New Technologies & Strategic Stability

Christopher F. Chyba

A variety of new technologies, ranging from broad enabling technologies to specific weapon systems, may threaten or enhance strategic stability. In this essay, I analyze a technology's potential to significantly affect stability along three axes: the pace of advances in, and diffusion of, this technology; the technology's implications for deterrence and defense; and the technology's potential for direct impact on crisis decision-making. I apply this framework to examples including hypersonic weapons, antisatellite weapons, artificial intelligence, and persistent overhead monitoring. Formal arms control to contain dangers posed by some of these seems technically possible, though currently politically difficult to achieve. Others, particularly enabling technologies, resist arms control based on effective verification. The major powers will therefore instead have to find other ways to cope with these technologies and their implications. These options should include exchanges with potential adversaries so that pathways to nuclear escalation, and possible mitigating steps, can be identified and discussed.

New technologies can have direct and indirect military significance that in some cases may threaten strategic stability. Such technologies can arise anywhere along a spectrum extending from research in pure science to systems development driven almost exclusively by military goals. Genetic engineering, and in particular its powerful realization in the new CRISPR technology, exemplifies the former; airborne high-powered laser counterspace weapons would be an example of the latter.[1]

Rather than choose a selection of these new technologies and examine their potential effects, which has now been done by many others,[2] I choose to step back and suggest a framework for analyzing the impact of new technologies on strategic stability. If this effort is successful, others might modify or add to the framework in the future. My hope with this framework is to increase the likelihood that consideration of a new technology with possible significant implications for strategic stability would include a systematic assessment of that technology's potential stabilizing and, especially, destabilizing effects. This assessment would need to be specific to capabilities of, and employment against, particular adversaries. By thinking systematically about these potential effects, it might be possible to make these choices more wisely, and to argue – domestically, bilaterally, or multilaterally – for appropriate restraint, transparency, or control.

https://doi.org/10.1162/DAED_a_01795

Whether a new technology or weapon system significantly impacts strategic stability depends on the intrinsic capacity of that technology or system to do so, but also on whether and how it is deployed and operationalized by different powers and the force structure of the adversaries against which it may be deployed. A classic example prior to the nuclear age was the debut of the aircraft carrier in 1917 by the British navy. It was the upstart navies of Japan and the United States that recognized that carriers could change the nature of sea power and they deployed them to this end. By contrast, the British navy, for a host of reasons, long viewed carriers as scouting and reconnaissance adjuncts to the battleship.[3] The destabilizing effect of naval aviation for the previous naval order therefore required not only the invention of the carrier, but their production in sufficient numbers and their appropriate deployment and use.

A quite different example from the nuclear era is the Cold War deployment by the United States and the Soviet Union of multiple independently targetable reentry vehicles (MIRVs) on both intercontinental and submarine-launched ballistic missiles (ICBMs and SLBMs). The deployment of MIRVs on ICBMs in either U.S. or Soviet silos vulnerable to first-strike nuclear attack is strategically destabilizing, since an adversary can hope to destroy many warheads on each silo-based missile with the expenditure of only one or two of its own warheads – thus tempting the adversary to strike first. But the deployment of the same technology on analogous missiles of intercontinental reach in the apparently invulnerable submarine ballistic nuclear (SSBN) fleet of the United States is less threatening to strategic stability, since the effectively invisible U.S. SSBNs do not tempt a first strike. (MIRVing SLBMs may still negatively impact stability by increasing an adversary's fear of an overwhelming first strike.)[4] This demonstrates that the destabilizing effects of a new technology can in fact be exacerbated or mitigated by deployment and doctrinal choices.

What is strategic stability? Because there is no single uncontested definition, this essay makes its own choice explicit.[5] I set aside broad non-nuclear definitions of the term involving a security environment in which states are not tempted to go to war.[6] Here I take *strategic stability* to include *crisis stability* and *arms race stability*. *Crisis stability* means that even in a crisis (possibly including conventional war or the near prospect of nuclear war), states do not escalate to nuclear weapons use. This means first that states choose not to escalate deliberately to nuclear first use (crisis or no), because each state recognizes that any such strike will lead to devastating nuclear retaliation. It also means that the situation is robust against inadvertent or mistaken nuclear escalation. The latter includes both escalation on the basis of misinterpreted or false information (whether intentionally created or accidentally acquired, the risks of both may be exacerbated in a crisis) and escalation due to breakdowns in command and control.[7] *Arms race stability* holds when the relevant powers have incentives to avoid action-reaction cycles that, in addition to being expensive, could also lead to deployments that undermine first-strike stability.

In principle, a new technology's impact on strategic stability could be positive with respect to some aspects of stability and negative with respect to others.

I define a "new" technology to be one that has not yet been overtly significantly deployed by any nation's military, so that its effects on strategic stability are still largely in prospect. By this definition, for example, ground-based midcourse ballistic missile defense (GMD) is not a new technology. True, substantial improvements in GMD's ability to differentiate warheads from decoys, or decisions to deploy much larger numbers of interceptors, or even announced doctrinal changes, could have serious consequences for strategic stability. But there are many currently deployed technologies for which qualitative improvements or quantitative expansion could have such consequences, and as a practical matter I choose not to include these many possibilities in this discussion. By my adopted definition, although "cyber" weapons have reportedly already been used in a variety of contexts – from targeting uranium centrifuges to interfering in national elections – their greatest potential impact in warfare remains undemonstrated and recessed.[8] Such technologies will therefore be included here.

Even with the restrictions placed by our definition, the list of new technologies that can be identified as having potential significant consequences for strategic stability is long. These include broadly applicable enabling technologies such as artificial intelligence (AI),[9] biotechnology (especially genetic engineering and synthetic biology),[10] and quantum computing and cryptography.[11] They include categories of counterspace weapons encompassing kinetic weapons, nonkinetic physical weapons (high-powered lasers and microwaves), cyber weapons, and electronic jamming and spoofing.[12] They also include weapons whose characteristics might appear to an adversary as suited for executing first strikes, such as conventional and nuclear hypersonic weapons, including hypersonic glide vehicles (HGVs), hypersonic cruise missiles (HCMs), and stealthy strategic autonomous systems.[13] And they include systems or capabilities that could help enable first strikes, such as persistent surveillance technologies for tracking mobile missiles, antineutrino detectors for tracking submerged SSBNs,[14] and some aspects of counterspace and cyber weapons.[15] There are also technologies that could in principle alter the underpinnings of multilateral strategic relationships, such as laser isotope separation for uranium enrichment.[16]

This is a vast array of technologies to be considered. Even if we constrain the challenge facing us by restricting the discussion to those technologies that could see significant deployment within the next twenty years, this likely rules out only the use of antineutrinos to detect the nuclear reactors of submerged submarines, and not necessarily any of the other technologies listed. In this essay, I further restrict discussion to the case of the major nuclear powers. I therefore will not consider, for example, the diffusion of laser enrichment technology, which, while potentially important for determining the number of nuclear powers and the

resulting web of strategic relationships, is unlikely to affect significantly the arsenals of the major powers over the coming twenty years.

