Assessing the Dangers: Emerging Military Technologies and Nuclear (In)Stability

Michael T. Klare

An Arms Control Association Report

February 2023

Assessing the Dangers: Emerging Military Technologies and Nuclear (In)Stability

An Arms Control Association Report

February 2023

Michael T. Klare

About the Author

Michael T. Klare is a Senior Visiting Fellow at the Arms Control Association, where he focuses on the impacts of emerging technologies on nuclear stability and arms control. From 1985 to 2018, Dr. Klare served as the Five College Professor of Peace and World Security Studies, a joint appointment at Amherst, Hampshire, Mount Holyoke, and Smith Colleges and the University of Massachusetts, Amherst. He is the author of 15 books, including, most recently *All Hell Breaking Loose: The Pentagon's Perspective on Climate Change*.

Acknowledgments

The author would like to thank his colleagues at the Arms Control Association, especially Executive Director Kimball and Senior Policy Analyst Shannon Bugos, for their assistance in making this report possible. Kimball conceived of the "Arms Control Tomorrow" series in *Arms Control Today* which resulted in the original versions of the chapters in this report and later their compilation in a single document; he also read the text and made multiple suggestions for its improvement. Bugos provided the author with invaluable guidance on recent developments in the field and made many beneficial improvements to the final text; she also contributed the tables of U.S., Russian, and Chinese hypersonic weapons on pages 35–36 and the Glossary of Terms on p. 63. ACA nuclear policy intern Heather Foye also assisted by copy editing the text. The author would like to extend special thanks to Allen Harris, production editor, for his skilled and creative work in design and layout of the report.

The author would also like to acknowledge the European Leadership Network and the Samuel Rubin Foundation for their support of the Arms Control Tomorrow research project.

Cover Photo

Cyberwarfare specialists serving with the 175th Cyberspace Operations Group of the Maryland Air National Guard engage in weekend training at Warfield Air National Guard Base, Middle River, Md., June 3, 2017.
(Photo: J.M. Eddins Jr./U.S. Air Force.)

The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.

TABLE OF CONTENTS

Preface

In commencing work on this document, I attended the Kalaris Intelligence Conference at Georgetown University in September 2019. Among the featured speakers at the conference, which focused on the military applications of artificial intelligence (AI), was Lt. Gen. Jack Shanahan, then-director of the Pentagon's Joint Artificial Intelligence Center (JAIC). After expounding for 30 minutes on the benefits of utilizing AI for military purposes, Shanahan opened the floor for questions. Quickly raising my hand, I inquired, "I understand your enthusiasm about exploiting the benefits of AI, but do you have any doubts about employing AI in computerized nuclear command-and-control systems?"

"You will find no stronger proponent of the integration of AI capabilities writ large into the Department of Defense," he responded, "but there is one area where I pause, and it has to do with nuclear command and control." Given the immaturity of technology today, "We have to be very careful. [You need to] give us a lot of time to test and evaluate."

This dichotomy between the impulse to weaponize AI as rapidly as possible and the deep anxiety about the risks in doing so runs throughout the official discourse on what are called "emerging technologies"—which, in addition to artificial intelligence, include robotics, autonomy, cyber, and hypersonics. The military utilization of these technologies, as claimed by their proponents, will provide U.S. military forces with a significant advantage in future wars against other well-armed major powers. At the same time, analysts within and outside the defense establishment have warned about potentially catastrophic consequences arising from their indiscriminate use.

The same dichotomy arises, for example, in the Final Report of the National Security Commission on Artificial Intelligence, submitted to Congress and the White House in February 2021. "Our armed forces' competitive military-technical advantage could be lost within the next decade if they do not accelerate the adoption of AI across their missions," the report warns in its opening pages. To ensure this does not occur, the armed forces must "achieve a state of military AI readiness by 2025." Much of the rest of the 756-page report focuses on proposals for achieving this status—many of which have since been incorporated into legislation or Pentagon directives. But once one reads deep into the report, they will find misgivings of the sort expressed by General Shanahan.

"While the Commission believes that properly designed, tested, and utilized AI-enabled and autonomous weapon systems will bring substantial military and even humanitarian benefit," the report states, "the unchecked global use of such systems potentially risks unintended conflict escalation and crisis instability." In recognition of this danger, the report devoted four pages to a few modest steps for reducing the risk of such dangers, but buried them in a long list of recommendations for accelerating the weaponization of AI.

