data is a potential enabler of the introduction of autonomous weapons.

Creation of a Strategic Advantage to Launch First

Use of AI, big data analytics, and persistent surveillance can give a nation's leadership the sense that they have superior and more detailed knowledge of an adversary's capability and intentions. This feeling of information superiority can create a sense of perceived advantage. When one party perceives itself as having such knowledge superiority, it may lead them to the conclusion that they can initiate a first strike attack. At the same time, if a nation's leadership perceives that it is at risk of falling well behind an adversary in these critical technologies, whether or not it is true, that leadership could in a crisis fell more compelled to escalate and strike first than it would if it had no such concerns. Either way, this leads to a more unstable world at greater risk of escalation to nuclear war.

Options for Addressing New Technology Threats

Options to address these new technology threats discussed above generally fall into five categories:

1. Arms control treaties
2. Establishing norms
3. Criminal prosecution
4. Export Controls
5. Lawfare under international law (including patent protection)
6. Committee on Foreign Investment in the United States (CFIUS)
7. Maintaining the Technical Edge Through Education

Arms Control Treaties

Arms control treaties have historically been a valuable tool for limiting and controlling the spread of dangerous technologies. They are entered into only by nations—not companies or terrorist organizations—which limits their span of influence. Such treaties are particularly useful in two situations.

First, they are effective where nation-state adversaries have discovered or realized the theoretical benefits of the new technology but have not yet made the investment to exploit them. An example of this can be seen in the way the United States and the former Soviet Union historically dealt with the issue of weaponization of space. In the late 1960s, both countries realized that there were potential strategic advantages to placing nuclear weapons in space. At the same time, both parties realized that the price tag for pursuing these technologies was astronomical. In this situation, it made sense for both parties to enter into a series of treaties limiting the weaponization of space before either side made huge investments that they would be inclined to want to protect once they had been made.

Second, treaties can be an effective way to deal with measure for measure reductions of a particular class of weapons such as nuclear warheads, cruise missiles, or strategic bombers. For example, one can look at the START, SALT, and INF reductions by the United States and Soviet Union as a textbook example of how this phenomenon works.

With regards to some of the technologies discussed above, particularly hypersonic strike technologies, high-energy laser weapons, and laser isotope separation technologies that could lead to the building of a nuclear weapon, multilateral or unilateral treaties may be in order. However, reaching treaty agreements to limit the use of emerging technologies may be harder than in years past when the signatures of only two superpowers (United States and Russia) were needed to reach a comprehensive agreement. Now other countries such as China, India, and perhaps some European nations would also need to be part of such treaties if they were to be effective. This is a complicating factor, but not necessarily an insurmountable one.

Establishing Norms

While they don't carry the legal weight of a treaty, the establishment of generally agreed-upon norms can help reduce the spread, and/or use of dangerous technologies. They are most effective in situations where they are considered to be politically and morally binding. The good thing

about norms is that a nation can comply with them without having to be bound by a restrictive treaty condition. Furthermore, the establishment of international treaties, such as the landmine treaty or the Comprehensive Test Ban Treaty (CTBT) may be influential in establishing normative behavior by those parties that have not signed up to or ratified those particular treaties. For example, the United States, while not a signatory to the CTBT, has not explosively tested a nuclear weapon in over 25 years. Thus, the CTBT has therefore operated as an effective restriction on behavior. Other norms, such as a "no first use" promise, can slow down the development or impede the use of dangerous weapons.

Adherence to norms may be particularly effective with regards to further development of cyber weapons. In 2009, approximately 20 experts in international cyber law wrote the Tallinn Manual. The Tallinn Manual was updated in 2017 in light of the many changes developed in just eight years. The importance of the Tallinn Manual is that it establishes a baseline for normative behavior in cyber operations. It may never carry the weight of a treaty on cyber operations, but it could give an aggressor a reason to pause and think about the consequences of their actions.

Criminal Prosecution

Criminal prosecutions against individuals that have stolen or misappropriated technology can be an effective deterrent to those individuals and, to a lesser extent, countries. The Bureau of Industrial Standards (BIS) publishes lists of technologies and items which may not be exported to foreign countries. They also identify the criteria for making these export control determinations, such as the nature of the item and/or the nature of the country that may wish to procure such items. Exporting banned items is a crime punishable by significant fines and/or jail time. While some individuals may be inclined to steal technologies for certain countries, they may not be as willing to risk jail time in order to do so.

Criminal prosecutions for stealing technology may go forward whether or not there is a specific control or restriction on the particular item. In other words, stealing is stealing, and stealing is criminally punishable regardless of any export control or classifications assigned to the stolen items. The broad criminal prohibition against stealing is helpful, as technology often advances faster than the law or the BIS listings can keep up with. This is especially important with regard to software technologies such as AI and machine learning as a full understanding of the national security implications of these technologies is not as readily apparent as would be the case with something like hypersonic weapon technologies.

The Justice Department's National Security Division established an office for prosecuting export control violations in 2001. In the last 17 years they have prosecuted multiple individuals for stealing sensitive technology. The downside to the criminal prosecution approach is that it is very expensive and time-consuming. Cases take years to develop, and even if a case does end up before a jury, there is no guarantee that a defendant will go to jail for their crimes. (Juries sometimes acquit the defendants, especially because cases of this nature can be highly complex and hard to understand by the average layperson.) Conversely, merely charging a business or individual with a violation may cause them to become shunned within the community. That, in turn, can lead to a severance of profitable business relationships and limit a business or individual's ability to obtain financing and access to credit markets. These potential negative consequences can serve as a substantive and practical deterrent.

Export Controls

Export controls have been a commonly used tool designed to prevent acquisition of militarily significant technologies to other countries. Use of this tool is challenging because of several factors.