The ability of a state to develop and deploy a technology with sufficient salience to alter strategic stability depends on factors that go beyond the readiness and scope of the technology. These include financial and organizational requirements as well as the extent to which adopting the technology would disrupt existing military practice or the status of relevant organizational elites.[17] At the same time, since strategic stability depends on perception as well as objective reality, it might be affected even by a very imperfect adoption of technology.

I analyze a technology's potential to significantly impact strategic stability along three axes: 1) the pace of advances in, and diffusion of, this technology; 2) the technology's implications for deterrence and defense; and 3) the technology's potential for direct impact on crisis decision-making. These three broad categories overlap and inform one another. Within each, I highlight several specific issues to consider.

1) Pace and diffusion. This category focuses on intrinsic properties of a technology that affect the speed at which the technology develops and the ease with which it may spread among major powers, albeit with a recognition of differences in adoptive capacity of individual states.

a) *Is the technology in question a weapon system or an enabling technology?*

An enabling technology is one that in itself is not a weapon, but that has broad implications for many areas of military and intelligence technology and practice.[18] A current example of a weapon system would be a hypersonic glide vehicle, and a contemporary example of an enabling technology would be artificial intelligence. The answer to the question has implications for the practicality of arms control measures for a given technology.

b) *Does the technology have characteristics in terms of cost, complexity, tacit knowledge, or commercial applications that suggest that it will diffuse quickly (or slowly) to the other major nuclear powers?*

For example, biotechnological power, by objective metrics, is falling exponentially in cost over time.[19] This reduction in cost is so rapid that continuing diffusion of this enabling technology among the major powers seems inevitable and commercial incentives so great that formal arms control seems fanciful.[20] Rapid diffusion of a technology may reduce potential "first-mover" advantages.[21] However, this conclusion depends on the force structure and posture of the states involved.

c) *Are there important advances that are likely to remain "invisible" to adversaries?*

If so, at least barring enforced transparency and verification via, for example, treaty requirements, a state is more likely to adopt worst-case models for an adversary's progress. Worst-case fears of an adversary may lead a state to adopt a posture in which nuclear weapons are more readily used. Strategic ballistic missile defense and cyber capabilities or artificial intelligence provide contrasting examples. The development of an even minimally credible strategic ballistic missile defense system requires testing that is visible to peer adversaries, even absent any arms control agreement facilitating monitoring and data-capture from each test. This stands in stark contrast with the development of cyber weapons, or with government-held advances in AI, which, absent espionage, likely remain unknown to an adversary until, and perhaps even beyond, actual use.

d) *Is the pace of technological advance so fast that it outstrips states' abilities to negotiate international regimes to manage the technology?*

Thomas Schelling and Morton Halperin famously defined "arms control" expansively as "all the forms of military cooperation between potential enemies in the interest of reducing the likelihood of war, its scope and violence if it occurs, and the political and economic costs of being prepared for it."[22] But at least some of these approaches are undermined when a technology is growing in scope and power so quickly that the pace of its technical evolution greatly outstrips the pace of international rule-making (and *a fortiori* treaty negotiation). An arms control regime that involves considerable transparency and monitoring measures, as with U.S.-Russian strategic weapons under New START,[23] fosters crisis stability by reassuring states that their adversary does not hold some secret advantage.

2) Deterrence and defense. This category addresses the level of destruction that could result from the use of the technology, as well as its implications for deterrence and defense.

a) *Could the damage or destruction resulting from the use of the technology rise to the level that would elicit a nuclear response?*

The answer to this question, at least formally, depends on the nuclear use doctrine of the target state. This question emphasizes that certain technologies may be destabilizing in the sense of fostering the use of nuclear weapons in response to their employment, without themselves being first-strike weapons. Biotechnology provides one example: the Obama administration's Nuclear Posture Review specifically calls out advanced bioweapons and their relation to biotechnology as one important reason why

the United States did not adopt a "sole purpose" doctrine for its nuclear arsenal.[24] (A sole purpose doctrine is one in which a state announces that the sole purpose of its nuclear weapons is to deter other states from using, or threatening to use, their own nuclear weapons.) The Trump administration's Nuclear Posture Review also identifies a potential link between "highly lethal biological weapons" and nuclear posture.[25]

b) *Is the attribution of an attack employing the technology straightforward or potentially difficult?*

(This includes the possibility of an attacker attempting to generate a misattribution for the attack.) Kinetic attacks are likely to be readily attributed: in the case of missiles, because their point of origin will probably be identified, as is also the case for launch-to-intercept antisatellite technology. (In general, because of its tracking capabilities, the United States seems likely to be able to trace the origin of any kinetic space attack, even one originating from an orbiting satellite. The Defense Intelligence Agency has stated that China and Russia also have significant space tracking capabilities.)[26] Attribution might be more challenging for nonkinetic weapons such as high-energy lasers, and could become difficult or very difficult for certain biological attacks and cyberattacks. In principle, this might also be true for nuclear attacks using stealth delivery systems, although nuclear forensics might, in this case, help provide an attribution.[27] Adversaries that anticipate that they are likely to remain unidentified are less likely to be deterred. Yet as we have seen, the attacked state may hold out an option to reply to sufficiently severe attacks with nuclear weapons. In this case, an adversary's hope to avoid attribution and the resulting deterrence failure could lead to escalation to nuclear use, either because attribution was nevertheless achieved or because the victimized state had reasons other than technical forensics to identify a particular state as responsible.

c) *Could the employment of the technology for intelligence, defense, or other purposes be misinterpreted as preparatory to a first strike?*

One technological example here is cyber capabilities. Cyber penetration of, for example, strategic command and control, artificial intelligence supporting war-fighting, or early-warning or surveillance satellites might take place for reasons of intelligence gathering. But it might not be apparent to the targeted country whether the penetration is for data extraction, intended to degrade certain conventional abilities in the context of a conventional war, or is an attempt to disable command and control systems in preparation for a first strike on the country's strategic forces.[28]

d) *Are there credible defensive measures (broadly understood) that a state could take to blunt or defeat an attack using the technology in question, and are these measures stabilizing or destabilizing?*

A credible defense that would seem ready to defeat or mitigate an attack could enhance stability by deterring the launching of the attack (deterrence through denial, by altering the risk/benefit calculation of the attacker), by reassuring the targeted state that rapid retaliation was not required, and/or by limiting the destruction caused by the attack to a level where retaliation with nuclear weapons seemed disproportionate. But defense may also be destabilizing if it has as the intended or ancillary effect of diminishing substantially a country's second-strike response to a first strike. There is a spectrum of examples. Improved disease surveillance and response to potential biological attack would seem to be purely stabilizing in its impact. Better defense against cyberattack might typically be stabilizing, although there may be forms of "active" defense that could be escalatory and hence destabilizing depending on an adversary's interpretation.[29] Finally, strategic ballistic missile defense might be stabilizing as a deterrent (by denial) for an adversary with very low numbers of ICBMs, such as North Korea currently, but simultaneously destabilizing with another potential adversary, for example by appearing to China to provide a U.S. capability to eliminate the small number of ICBMs that might "leak through" a U.S. first strike on China's intercontinental forces and command and control, thus weakening China's deterrent against a potential first strike.