We at the Arms Control Association believe that appeals for the military utilization of emerging technologies and assessments of their destabilizing and escalatory dangers require a better balance. While not denying that certain advanced technologies may provide potential military benefits, this primer aims to balance the scales by way of a thorough and rigorous appraisal of the likely downsides of such utilization. In particular, it focuses on the threats to "strategic stability" posed by the military use of these technologies—that is, the risk that their use will result in the accidental, unintended, or premature use of nuclear weapons in a great-power crisis.

By publishing this report, we aim to better inform policymakers, journalists, educators, and members of the public about the race to weaponize emerging technologies and the dangers inherent in doing so. While the media and the U.S. Congress have devoted much attention to the purported benefits of exploiting cutting-edge technologies for military use, far less has been said about the risks involved. Hopefully, this primer will help overcome this imbalance by illuminating the many dangers inherent in the unconstrained exploitation of these technologies.

The primer is organized into six chapters, each based on an article that originally appeared in ACA's flagship journal, *Arms Control Today (ACT)*.

Chapter 1, "The Challenges of Emerging Technologies," introduces the concept of "emerging technologies" and summarizes the debate over their utilization for military purposes and their impact on strategic stability. It highlights the centrality of artificial intelligence in many of these advances, particularly the development of autonomous or "unmanned" weapons systems. Chapter 1 also provides a brief overview of the four technologies given close examination in this report: autonomous weapons systems, hypersonic weapons, cyberweapons, and automated battlefield decision-making systems. This chapter is based on an article that first appeared in the December 2018 issue of *ACT*.

Chapter 2, "Autonomous Weapons Systems and the Laws of War," focuses on lethal autonomous weapons systems. Devices of this sort combine combat platforms of varying sorts—planes, tanks, ships, and so on—with AI software enabling them to survey their surroundings, identify possible enemy targets, and, under certain predetermined conditions, independently decide to attack those targets. This chapter identifies the types of unmanned weapons now being developed and deployed by the major powers and discusses the moral and ethical objections about their use, as well as their potential conflict with the laws of war. This chapter is based on an article that first appeared in the March 2019 issue of *ACT*.

Chapter 3, "An 'Arms Race in Speed': Hypersonic Weapons and the Changing Calculus of Battle," examines hypersonic weapons, or projectiles that fly at more than five times the speed of sound (Mach 5). Projectiles of this sort appeal to military officials given their speed and maneuverability, but also pose a threat to strategic stability by endangering key defensive assets of nuclear-armed states, possibly leading to the premature use of nuclear weapons. This chapter is based on an article that first appeared in the June 2019 issue of *ACT*.

Chapter 4, "Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation," looks at cyberspace and the dangers arising from the offensive use of cyberweapons in a great-power conflict. As the chapter suggests, a cyberattack on an adversary's nuclear command, control, and communications systems during such a crisis might lead the target state to believe it faces an imminent nuclear attack and so prompt it to launch its own nuclear weapons. This chapter is based on an article that first appeared in the November 2019 issue of *ACT*.

Chapter 5, "'Skynet' Revisited: The Dangerous Allure of Nuclear Command Automation," considers the implications of automating combat decision-making systems. While such systems—such as the Pentagon's Joint All-Domain Command-and-Control (JADC2) enterprise—could theoretically help battlefield commanders cope with the deluge of incoming information they are often confronted with, they might also usurp the role of humans in combat decision-making, leading to accidental or inadvertent escalation. This chapter is based on an article that first appeared in the April 2020 issue of *ACT*.

Finally, Chapter 6, "A Framework Strategy for Reducing the Escalatory Dangers of Emerging Technologies," summarizes the analyses articulated in the first five chapters and provides an overarching strategy for curtailing the indiscriminate weaponization of emerging technologies. While no single approach can adequately meet a challenge of this magnitude, a constellation of targeted measures—ranging from awareness-raising to unilateral actions, Tracks 2 and 1.5 diplomacy, strategic stability talks, confidence-building measures, and formal agreements—could, in time, slow the pace of weaponization and bolster strategic stability. This chapter is based on an article that first appeared in the December 2020 issue of *ACT*.