First, enforcing export controls can lead to a cat-and-mouse game between those attempting to acquire a technology and those except attempting to protect it. For instance, a large piece of equipment can often be divided into parts. Export controls on a large piece of equipment, such as a centrifuge, may not prevent the export of the component parts, such as rotors, casings, and ball bearings, which would allow the controlled item to be shipped in several different subparts that may not be considered controlled items, or may not raise suspicions. Once all of these parts arrive at their destination they can then be assembled into a centrifuge.

Second, certain laws in the United States outlaw the export of a "deemed export," which is the implicit and intangible technical knowledge that is gained by working on a certain technology. Controlling deemed exports is particularly tricky for governments, such as the United States', to control when one considers that many foreign students working with professors in the United States can acquire this deemed export knowledge rather casually. The idea of controlling deemed exports, or knowledge, is a cultural anathema to laboratories and big universities where the concept of sharing knowledge is an important factor in advancing the state of knowledge. Collaboration is seen as a virtue and possible stepping stone to greater social and professional recognition within academia's cultural context.

Lawfare

As pointed out above, the softer technologies such as AI, big data, and persistent surveillance are all being driven by the needs of the commercial sector. Relying on traditional arms control treaty structures (involving governments as the parties to the agreements) will not work to control or limit the spread of soft analytical technologies. These softer technologies cannot be characterized as "things" that can be quantified and reduced on a tit-for-tat basis, as is done in most arms control treaties. Furthermore, the companies making advances in these areas, such as AI, are not heavily reliant on DOD or intelligence community funding, as has historically been the case regarding the development of new technologies relevant to national security interests, which limits the U.S. government's ability to apply leverage. Because protecting and controlling access to AI technology is more of a commercial concern for developers and investors than a national security issue, it might be best to look at solutions normally employed by the commercial sector to control the transfer of these technologies. One way to keep dangerous technologies out of the hands of our adversaries may be through the use of strategic civil lawsuits or what is sometimes referred to as "lawfare."

Fortunately, American technology companies do not need the help of the U.S. government to bring these civil lawsuits against foreign companies who might steal their intellectual property or violate the terms of a licensing agreement. These companies can simply sue the violators in U.S. civil courts for money damages, including punitive damages which may be quite significant. The advantage of using civil lawsuits versus criminal lawsuits is that the standard of proof is a much lower bar to clear, making it much easier for American companies to hire commercial litigators and sue in U.S. courts. Jurisdiction over foreign defendants is obtained due to the fact that the act

of misappropriation occurred in the United States. In the best-case scenario, the victim company will have their judgment satisfied by the defendant. But even if the judgment is not collectible, its effect can be consequential. Foreign companies or individuals with a history of civil lawsuit violations find it hard to raise capital in any jurisdiction or partner with other commercial firms. These factors create a disincentive for those individuals and entities were found guilty of violating U.S. laws and give teeth to the civil litigation approach.

Patent Protection Lawsuits

A vehicle for initiating a lawfare strategy as defined above is the targeted use of patent protection lawsuits. One of the defining characteristics of the new softer technologies, such as AI, is that unlike many past technologies useful to the intelligence and defense communities, these technologies were not "born secret." Rather, they were invented or "born" into the commercial space for commercial purposes, often funded by capitalist investors whose sole aim is to see a return on their investments. It would be almost impossible for any government to classify and control the spread of such a fast-growing ubiquitous technology—and once the technology is pilfered, the proverbial genie is out of the bottle and cannot be returned. The result is that many of the most important technologies with military applications are known and can be easily replicated or used by adversaries. Thus, protecting a predominantly commercial technology investment requires a more commercially-driven solution. The technologies' owners have a tremendous monetary incentive to go after those who steal their protected inventions. When the economics are conducive, they will do so independent of a government's wishes.

The Committee on Foreign Investment in the United States (CFIUS)

CFIUS is an inter-agency committee that reviews attempts by foreign entities to acquire U.S. companies and, by extension, their technologies. CFIUS can deny foreign companies from purchasing U.S. companies if those U.S. companies have products or technologies that are critically important for national security. Since 2006, CFIUS has been active in denying purchases of companies by foreign entities, including purchases that have a more tenuous relation to pure national security needs. This reflects the fact that many national security technologies have significant economic impact on the U.S. economy in addition to any technology concerns such foreign purchases would trigger. Additionally, the mere threat of a CFIUS review can stall acquisition efforts by foreign entities before a request is ever initiated. Furthermore, the number of withdraws from consideration for CIFIUS review has grown exponentially over the last 10 years. This statistic suggests that the CFIUS review process is an effective deterrent to those governments and entities seeking to acquire sensitive U.S. technologies.

CFIUS is an important break on speedy acquisition of U.S. technology in the commercial sector. The challenge is that companies seeking to acquire U.S. technology may not always subject themselves to the CFIUS process. Currently, CIFUS review is undertaken only in those instances where an acquiring company seeks a review and/or opinion. Normally this only done by large foreign companies seeking to invest in or acquire an interest in U.S. based firms. Smaller, lesser-known companies may operate below the radar and that may pose a greater risk of technology transfer.

Maintaining the Technical Edge through Education

Maintaining a technical edge in technology is a function of society's will to invest in maintaining that edge. That translates into a need to have more money spent on basic research in universities—whether funded by government or private entities. The one concern is that foreign nationals attracted to U.S. universities may learn of sensitive technologies and take that knowledge back with them to their countries of origin upon completion of their studies. However, if U.S. universities can maintain their competitiveness through sheer thirst for discovery and embracing new technologies, then the advantages gained by students returning to their home countries after studying in the U.S. will diminish over time.