3) Effects on crisis decision-making. New technologies could affect decision-making in a crisis – pushing those decisions toward or away from nuclear use – in a variety of ways.

a) *Does the technology confer such a significant advance in first-strike capabilities that an adversary would be more likely to launch first, or to launch a second strike with less deliberation, for example, on warning of an attack?*

A historical example of such technologies would be the marriage between MIRVed ICBMs and SLBMs – thus providing the attacker with far more warheads per ballistic missile – and the ongoing revolution in accuracy that putatively allows these warheads to be placed close enough to their intended destination to destroy even extremely hardened targets.[30]

b) *Could the technology substantially reduce (or enhance) decision-making time or strategic situational awareness for the leadership of a targeted state?*

Technologies might reduce decision-making time directly by putting command and control or second-strike forces at risk on a shorter timescale

than was previously the case. Or a technology might be used to disable, jam, or subvert early-warning satellites, or intercept and spoof communications from such sensors to command and control destinations, reducing a state's leaders' ability to determine if a strategic attack were underway. Either of these effects could make premature or mistaken escalation to nuclear weapons use more likely. At the same time, certain new technologies hold the prospect of reducing an adversary's ability to intercept and spoof without detection. Advanced weapons expert Lora Saalman has suggested, for example, that China's "avid" push for quantum encryption is driven by this desire to protect communications and data transmission against bogus information that could be inserted to create either false negatives or positives in the context of a U.S. first strike.[31] Perhaps in part to this and related ends, China launched the Micius satellite in 2016 as an experimental demonstration – using entangled photons – of quantum encrypted transmission from a space satellite.[32]

c) *Would a particular deployment scenario for the technology be likely to fulfill the criteria for normal accidents?*

Normal accident theory identifies systems that simultaneously have high interactive complexity (meaning that the interactions of the system's components are nonlinear and can lead to unanticipated outcomes) and tight coupling (meaning that these interactions often happen too fast for humans to intervene effectively) as especially likely to suffer serious failures, and in ways that are not easily overcome (and may even be exacerbated) by usual practices intended to enhance reliability and minimize error.[33] In the strategic stability context, such failures could come in the form of misinterpretation or other errors that could increase the likelihood of escalation to nuclear use.

To illustrate the framework developed above, I will now apply it to several examples of new technologies with implications for strategic stability. I choose my examples from among those technologies that Secretary of Defense Jim Mattis singled out as particularly salient in his April 2018 U.S. Senate testimony, in which he stated:

> Rapid technological change includes developments in advanced computing, big data analytics, artificial intelligence, autonomy, robotics, miniaturization, additive manufacturing, directed energy, and hypersonics – the very technologies that ensure we will be able to fight and win wars of the future. Ultimately, these technologies will change the character of war, a reality embraced by DoD.[34]

First, consider hypersonic weapons: weapons that will travel at more than five times the speed of sound.[35] The United States, Russia, China, and other countries are spending billions of dollars in pursuit of these weapons.[36] One particular example is hypersonic glide vehicles (HGVs), intended to be boosted into the upper atmosphere by rockets, after which they follow an unpowered glide to their target, possibly with midcourse propulsion for flight adjustments.[37] These vehicles could be developed to carry either conventional or nuclear warheads, and would be both very fast and, because of their maneuverability, possibly very accurate.

Consider HGVs according to the set of questions presented here. HGVs are a specific weapon type driven primarily by military applications that have spread rapidly among the major nuclear powers. As a kinetic system that requires testing, it seems likely that the major powers will have a fair sense of one another's progress, giving warning time to lessen any first-mover advantages. The pace of development is not so fast as to exclude formal or informal arms control measures, suggesting that destabilizing impacts of HGVs could be mitigated.

But a recent essay by Adam Lowther and Curtis McGiffin, strategic and nuclear deterrence scholars with the U.S. Air Force, asserts that because arms control for hypersonics would need to be multilateral, which would likely prove untenable, Russian HGVs (like the Avangard), as well as stealthy nuclear delivery vehicles (such as the Ocean Multipurpose System Status-6 underwater drone, were it to prove credible) could so greatly reduce U.S. command and control warning or response time as to threaten the credibility of the U.S. nuclear deterrent. Lowther and McGiffin argue that as a result, the United States may have to "develop a system based on artificial intelligence, with predetermined response decisions, that detects, decides, and directs strategic forces with such speed that the attack-time compression challenge does not place the United States in an impossible position."[38] These authors' intention is to protect strategic stability in the face of new technologies, but at the cost of placing weapons that could end human civilization under the control of an artificial intelligence.[39] Consider some of the framework elements described above, applied to this specific example of new Russian weapons (or potential weapons) and the proposed U.S. response: The deployment, or threat of deployment, of compressed-timescale or stealth delivery weapons increases U.S. concerns about a Russian first strike. AI-enhanced or even AI-controlled command and control is suggested as a defensive measure that would improve the deterrence of such an attack and possibly blunt it were it to take place. Yet deploying this potential U.S. defense, and its interactions with new Russian capabilities, seems likely to fulfill the criteria for normal accidents, thereby increasing the likelihood of serious error and possible disaster. Clearly this extraordinary defensive step would create a myriad of its own dangers to stability.