As General Shanahan indicated in 2019, the initiation of nuclear combat represents the "ultimate human decision." During the Cold War, the world's top leaders came face-to-face with the risk of Armageddon, prompting significant arms control efforts to reduce that risk. Today, however, developments in geopolitics and technology are again increasing the danger of nuclear weapons use. We hope that this primer will help readers understand the technological aspects of this danger and spur them to advocate for reasonable limitations on the military use of destabilizing technologies.

—Michael T. Klare
Senior Visiting Fellow, Arms Control Association,
February 2023

Executive Summary

Increasingly in recent years, the major powers have sought to exploit advanced technologies—artificial intelligence (AI), autonomy, cyber, and hypersonics, among others—for military purposes, with potentially far-ranging, dangerous consequences. Similar to what occurred when chemical and nuclear technologies were first applied to warfare, many analysts believe that the military utilization of AI and other such "emerging technologies" will revolutionize warfare, making obsolete the weapons and the strategies of the past. In accordance with this outlook, the U.S. Department of Defense is allocating ever-increasing sums to research on these technologies and their application to military use, as are the militaries of the other major powers.

But even as the U.S. military and those of other countries accelerate the exploitation of new technologies for military use, many analysts have cautioned against proceeding with such haste until more is known about the inadvertent and hazardous consequences of doing so. Analysts worry, for example, that AI-enabled systems may fail in unpredictable ways, causing unintended human slaughter or uncontrolled escalation.

Of particular concern to arms control analysts is the potential impact of emerging technologies on "strategic stability," or a condition in which nuclear-armed states eschew the first use of nuclear weapons in a crisis. The introduction of weapons employing AI and other emerging technologies could endanger strategic stability by blurring the distinction between conventional and nuclear attack, leading to the premature use of nuclear weapons.

Animated by such concerns, arms control advocates and citizen activists in many countries have sought to slow the weaponization of AI and other emerging technologies or to impose limits of various sorts on their battlefield employment. For example, state parties to the Convention on Certain Conventional Weapons (CCW) have considered proposals to ban the development and the deployment of lethal autonomous weapons systems—or "killer robots," as they are termed by critics. Other approaches to the regulation of emerging technologies, including a variety of unilateral and multilateral measures, have also advanced in recent years.

AI and Autonomous Weapons Systems

Among the most prominent applications of emerging technologies to military use is the widespread introduction of autonomous weapons systems—devices that combine AI software with combat platforms of various sorts (ships, tanks, planes, and so on) to identify, track, and attack enemy targets on their own. Typically, these systems incorporate software that determines the parameters of their operation, such as the geographical space within which they can function and the types of target they may engage, and under what circumstances.

At present, each branch of the U.S. military, and the forces of the other major powers, are developing—and in some cases fielding—several families of autonomous combat systems, including unmanned aerial vehicles (UAVs), unmanned ground vehicles (UGVs), unmanned surface vessels (USVs), and unmanned undersea vessels (UUVs).

The U.S. Navy, for example, intends to employ a fleet of USVs and UUVs to conduct reconnaissance operations in contested areas and, if war breaks out, launch antiship and land-attack missiles against enemy targets. The U.S. Air Force has embraced a "loyal wingman" approach, whereby armed UAVs will help defend manned aircraft when flying in contested airspace by attacking enemy fighters. The U.S. Army seeks to reduce the dangers to its frontline troops by developing a family of robotic combat systems, including, eventually, a robotic tank. Russian and Chinese forces are developing and deploying unmanned systems with similar characteristics.

The development and the deployment of lethal autonomous weapons systems like these raise significant moral and legal challenges. To begin with, such devices are being empowered to employ lethal force against enemy targets, including human beings, without significant human oversight—moves that run counter to the widely-shared moral and religious principle that only humans can take the life of another human. Critics also contend that the

A Chinese WZ-8 hypersonic reconnaissance drone is on display at the 13th China International Aviation and Aerospace Exhibition (Airshow China 2021) on September 28, 2021 in Zhuhai, Guangdong Province of China. (Photo by Chen Wen/China News Service via Getty Images)

weapons will never be able to abide by the laws of war and international humanitarian law, as spelled out in the Hague Conventions of 1899 and 1907 and the Geneva Convention and 1949. These statutes require that warring parties distinguish between combatants and non-combatants when conducting military operations and employ only as much force as required to achieve a specific military objective. Proponents of autonomous weapons claim that the systems will, in time, prove capable of making such distinctions in the heat of battle, but opponents insist that only humans possess this ability, and so all such devices should be banned.

In recognition of these dangers, a concerted effort has been undertaken under the aegis of the CCW to adopt an additional protocol prohibiting the deployment of lethal autonomous weapons systems. As the CCW operates by consensus and state parties have opposed such a measure, proponents of a ban are exploring other strategies for their prohibition, such as an international treaty under UN General Assembly auspices. Some members of the European Union have also proposed a non-binding code of conduct covering LAWS deployment, requiring continuous human supervision of their use in combat.

Hypersonic Weapons

Hypersonic weapons are usually defined as missiles than can travel at more than five times the speed of sound (Mach 5) and fly at lower altitudes than intercontinental ballistic missiles (ICBMs), which also fly at hypersonic speeds. At present, the United States, China, Russia, and several other countries are engaged in the development and fielding of two types of hypersonic weapons (both of which may carry either nuclear or conventional warheads): hypersonic glide vehicles (HGVs), unpowered projectiles that "glide" along the Earth's outer atmosphere after being released from a booster rocket; and hypersonic cruise missiles (HCMs), which are powered by high-speed air-breathing engines, called "scramjets."

Weapons of these types possess several capabilities that make them attractive to military officials. Due to their high speed and superior maneuverability,

hypersonic missiles can be used early in a conflict to attack high-value enemy assets, such as air-defense radars, missile batteries, and command-and-control (C2) facilities. Since hypersonic missiles fly closer to the Earth than ICBMs and possess greater maneuverability, they may be capable of evading anti-missile systems designed to work against other types of offensive weapons.

All three major powers have explored similar types of hypersonic missiles, but their strategic calculations in doing so appear to vary: The United States currently seeks such weapons for use in a regional, non-nuclear conflict, whereas China and Russia appear to be emphasizing their use in nuclear as well as conventional applications.

The U.S. Air Force has undertaken the development of two such missiles for use in a regional context: the Air-Launched Rapid Response Weapon (ARRW), slated to be the first U.S. hypersonic weapon to enter service, and the hypersonic attack cruise missile (HACM). Concurrently, the U.S. Army and Navy have been working jointly on a common hypersonic boost-glide vehicle for use by both services, along with booster rockets to carry the HGV into the atmosphere. Russia has deployed the nuclear-armed Avangard HGV on a number of its SS-19 Stiletto ICBMs, while China has tested the Dongfeng-17 (DF-17), a medium-range ballistic missile fitted with a dual-capable (nuclear or conventional) HGV warhead.

While most of these weapons programs remain in the development or early deployment stage, their presence has already sparked concerns among policymakers and arms control advocates regarding their potential impact on strategic stability. Analysts worry, for example, that the use of hypersonic weapons early in a conventional engagement to subdue an adversary's critical assets could be interpreted as the prelude to a nuclear first-strike, and so prompt the target state to launch its own nuclear munitions if unsure of its attacker's intentions.

At present, there is no established venue in which officials of China, Russia, and the United States can meet to discuss formal limits on hypersonic weapons. The U.S.-Russia Strategic Stability Dialogue could serve as a possible forum for direct talks between government officials on these topics. While Washington paused the dialogue following Russia's invasion of Ukraine, the two sides should return to the table as soon as circumstances allow. A U.S.-China strategic dialogue, if and when established, could address similar concerns.

Cyberattack and Nuclear C3

The cyberspace domain—while immensely valuable for a multitude of public, private, and commercial functions—has also proven to be an attractive arena for great-power competition, given the domain's vulnerability to a wide variety of malicious and aggressive activities. These range from cyberespionage, or the theft of military secrets and technological data, to offensive actions intended to disable an enemy's command, control, and communications (C3) systems, thereby degrading its ability to wage war successfully. Such operations might also be aimed at an adversary's nuclear C3 (NC3) systems; in such a scenario, one side or the other—fearing that a nuclear exchange is imminent—could attempt to minimize its exposure to attack by disabling its adversary's NC3 systems.

With the proliferation of cyberweapons creating new and severe threats to strategic stability, policymakers bear responsibility for developing strategies to prevent accidental and unintended escalation.

Analysts warn that any cyberattack on an adversary's NC3 systems in the midst of a major crisis or conventional conflict could prove highly destabilizing. Upon detecting interference in its critical command systems, the target state might well conclude that an adversary had launched a pre-emptive nuclear strike against it, and so might launch its own nuclear weapons rather than risk their loss to the other side.