Along a different leg of the U.S.-Russia-China triangle, U.S. HGVs, whether conventional or potentially nuclear-armed, could arguably both increase the

threat to China's second-strike force and do so with a velocity that might reduce China's decision-making time. Joshua Pollack, editor of *Nonproliferation Review*, has written that the perception of reduced decision-making times "is encouraging the Chinese military to modify its nuclear posture in ways that tend to create greater risks for both sides," including discussions of shifting to a more alert posture and to continual patrolling with SSBNs.[40] That is, some (but not all) of the defensive measures China could take in response to HGV capabilities would lower the threshold for nuclear use. But a framework question described above – Does the technology confer such a significant advance in first-strike capabilities that an adversary would be more likely to launch first, or to launch a second strike with less deliberation? – leads us to ask whether HGVs would actually represent such a significant advance in first-strike capabilities that China would be more likely to launch first. Would HGV flight times really be shorter than existing SLBM attack times? Chinese nuclear policy expert and contributor to this *Dædalus* volume Li Bin has pointed out that a U.S. SLBM warhead has a flight time of only fourteen minutes, starting with launch from a range of four thousand kilometers.[41] SLBM (and ICBM) warheads are already hypersonic, reentering the atmosphere after ballistic trajectory at velocities as high as twenty-nine thousand kilometers per hour, or Mach 24.[42] For various possible scenarios, military analysts should rigorously ask under what circumstances HGVs would actually reduce warning times below those from the existing SLBM force. Or is it some other HGV capability – such as hypersonic *conventional* warheads – not flight speed as such, that is the putatively destabilizing characteristic? Dean Wilkening, defense analyst at the Johns Hopkins University Applied Physics Laboratory, has argued that the anticipated "exceptional maneuverability" of HGVs and hypersonic cruise missiles will make their targets – conventional or strategic – "difficult to discern until the last few minutes before impact." The resulting de facto entanglement of conventional and strategic targets could pressure Chinese leadership to launch strategic weapons while the hypersonic attack vehicles were still in flight, even if the United States had launched the attack purely to eliminate Chinese conventional targets.[43]

As a second example, consider growing Chinese and Russian capabilities in antisatellite (ASAT) technologies. The U.S. Director of National Intelligence (DNI) issued a threat assessment in 2018 that found that Russia and China had ASAT weapons that would reach "initial operational capacity" within the next several years.[44] These would likely be ground-launched missiles, but both countries were also moving forward with directed-energy weapons to blind U.S. remote-sensing or missile-defense satellites. The DNI report assessed that in the event of a future conflict between either country and the United States, each country could use attacks against U.S. satellites to offset any perceived U.S. advantage from military or commercial space systems. James Acton, co-director of the Nuclear Policy Program at the Carnegie Endowment for International Peace and an author in

this collection, has similarly argued that, in wartime, the Chinese might decide to strike U.S. early-warning satellites (satellites used for both conventional and strategic nuclear warning) in order to enable Chinese conventional ballistic missiles to circumvent U.S. defenses and reach their targets in East Asia. Acton warns that such strikes could be misinterpreted by the United States as an attempt to blind U.S. early warning against a Chinese strategic nuclear attack. Various paths to escalation to nuclear use would then exist.[45] The framework element questioning a technology's potential to reduce or enhance decision-making time or situational awareness was meant in part to capture this kind of destabilizing result.

There are many steps that the United States could take to mitigate the destabilizing effects of Chinese and Russian ASAT technologies. A 2015 Department of Defense white paper describes measures ranging from defensive actions, to rapid reconstitution (by launching replacement satellites), to resilience (such as spreading orbital capabilities among multiple payloads) that could be employed to reduce the effectiveness of Russian and Chinese ASAT capabilities.[46] The concern of the white paper is to identify measures that can be taken by the United States to "achieve warfighting mission assurance." But an element in the above framework – Are there credible defensive measures (broadly understood) that a state could take to blunt or defeat an attack using the technology in question, and are these measures stabilizing or destabilizing? – emphasizes the need for a second filter to be applied to these responses: an assessment of which of the measures considered would, while helping achieve mission assurance, most enhance strategic stability. So, for example, while the ability to rapidly replace early warning satellites is intrinsically valuable and might in some important cases deter an adversary from targeting them, unless this replacement could take place on less than the thirty-minute timescale of a strategic missile attack against the United States, it might do too little to enhance crisis stability. U.S. leaders concerned about a Russian or Chinese strategic attack that would occur shortly after the U.S. losing some early warning satellite capability would not likely feel reassured by the thought that replacements would be in place some hours later. A focus on strategic stability would instead favor enhancing the resilience of U.S. orbiting platforms, for example through options outlined in the white paper of disaggregation, distribution, diversification, passive protection, proliferation, and deception.

A final and very different example is provided by artificial intelligence.[47] AI is a fast-moving, largely commercially driven (in the United States) enabling technology that will have increasingly important impacts throughout society as well as military operations. All of the major nuclear powers are strongly committed to it.[48] It is hard to imagine any plausible monitoring and inspection regime for this technology, though this characteristic is typical of enabling technologies, and not unique to AI: the technology is too widespread for a monitoring and inspection model to provide a good fit. It is also likely that at least certain specific

military-relevant advances will occur under cover of secrecy. The rate of advance in AI is now so strong that some observers are asking not whether its pace outstrips possible arms control regimes, but whether its pace will outstrip human civilization's ability to prevent AI takeover.[49]

Because it is such a broadly pervasive enabling technology, AI's impact on strategic stability will likely be both widespread and widely varying by application. For concreteness, consider one application that has attracted particular attention: the fusion of AI with big data analytics in the context of persistent overhead surveillance by satellite constellations.[50] The strategic context for such surveillance would be, for example, the tracking of road-mobile ICBMs in something approaching real time after they have left their garrisons. Russian and Chinese road mobile ICBMs provide a potentially survivable response to the revolution in accuracy in U.S. strategic systems. Multihundred kiloton weapons that will putatively fall within one hundred meters of their target will defeat any degree of hardening, so first-strike elimination of most silo-based ICBMs seems plausible.[51] One solution to this dilemma is to make the ICBMs mobile (albeit therefore unhardened) so that they cannot be successfully targeted and eliminated. The vast amounts of data that would be returned from persistent monitoring of the entire relevant road network of an adversary's mobile ICBMs, necessarily analyzed by AI, would be one realization of a new revolution in military affairs that moves beyond accuracy to include reliable and routine near-real-time localization of the enemy's targeted forces. Were such a scheme ever to become credible, it would be so first for the less-challenging case of North Korea than for the cases of Russia or China.[52] However, in this essay I am concerned primarily with the latter two cases, against which great numbers of satellites (sometimes called "swarms") would have to be deployed to enable near-continuous coverage of vast land areas.