The widespread integration of conventional with nuclear C3 compounds these dangers. For reasons of economy and convenience, the major powers have chosen to rely on the same early-warning and communications links to serve both their nuclear and conventional forces—a phenomenon described by James Acton of the Carnegie Endowment for International Peace as "entanglement." In the event of a great-power conflict, one side or the other might employ cyberweapons to disable the conventional C3 systems of its adversary in the opening stages of a nonnuclear assault, but its opponent—possibly fearing that its nuclear systems are the intended target—might launch its nuclear weapons prematurely.

The utilization of cyberspace for military purposes poses significant challenges for arms control. Existing

means of inspection and verification cannot currently detect cyberweapons, whose very existence is often hard to prove. With the proliferation of cyberweapons creating new and severe threats to strategic stability, policymakers bear responsibility for developing strategies to prevent accidental and unintended escalation. Some of the most effective, stabilizing measures, analysts agree, would be U.S.-Russian and U.S.-Chinese bilateral agreements to abstain from cyberattacks on each other's NC3 systems.

Automated Battlefield Decision-Making

With the introduction of new hypersonic weapons and other highly capable conventional weapons, the pace of warfare will likely increase and, as a result, exacerbate the pressure on battle commanders to make rapid combat decisions. In response, the militaries of the major powers plan to rely increasingly on AI-enabled battlefield decision-making systems to aid human commanders in processing vast amounts of data on enemy movements and identifying possible combat responses.

Within the U.S. military, the principal mechanism for undertaking the development of automated systems of this sort is the Joint All-Domain Command and Control (JADC2) program. Overseen by the Air Force under its Advanced Battlefield Management System, JADC2 is envisioned as a constellation of computers working together to collect sensor data from myriad platforms, organize the data into digestible chunks, and provide commanders with a menu of possible combat options. While JADC2 is initially intended for conventional operations, the program will eventually connect to the nation's NC3 systems.

The increased automation of battlefield decision-making, especially given the likely integration of nuclear and conventional C3 systems, gives rise to numerous concerns. Many of these technologies are still in their infancy and prone to often unanticipated malfunctions. Skilled professionals can also fool, or "spoof," AI-enabled systems, causing unintended and possibly dangerous outcomes. Furthermore, no matter how much is spent on cybersecurity, computer systems will always remain vulnerable to hacking by sophisticated adversaries.

Given these risks, Chinese, Russian, and U.S. policymakers should be leery of accelerating the automation of their C3 systems. Ideally, government officials and technical experts of the three countries should meet—presumably in a format akin to the U.S.-Russian Strategic Stability Dialogue—to consider limitations on the use of any automated decision-making devices with ties to nuclear command systems. Until meetings of this sort become feasible, experts

An unmanned Boeing MQ-25 T1 Stingray test aircraft, left, refuels a manned F/A-18 Super Hornet, June 4, 2021, near MidAmerica Airport in Mascoutah, Illinois. (U.S. Navy photo courtesy of Boeing)

from these countries should meet in neutral venues to identify the dangers inherent in reliance on such systems and explore various measures for their control.

A Framework Strategy for Reducing the Escalatory Dangers of Emerging Technologies

Military leaders of the major powers aim to exploit the perceived benefits of emerging technologies as rapidly as possible, in the belief that doing so will give them a combat advantage in future great-power conflicts. However, this drive to exploit emerging technologies for military use has accelerated at a much faster pace than efforts to assess the dangers they pose and to establish limits on their use. It is essential, then, to slow the pace of weaponizing these technologies, to carefully weigh the risks in doing so, and to adopt meaningful restraints on their military use.

Given the variety and the complexity of the technologies involved in this endeavor, no single overarching treaty or agreement will likely be able to institute restraints on all of the technologies involved. Thus, leaders of the relevant countries should focus on adopting a *framework strategy*, aimed at advancing an array of measures which, however specific their intended outcome, all contribute to the larger goal of preventing unintended escalation and enhancing strategic stability.

In devising and implementing such measures, policymakers can proceed in a step-by-step fashion, from more informal, non-binding measures to increasingly specific, binding agreements. The following proposed action steps are derived from the toolbox developed by arms control advocates over many years of practice and experimentation.

- *Awareness-Building:* Efforts to educate policymakers and the general public about the risks posed by the unregulated military use of emerging technologies.
- *Track 2 and Track 1.5 Diplomacy:* Discussions among scientists, engineers, and arms control experts from the major powers to identify the risks posed by emerging technologies and possible strategies for their control. "Track 2 diplomacy" of this sort can be expanded at some point to include governmental experts ("Track 1.5 diplomacy").
- *Unilateral and Joint Initiatives:* Steps taken by the major powers on their own or among groups of like-minded states to reduce the risks associated with emerging technologies in the absence of formal arms control agreements to this end.
- *Strategic Stability Talks:* Discussions among senior officials of China, Russia, and the United States on the risks to strategic stability posed by the weaponization of certain emerging technologies and on joint measures to diminish these risks. These can be accompanied by *confidence-building measures* (CBMs), intended to build trust in implementing and verifying formal agreements in this area.
- *Bilateral and Multilateral Arrangements:* Once the leaders of the major powers come to appreciate the escalatory risks posed by the weaponization of emerging technologies, it may be possible for them to reach accord on bilateral and multilateral arrangements intended to minimize these risks.

The failure to adopt such measures will allow for the application of cutting-edge technologies to military systems at an ever-increasing tempo, greatly magnifying the risks to world security. A more thorough understanding of the distinctive threats to strategic stability posed by certain destabilizing technologies and the imposition of restraints on their military use would go a long way toward reducing the risks of Armageddon.

Chapter 1:
The Challenges of Emerging Technologies

In seemingly every other generation, humans develop new technologies that alter the nature of warfare and pose fresh challenges for those seeking to reduce the frequency, destructiveness, and sheer misery of violent conflict. During World War I, advances in chemical processing were utilized to develop poisonous gases for battlefield use, causing massive casualties; after the war, horrified citizenries pressed their leaders to sign the Geneva Protocol of 1925, which prohibits the use of asphyxiating, poisonous, and other lethal gases in war. Thirty years later, World War II witnessed the tragic application of nuclear technology to warfare, again resulting in massive human death and suffering; this, too, inspired vigorous international efforts to ban or restrict the use of such munitions.

Today, a whole new array of technologies—artificial intelligence (AI), robotics, cyber, and hypersonics, among others—is being applied to military use, with potentially far-ranging consequences. As was the case when chemical and nuclear technologies were first applied to warfare, many analysts believe that the military utilization of AI and other such "emerging" technologies will revolutionize warfare, making obsolete the weapons and strategies of the past. "AI will transform all aspects of military affairs," the National Security Commission on Artificial Intelligence (NSCAI) affirmed in its Final Report of March 2021. "The sources of battlefield advantage will shift from traditional factors like force size and levels of armaments to factors like superior data collection and assimilation, connectivity, computing power, algorithms, and system security."[1]

This prospect has provoked widespread interest and excitement among military officials in the United States and the other major powers. On one hand, senior officers are keen to exploit the purported capabilities of the new technologies for battlefield advantage; on the other, they fear similar strides by rival powers, potentially putting them at a disadvantage. In a characteristic expression of this outlook, Chairman of the Joint Chiefs of Staff General Mark A. Milley affirmed in 2021 that "the country that masters those technologies, combines them with their doctrine, develops their leadership to take maximum advantage of them, is likely going to have significant—perhaps even decisive—advantage at the beginning of the next war."[2]

In accordance with this outlook, the U.S. Department of Defense is allocating ever-increasing sums to research on the underlying science of key emerging technologies and to their application for military use. Priorities for the department include artificial intelligence, autonomous (or "unmanned") weaponry, hypersonic missiles, automated battlefield decision-making systems, and cyberweapons. In its budget request for fiscal year (FY) 2023, for example, the department sought $3.0 billion for unmanned air and sea vehicles, $4.7 billion for hypersonic weapons, $11.1 billion for cybersecurity operations, and $1.1 billion for "core AI" research.[3]

But even as the Department of Defense—and the militaries of the other major powers—rush ahead with the weaponization of advanced technologies, many analysts and policymakers have cautioned against moving with such haste until more is known about how the various military capabilities stemming from these technologies may lead to unintended and hazardous outcomes. Non-military devices governed by AI, such as self-driving cars and facial-recognition systems, have been known to fail in dangerous and unpredictable ways; should similar failures occur among AI-empowered weaponry during wartime, the outcomes could include the unintended slaughter of civilians or the outbreak of nuclear war. As suggested by Eric Schmidt, the former chief executive officer of Google, "even those powers creating or wielding an AI-designed or AI-operated weapon may not know exactly how powerful it is, or what it will do in a given situation."[4]