Satellite deployments already underway indicate that this idea may not be incredible on a twenty-year timescale.[53] For example, SpaceX is deploying a constellation of optically cross-linked mass-produced small satellites (individual satellite masses of hundreds of kilograms) to create a space-based Internet communication system called "Starlink." SpaceX hopes to deploy twelve thousand of these satellites in three shells of low-Earth orbits with over two thousand in orbit by the mid-2020s, and a possible ultimate expansion to forty-two thousand.[54] The size of this constellation may be compared to the approximately 2,100 active satellites orbiting Earth in August 2019.[55] Starlink does not perform ground surveillance, but its numerical scale shows what is possible. In fact, swarms of surveillance satellites are already being put into orbit by the private sector. Planet Labs' more than three hundred miniature satellites now monitor Earth's entire landmass daily at three-to-five-meter resolution; the company's website promises "persistent global monitoring with low latency tasking to deliver early intelligence" for defense and intelligence purposes.[56] And Capella Space is launching a constellation of

forty-kilogram radar imaging satellites in polar orbits that will allow all-weather "hourly coverage of every point on Earth, rendered in sub-meter resolution."[57]

None of these constellations does, nor is intended to do, what would be required for monitoring ongoing positions of Russian or Chinese road-mobile ICBMs. To reach that objective, persistent all-weather overhead imaging would need almost continuously to surveil vast areas, coupled with an AI able to sift and interpret the enormous data set that would be returned in near real time. Even then, there would be legitimate questions about the efficacy of defensive measures: clever ways to hide road mobile forces, including simply taking advantage of particular terrain or tunnels; flooding the roads with decoys; or using cyber, jamming, or other techniques to hack or confound the satellite constellations.[58] But because of the powerful *potential* threat to Russian and Chinese second-strike capabilities that it could pose, such a system, even if objectively imperfect and vulnerable, would likely be destabilizing from the perspective of the countries that felt themselves targeted. Even if such a constellation were openly devoted to other purposes, potential adversaries might plan on the assumption that it was either nevertheless intended to support a first strike, or that it could in the future, in a change of doctrine rapidly become so intended. That conclusion has likely been reinforced by analogy, in the decision by the United States in its 2019 Missile Defense Review to state explicitly that U.S. missile defense "policy, strategy and capabilities" must also address anticipated advanced Russian and Chinese delivery systems, not just the missiles of North Korea and Iran.[59]

Some of the defensive measures that China and Russia would seem likely to take in response to such AI-enabled surveillance swarms would be destabilizing. The construction of multiple road-mobile decoys would in itself be stabilizing by making a first strike harder to execute, even while making strategic arms control, and the broadly stabilizing confidently known quantitative knowledge that comes with it, harder to execute. Defensive efforts to jam, blind, or cyber-corrupt large numbers of targets in satellite constellations might be interpreted as a prelude to nuclear use, rather than as motivated by furthering nuclear target survival. And the country being surveilled might decide that even its road-mobile launchers were so vulnerable that their employment had to include the capability and doctrine appropriate for launch-on-warning.

Now evaluate this scenario from the perspective of the elements of the framework above. The combination of surveillance perceived as threatening to road-mobile second-strike systems, hypersonic weapons with the accuracy to strike located road-mobile systems rapidly before their location was lost, and counterspace and cyber weapons intended to degrade either that surveillance or its command and control (the framework element considering potential for misinterpreting a technology's employment as preparatory to a first strike) would be a dangerous brew. In a conventional war, many of these capabilities would be employed for

reasons other than nuclear first strike, but in an environment in which decisions could increasingly have to be made at "machine speed," since AI-enabled systems will require each party to exhibit the same rapidity of decisions and actions or be at a disadvantage. Even were this not done autonomously, and humans remained in or at least on the loop, the amount of data that would be processed, interpreted, and presented by AI might lead to automation bias, in which humans surrender judgment to an intelligent decision-support system that they may feel they have no choice but to trust.[60] This landscape seems almost designed to realize the criteria of normal accident theory summarized in the framework above (considering if a technology deployment scenario would likely fulfill the criteria for normal accidents), suggesting a reasonable likelihood for misinterpretation or mistakes that in this context could lead to nuclear escalation.

Formal arms control for a subset of these technologies (for classes of hypersonic vehicles, for example) would seem technically possible. But such efforts would face the desire of the parties to have conventional versions of these weapons, the likely requirement that any such treaty would need to impose constraints multilaterally, and the present context of U.S.-Russian collapsing bilateral arms control. In principle, these problems could all be overcome.[61] For example, satellite constellations could be made more resilient to attack, or states could refrain from building constellations that were so large and capable that road-mobile missiles became vulnerable. Satellite numbers and orbits are strongly verifiable, and limiting total numbers carries the ancillary benefit of lessening the space debris challenge.[62] This would require a willingness to trade (and in the U.S. system to explain successfully to Congress and the public) the prospect of damage limitation for the sake of greater strategic stability, a suggestion to which the political counterarguments are obvious but nevertheless need to be engaged. Finally, some proponents of a new technology may intentionally be choosing the pursuit of an advantage, or the hope for eventual primacy, over near-term strategic stability. Even in this case, however, the implications for stability of different technologies must be understood and weighed.

Many other technologies, particularly enabling technologies whose use is pervasive and not credibly subject to monitoring, resist arms control based on effective verification.[63] And in any case, such verification may, at this time, be politically difficult. The major powers will therefore instead have to find other ways to cope with these technologies and their implications. These efforts should include robust exchanges with potential adversaries so that pathways to nuclear escalation, and possible preventive or mitigating steps, can be identified and discussed.

ABOUT THE AUTHOR

Christopher F. Chyba is Professor of Astrophysical Sciences and International Affairs at Princeton University. He is Cochair of the "Meeting the Challenges of the New Nuclear Age" project at the American Academy, and has previously served on the staffs of the National Security Council and the Office of Science and Technology Policy, and as a member of the President's Council of Advisors on Science and Technology.

ENDNOTES

[1] On gene editing, see Jennifer A. Doudna and Emmanuelle Charpentier, "The New Frontier of Gene Editing with CRISPR-Cas9," *Science* 346 (6213) (2014), http://doi.org/10.1126/science.1258096; and Matthew Cobb, "The Brave New World of Gene Editing," *New York Review of Books*, July 13, 2017. On counterspace weapons, see Brian Garino and Jane Gibson, "Space Systems Threats," in *AU-18 Space Primer*, 2nd ed., ed. Air Command and Staff College Space Research Electives Seminars (Maxwell Air Force Base, Ala.: Air University Press, 2009), chap. 21, https://www.airuniversity.af.edu/Portals/10/AUPress/Books/AU-18.PDF.

[2] See Christopher A. Bidwell and Bruce W. MacDonald, *Emerging Disruptive Technologies and Their Potential Threat to Strategic Stability and National Security* (Washington, D.C.: Federation of American Scientists, 2018); James M. Acton, "Technology, Doctrine, and the Risk of Nuclear War," in *Meeting the Challenges of the New Nuclear Age: Emerging Risks and Declining Norms in the Age of Technological Innovation and Changing Nuclear Doctrines* (Cambridge, Mass.: American Academy of Arts and Sciences, 2018); Keir A. Lieber and Daryl G. Press, "The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence," *International Security* 41 (4) (2017): 9–49; Benoît Pelopidas, Keir A. Lieber, and Daryl G. Press, "New Era or New Error? Technology and the Future of Deterrence," *International Security* 43 (3) (2018/19): 190–193; Dean Wilkening, "Hypersonic Weapons and Strategic Stability," *Survival* 61 (5) (2019): 129–148; Todd Harrison, Kaitlyn Johnson, and Thomas G. Roberts, *Space Threat Assessment 2019* (Washington, D.C.: Center for Strategic and International Studies, 2019), https://www.csis.org/analysis/space-threat-assessment-2019; and Edward Geist and Andrew J. Lohn, *How Might Artificial Intelligence Affect the Risk of Nuclear War?* (Santa Monica, Calif.: RAND Corporation, 2018).

[3] Emily O. Goldman, "Reciprocity to Revolution: Carrier Air Power in Peace and War," in *The Diffusion of Military Technology and Ideas*, ed. Emily O. Goldman and Leslie C. Eliason (Stanford, Calif.: Stanford University Press, 2003), 267–303; and Michael C. Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics* (Princeton, N.J.: Princeton University Press, 2010).

[4] I am grateful to David C. Logan for emphasizing the MIRV example to me, and to Leyatt Betre for deepening my understanding of the deployment of MIRVs on ICBMs and SLBMs during the Cold War.

[5] See, for example, discussions in Elbridge A. Colby and Michael S. Gerson, eds., *Strategic Stability: Contending Interpretations* (Carlisle, Penn.: Strategic Studies Institute, U.S. Army War College, 2013); Bidwell and MacDonald, *Emerging Disruptive Technologies*; and Geist and Lohn, *How Might Artificial Intelligence Affect the Risk of Nuclear War?*

[6] For a discussion of these broader definitions, see Linton F. Brooks, "The End of Arms Control?" *Dædalus* 149 (2) (2020).

[7] For example, see Barry R. Posen, *Inadvertent Escalation: Conventional War and Nuclear Risks* (Ithaca, N.Y.: Cornell University Press, 1991). In principle, one could define crisis stability to include strong incentives not to escalate higher after nuclear weapons have already been used at a lower level of intensity. While clearly important should the nuclear-use threshold ever be breached, I focus here on that initial escalation to nuclear weapons use. A memorable discussion is that of Herman Kahn, who identifies forty-four distinct rungs on the escalation ladder. See Herman Kahn, *On Escalation: Metaphors and Scenarios* (Santa Barbara, Calif.: Praeger, 1965).

[8] David E. Sanger, *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age* (New York: Crown, 2018).

[9] Michael C. Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," *Texas National Security Review* 1 (3) (2018): 36–57; Geist and Lohn, *How Might Artificial Intelligence Affect the Risk of Nuclear War?*; Lora Saalman, "Fear of False Negatives: AI and China's Nuclear Posture," *Bulletin of the Atomic Scientists*, April 24, 2018, https://thebulletin.org/2018/04/fear-of-false-negatives-ai-and-chinas-nuclear-posture/; Herbert Lin, "Escalation Risks in an AI-Infused World," in *AI, China, Russia and the Global Order: Technological, Political, Global, and Creative Perspectives*, ed. Nicholas D. Wright (Washington, D.C.: U.S. Department of Defense, 2018), chap. 19; and Vincent Boulanin, ed., *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk* (Stockholm: SIPRI, 2019), https://www.sipri.org/sites/default/files/2019-05/sipri1905-ai-strategic-stability-nuclear-risk.pdf.

[10] Christopher F. Chyba, "Biotechnology and the Challenge to Arms Control," *Arms Control Today*, October 2006, 11–17; Daniel M. Gerstein, *National Security and Arms Control in the Age of Biotechnology* (Lanham, Md.: Rowman & Littlefield, 2013); and Kate Charlet, "The New Killer Pathogens: Countering the Coming Bioweapons Threat," *Foreign Affairs* 97 (3) (2018), https://www.foreignaffairs.com/articles/2018-04-16/new-killer-pathogens.

[11] George Greenstein and Arthur G. Zajonc, *The Quantum Challenge: Modern Research on the Fundamentals of Quantum Mechanics*, 2nd ed. (Boston: Jones & Bartlett, 2006), chap. 9 and 10.

[12] I am grateful for discussions with Eric Snyder about space weapons, stability, and the recent literature. See Garino and Gibson, "Space Systems Threats"; and Harrison, Johnson, and Roberts, *Space Threat Assessment 2019*.

[13] I am grateful to Anne Stickells for discussions of hypersonic weapons. See National Research Council, *U.S. Conventional Prompt Global Strike: Issues for 2008 and Beyond* (Washington, D.C.: The National Academies Press, 2008); Amy Woolf, *Conventional Prompt Global Strike and Long-Range Ballistic Missiles: Background and Issues* (Washington, D.C.: Congressional Research Service, 2018); James M. Acton, "Hypersonic Boost-Glide Weapons," *Science & Global Security* 23 (3) (2015): 191–219; Richard H. Speier, George Nacouzi, Carrie Lee, and Richard M. Moore, *Hypersonic Missile Nonproliferation: Hindering the Spread of a New Class of Weapons* (Santa Monica, Calif.: RAND Corporation, 2017), https://www.rand.org/pubs/research_reports/RR2137.html; Bidwell and MacDonald, *Emerging Disruptive Technologies*; and Wilkening, "Hypersonic Weapons."

[14] Bidwell and MacDonald, *Emerging Disruptive Technologies*. See also Adam Bernstein, George Baldwin, Brian Boyer, et al., "Nuclear Security Applications of Antineutrino Detectors:

Current Capabilities and Future Prospects," *Science & Global Security* 18 (3) (2010): 127–192.

[15] Bidwell and MacDonald, *Emerging Disruptive Technologies*.

[16] Ryan Snyder, "A Proliferation Assessment of Third Generation Laser Uranium Enrichment Technologies," *Science & Global Security* 24 (2) (2016); and Bidwell and MacDonald, *Emerging Disruptive Technologies*.

[17] The adoptive capacity of states, and what determines it, is a central concern of the military technology diffusion literature. See Goldman and Eliason, *The Diffusion of Military Technology*; Horowitz, *The Diffusion of Military Power*; and Horowitz, "Artificial Intelligence." For an argument that the "exponential increase in the complexity of military technology" offsets "the diffusing effects of globalization," at least for certain weapons and states, see Andrea Gilli and Mauro Gilli, "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage," *International Security* 43 (3) (2018/19): 141–189.

[18] I adopt the term "enabling technology" from Horowitz, "Artificial Intelligence."

[19] Robert Carlson, "The Pace and Proliferation of Biological Technologies," *Biosecurity and Bioterrorism* 1 (3) (2003): 203–214; and Robert Carlson, *Causes and Consequences of Bioeconomic Proliferation: Implications for U.S. Physical and Economic Security* (Washington, D.C.: Department of Homeland Security Science and Technology Directorate, 2012), http://www.biodesic.com/s/Carlson_Bioeconomic_Proliferation_Final_edited_for_public_release.pdf.