Animated by such concerns, policymakers, arms control advocates, and citizen activists in many countries have sought to slow the weaponization of AI and other emerging technologies, or to

More than 800 service members and civilians took part in Cyber Shield 18, an Army National Guard training exercise at Camp Atterbury, Indiana from May 6–18, 2018. (Photo: Staff Sgt. Jeremiah Runser/U.S. Army Cyber Command)

institute rules of use or limits of various sorts on their battlefield employment. State parties to the Convention on Certain Conventional Weapons (CCW), for example, have considered measures to limit or prohibit the development and deployment of autonomous weapons systems—or "killer robots," as they are termed by critics. The United Nations has pursued the adoption of limits on the military use of cyberweapons, while the U.S. and Russia have discussed the possibility of addressing, potentially through arms control, the destabilizing impacts of hypersonic weapons in future iterations of their "strategic security dialogue."

Such efforts are being hampered, however, by the desire of senior military officials in the United States, Russia, China, and several other countries to rapidly exploit the potential battlefield applications of emerging technologies. Indeed, Russia is reported to have made widespread use of hypersonic missiles and cyberweapons during its February 2022 invasion of Ukraine (though to arguably limited effect), and the U.S. and its allies supplied Ukraine with a variety of sophisticated attack and reconnaissance drones. As the war in Ukraine was raging, moreover, Secretary of Defense Lloyd J. Austin III affirmed that emerging technologies will play an ever-increasing role in U.S. military strategy. Exploiting these technologies for military use, he declared at a regional security conference in Singapore, "holds out the promise of progress across a range of emerging tech areas that can bolster our deterrence, from AI to hypersonics."[5]

As during World Wars I and II, the major powers are rushing ahead with the weaponization of advanced technologies before they have fully considered—let alone attempted to mitigate—the consequences of doing so, including the risk of significant civilian casualties and the accidental or inadvertent escalation of conflict. Given these perils, it is essential that policymakers, educators, and the general public become more familiar with the new technologies and the implications of their future use.

Emerging Technologies and Strategic Stability

What constitutes an "emerging technology"? While there is no formal definition of such a category, the Congressional Research Services (CRS) of the Library of Congress has described a number of scientific and technical fields that might fall under this heading, including AI, lethal autonomous

weapons, hypersonics, and quantum computing. These technologies stand out, it explained, because they "could have a *disruptive impact* on U.S. national security in the years to come" (emphasis added).[6]

Running through this and other assessments of the field is the notion that AI and other emerging technologies will have a "disruptive" impact on all existing aspects of military planning and organization, and on the conduct of war itself. "To compete, deter, and if necessary fight and win" on future battlefields, the National Security Commission on Artificial Intelligence (NSCAI) suggested in 2021, America's military will require "wholesale adjustments to operational concepts, technologies, organizational structures, and how we integrate allies and partners into operations."[7]

Emerging technologies are also viewed as "disruptive" because they potentially endanger strategic stability, a vital aspect of the existing nuclear order. Although there is no accepted formal definition of strategic stability, it is usually said to denote a condition in which nuclear-armed states have no incentive to strike first in a crisis. As suggested by Prof. Christopher F. Chyba of Princeton University, strategic stability implies that even when engaged in non-nuclear combat, nuclear-armed adversaries will eschew the first use of nuclear weapons because they understand that any such strike will lead to devastating nuclear retaliation.[8]

Although never entirely free from risk, strategic stability is thought to face new and unprecedented hazards from the introduction of weapons employing certain emerging technologies, such as AI, cyber, and hypersonics. Such weapons, it is feared, could blur the distinction between conventional and nuclear attack, leading a nuclear-armed state to misinterpret an enemy's non-nuclear operations as the prelude to a nuclear attack and so launch its own atomic munitions for fear of losing them entirely. A hypersonic missile strike on a nation's key command-and-control (C2) centers, for example, might be perceived as the initial move in a nuclear attack and so prompt an escalatory response; a cyberattack on such C2 systems could produce comparable fears and cause a similar escalatory outcome.[9] "There is a dark side to the new technologies," said Heiko Maas, then Germany's minister for foreign affairs, at a November 2020 conference on the topic. "Their military use in future conflict could threaten strategic stability and lead to devastating consequences."[10]