[20] Chyba, "Biotechnology and the Challenge to Arms Control."

[21] Horowitz, *The Diffusion of Military Power*; and Horowitz, "Artificial Intelligence."

[22] Thomas C. Schelling and Morton H. Halperin, *Strategy and Arms Control* (New York: Twentieth Century Fund, 1961).

[23] Vince Manzo, *Nuclear Arms Control Without a Treaty? Risks and Options After New START*, (Arlington, Va.: CNA, 2019), https://www.cna.org/CNA_files/PDF/IRM-2019-U-019494.pdf; and Brooks, "The End of Arms Control?"

[24] The relevant language reads [italics mine]:

> The United States is now prepared to strengthen its long-standing "negative security assurance" by declaring that the United States will not use or threaten to use nuclear weapons against non-nuclear weapons states that are party to the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) and in compliance with their nuclear non-proliferation obligations....*Given the catastrophic potential of biological weapons and the rapid pace of bio-technology development, the United States reserves the right to make any adjustment in the assurance that may be warranted by the evolution and proliferation of the biological weapons threat and U.S. capacities to counter that threat.* In the case of countries not covered by this assurance–states that possess nuclear weapons and states not in compliance with their nuclear non-proliferation obligations – *there remains a narrow range of contingencies in which U.S. nuclear weapons may still play a role in deterring a conventional or CBW attack against the United States or its allies and partners. The United States is therefore not prepared at the present time to adopt a universal policy that the "sole purpose" of U.S. nuclear weapons is to deter nuclear attack* on the United States and our allies and partners, but will work to establish conditions under which such a policy could be safely adopted.

See U.S. Secretary of Defense, *2010 Nuclear Posture Review Report* (Washington, D.C.: Office of the Secretary of Defense, 2010), 15–16, https://www.hsdl.org/?view&did=777468.

[25] The relevant language reads [italics mine]:

"*There are two forms of uncertainty regarding the future security environment which U.S. nuclear policy, strategy, and posture must take into account.* The first is geopolitical uncertainty.... The second form of uncertainty is technological. This includes the potential for unanticipated technological breakthroughs in the application of existing technologies, or the development of wholly new technologies, that change the nature of the threats we face and the capabilities required to address them effectively. For example, breakthroughs that would render U.S. nuclear forces or U.S. command and control of those forces highly vulnerable to attack would dramatically affect U.S. nuclear force requirements, policy, and posture. *The proliferation of highly-lethal biological weapons is another example*."

See U.S. Secretary of Defense, *Nuclear Posture Review 2018* (Washington, D.C.: Office of the Secretary of Defense, 2018), 14, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.

[26] Defense Intelligence Agency, *Challenges to Security in Space* (Washington, D.C.: Defense Intelligence Agency, 2019), https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

[27] "The difficulty in successful forensics work, especially as part of an attribution process, should not be underestimated. However, the potential for nuclear forensics to play a crucial role in analysis of both pre- and post-detonation materials is enormous." See American Physical Society and the American Association for the Advancement of Science, *Nuclear Forensics: Role, State of the Art, Program Needs* (Washington, D.C.: American Association for the Advancement of Science, 2008), 4.

[28] James M. Acton, "Cyber Warfare & Inadvertent Escalation," *Dædalus* 149 (2) (Spring 2020); and Harrison et al., *Space Threat Assessment*.

[29] For one Chinese view, see Lyu Jinghua, "A Chinese Perspective on the Pentagon's Cyber Strategy: From 'Active Cyber Defense' to 'Defending Forward,'" *Lawfare*, October 19, 2018, https://www.lawfareblog.com/chinese-perspective-pentagons-cyber-strategy-active-cyber-defense-defending-forward.

[30] Donald MacKenzie, *Inventing Accuracy: A Historical Sociology of Nuclear Missile Guidance* (Cambridge, Mass.: The MIT Press, 1990); and Keir Lieber and Daryl Press, "The End of MAD? The Nuclear Dimension of U.S. Primacy," *International Security* 30 (4) (2006): 7–40.

[31] Franz-Stefan Gady, "Lora Saalman on How Artificial Intelligence Will Impact China's Nuclear Strategy," *The Diplomat*, November 7, 2018, https://thediplomat.com/2018/11/lora-saalman-on-how-artificial-intelligence-will-impact-chinas-nuclear-strategy/.

[32] I thank Sadiki Wiltshire for educating me about Chinese progress in quantum encryption. See, for example, "China Launches Quantum Enabled Satellite Micius," BBC News, August 16, 2016, https://www.bbc.com/news/world-asia-china-37091833; and Defense Intelligence Agency, *Challenges to Security in Space*.

[33] Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (New York: Basic Books, 1984); and Scott D. Sagan, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons* (Princeton, N.J.: Princeton University Press, 1993).

[34] Jim Mattis, "Secretary of Defense Jim Mattis Senate Armed Services Committee Written Statement for the Record," April 26, 2018, 13.

[35] Existing warheads from ICBMs and SLBMs are hypersonic, but the term is typically used to refer to new technologies that are not ballistic or not purely ballistic.

[36] Woolf, *Conventional Prompt Global Strike*; Aaron Gregg, "Air Force Awards Massive Hypersonic Contract to Lockheed Martin," *The Washington Post*, April 18, 2018; Ben Brimelow, "Russia, China, and the U.S. Are in a Hypersonic Weapons Arms Race–And Officials Warn the U.S. Could Be Falling Behind," *Business Insider*, April 30, 2018, https://www.businessinsider.com/hypersonic-weapons-us-china-russia-arms-race-2018-4; and Kosuke Takahashi, "Japan Developing Hypersonic Glide Weapon to Defend Remote Islands," *Jane's 360*, September 27, 2018, https://www.janes.com/article/83397/japan-developing-hypersonic-glide-weapon-to-defend-remote-islands.

[37] Acton, "Hypersonic Boost-Glide Vehicles"; Speier et al., *Hypersonic Missile Nonproliferation*; and Wilkening, "Hypersonic Weapons."

[38] Adam Lowther and Curtis McGiffin, "America Needs a 'Dead Hand,'" War on the Rocks, August 16, 2019, https://warontherocks.com/2019/08/america-needs-a-dead-hand/.

[39] As Lowther and McGiffin note in ibid., their suggestion is in some ways reminiscent of the Soviet Union's reported "dead hand" retaliatory system. See David E. Hoffman, *The Dead Hand: The Untold Story of the Cold War Arms Race and Its Dangerous Legacy* (New York: Doubleday, 2009).

[40] Joshua H. Pollack, "Boost-Glide Weapons and U.S.-China Strategic Stability," *The Nonproliferation Review* 22 (2) (2015): 155–164.

[41] Li Bin, "Tracking Chinese Strategic Mobile Missiles," *Science & Global Security* 15 (1) (2007): 1–30.

[42] Dietrich Schroeer, *Science, Technology, and the Arms Race* (New York: John Wiley, 1984), 140–143.

[43] Wilkening, "Hypersonic Weapons."

[44] Daniel R. Coats, *Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community* (Washington, D.C.: Office of the Director of National Intelligence, 2018), https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

[45] James Acton, "Escalation Through Entanglement," *International Security* 43 (1) (2018): 56–99.

[46] Office of the Assistant Secretary of Defense for Homeland Defense & Global Security, *Space Domain Mission Assurance: A Resilience Taxonomy* (Washington, D.C.: Office of the Assistant Secretary of Defense for Homeland Defense & Global Security, 2015), https://fas.org/man/eprint/resilience.pdf. See also James Timbie, "A Way Forward," *Dædalus* 149 (2) (Spring 2020).

[47] An illuminating informal definition of AI is "the use of computers to simulate the behavior of humans that requires intelligence," from Horowitz, "Artificial Intelligence," 40. John McCarthy, one of the founders of AI research, once wryly remarked that "As soon as it works, no one calls it AI anymore." See Bertrand Meyer, "John McCarthy," *Communications of the ACM*, October 28, 2011, https://cacm.acm.org/blogs/blog-cacm/138907-john-mccarthy/fulltext.

[48] I am grateful to Carlton Haelig for highlighting China's dedication to AI. See Gregory C. Allen, *Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial*

Intelligence and National Security (Washington, D.C.: Center for a New American Security, 2019); and Elsa Kania, "Artificial Intelligence in Future Chinese Command Decision-Making," in *AI, China, Russia and the Global Order: Technological, Political, Global, and Creative Perspectives*, ed. Nicholas D. Wright (Washington, D.C.: U.S. Department of Defense and Joint Chiefs of Staff, 2018), chap. 20. Russia's President Putin famously predicted that whoever becomes the leader in AI "will become the ruler of the world." See James Vincent, "Putin Says the Nation that Leads in AI Will Be the Ruler of the World," *Verge*, September 4, 2017; and Samuel Bendett, "The Development of Artificial Intelligence in Russia," in *AI, China, Russia and the Global Order*, chap. 22.

[49] Eliezer Yudkowsy, "Artificial Intelligence as a Positive and Negative Factor in Global Risk," in *Global Catastrophic Risks*, ed Nick Bostrom and Milan M. Cirkovic (Oxford: Oxford University Press, 2008), 308–345; Nick Bostrom, *Superintelligence: Paths, Dangers, Strategies* (Oxford: Oxford University Press, 2014); and Henry A. Kissinger, "How the Enlightenment Ends," *The Atlantic*, June 2018, https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-human-history/559124/.

[50] Bidwell and MacDonald, *Emerging Disruptive Technologies*; and Lieber and Press, "The New Era of Counterforce." Paul Bracken also considers AI fused with big data from persistent surveillance of other, less obviously realizable types, including swarms of oceanic vehicles or data obtained via systematic hacking of other countries' surveillance systems; see Paul Bracken, "The Cyber Threat to Nuclear Stability," *Orbis* 60 (2) (2016): 188–203. See also Austin Long and Brendan Rittenhouse Green, "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy," *Journal of Strategic Studies* 38 (1–2) (2015): 38–73.

[51] Lieber and Press, "The End of MAD?" See also Peter C. W. Flory, Keith Payne, Pavel Podvig, and Alexei Arbatov, "Nuclear Exchange: Does Washington Really Have (or Want) Nuclear Primacy?" *Foreign Affairs* 85 (5) (2006): 149–157; and Jeffrey Lantis, Tom Sauer, James Wirtz, et al., "The Short Shadow of U.S. Primacy?" *International Security* 31 (3) (2006/07): 174–193.

[52] Bidwell and MacDonald, *Emerging Disruptive Technologies*; and Lieber and Press, "The New Era of Counterforce."

[53] I am grateful to David Zikusoka for bringing the following examples to my attention.

[54] Starlink's first tranche of sixty satellites successfully orbited in May 2019. See Shannon Hall, "After SpaceX Starlink Launch, a Fear of Satellites that Outnumber All Visible Stars," *The New York Times*, June 1, 2019, https://www.nytimes.com/2019/06/01/science/starlink-spacex-astronomers.html; Matt Williams, "SpaceX's Starlink Constellation Construction Begins. 2,200 Satellites Will Go Up Over the Next Five Years," *Universe Today*, April 16, 2019, https://www.universetoday.com/141980/spacexs-starlink-constellation-construction-begins-2200-satellites-will-go-up-over-the-next-5-years/; and Caleb Henry, "SpaceX Submits Paperwork for 30,000 More Starlink Satellites," *Space News*, October 15, 2019, https://spacenews.com/spacex-submits-paperwork-for-30000-more-starlink-satellites/.

[55] Union of Concerned Scientists, "UCS Satellite Database," December 8, 2005, https://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database.

[56] See Planet Labs Incorporated, "Defense and Intelligence," https://www.planet.com/markets/defense-and-intelligence/.

[57] See Capella Space, "The Capella 36," https://www.capellaspace.com/technology/.

[58] Li, "Tracking Chinese Strategic Mobile Missiles."

[59] "New ballistic missile systems feature multiple independently targetable reentry vehicles (MIRV) and maneuverable reentry vehicles (MaRV), along with decoys and jamming devices. Russia and China are developing advanced cruise missiles and hypersonic missile capabilities that can travel at exceptional speeds with unpredictable flight paths that challenge existing defensive systems. These are challenging realities of the emerging missile threat environment that U.S. missile defense policy, strategy, and capabilities must address." U.S. Department of Defense, *2019 Missile Defense Review* (Washington, D.C.: Office of the Secretary of Defense, 2019), ii.

[60] M. L. Cummings, "Automation Bias in Intelligent Time Critical Decision Support Systems," presented at AIAA First Intelligent Systems Technical Conference, Chicago, Illinois, September 20–22, 2004, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.91.2634&rep=rep1&type=pdf.

[61] See Timbie, "A Way Forward."

[62] For a related discussion of verifiable space arms control and its limits, see Ross Liemer and Christopher F. Chyba, "A Verifiable Limited Test Ban for Anti-Satellite Weapons," *The Washington Quarterly* 33 (3) (2010): 149–163.

[63] The requirements for effective verification are described in Paul H. Nitze, "Security Challenges Facing NATO in the 1990s," *U.S. Department of State Bulletin* 89 (2145) (1989): 46, http://www.archive.org/download/departmentofstatb89unit/departmentofstatb89unit_bw.pdf.