And it is not only strategic stability that is said to be threatened by the introduction of emerging technologies: many analysts also worry about the progressive loss of human control over the weapons use and the conduct of war itself. The expanded employment of AI, cyber, hypersonics, and autonomous weaponry on the future battlefield is bound to increase the pace and complexity of combat operations, undermining humans' control over the fighting by forcing them to rely increasingly on machines for help in battlefield management, data-processing, and decision-making, with potentially catastrophic consequences. "Greater reliance on automated capabilities, combined with the intense decision-making time pressures that attend operations conducted at machine speeds, could lead to rapid and even unintended escalation," Eric Schmidt warned in a 2022 essay.[11]

In this report, we use "emerging technologies" as shorthand for a range of scientific and technical developments that, if applied to military use, are likely to have a transformative impact on the future of warfare in ways that are unpredictable and potentially hazardous. We focus in particular on four such fields: AI-enabled autonomous weapons, hypersonic missiles, cyberweapons, and automated command-and-control systems. These four were chosen for intensive study because they entail a potential threat to strategic stability and human control, and because they are the closest to being employed in actual combat. Particular attention is also paid to the pivotal role of artificial intelligence, as it figures prominently in the design, development, and use of all the others.

Artificial Intelligence

What is artificial intelligence, and why does it play such a significant role in our investigation? Although there is no accepted common definition for artificial intelligence, it is usually said to encompass the software systems used to invest machines with an ability to monitor their surroundings—whether in the material world or cyberspace—and to take independent action in response to various stimuli. Congress, in authorizing increased Pentagon research in this field, defined AI as "an artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision-making, and acting.[12]

Crucial to the application of AI to military use is the development of ever-more capable algorithms—computer programs that have been "trained" through exposure to vast troves of data to identify various external patterns and select particular responses to them based on a menu of possible options. As explained by the CRS, this approach to AI, called machine learning, "involves statistical algorithms that replicate human cognitive tasks by deriving their own procedures through analysis of large training data sets."[13]

Algorithms can be developed to manage a wide variety of devices and processes, including both

physical objects like tanks and planes, as well as purely digital systems, such as cyberweapons and automated communications networks. In this sense, AI is viewed as an "omni-use" technology, applicable to a wide spectrum of potential military functions. These run the gamut from relatively mundane tasks like logistical and maintenance oversight to such combat-related functions as surveillance, intelligence analysis, target identification, and autonomous drone strikes. Algorithms have also been developed to permit "swarming," or the use of drone ships or planes in self-directed ensembles, able to communicate and coordinate their movements with one another.

Many analysts believe that AI will revolutionize warfare by allowing military commanders to supplement or, in some cases, replace their human-crewed weapons with a wide variety of unmanned systems. As warfare among the major powers grows increasingly fast-paced, moreover, battle commanders are likely to place ever-greater reliance on AI-enabled machines to monitor enemy actions, evaluate the trove of information that is collected, and initiate appropriate countermeasures. "AI applications will help militaries prepare, sense and understand, decide, and execute faster and more efficiently," the NSCAI affirmed in its 2021 report. "In the future, warfare will pit algorithm against algorithm."[14]

In consonance with this assessment, senior Pentagon officials insist that mastering AI and applying it to a wide variety of military functions will prove essential as the United States faces ever-more capable adversaries in the years ahead. "AI holds tremendous promise to improve the ability and function of nearly all systems and operations," The Department of Defense noted in its budget request for FY 2023. "Tomorrow's AI must further accelerate these capabilities, while . . . discovering new applications through scientific discovery and expediting the Department's modernization efforts."[15]

But while the U.S. military and those of many other countries have pursued the application of artificial intelligence to combat functions with great enthusiasm, many analysts have expressed concern about the many dangers of doing so. Even after extensive training, advanced algorithms have been known to make significant errors in identifying objects (or people), and scientists still do not know

A Chinese Yilong II (Wing-Loong II) reconnaissance-strike drone demonstrates on the opening day of the 13th China International Aviation and Aerospace Exhibition (Airshow China 2021) on September 28, 2021 in Zhuhai, Guangdong Province of China. (Photo by VCG via Getty Images)

how these systems arrive at their decisions. Like other cyber-dependent systems, moreover, AI-enabled machines are vulnerable to hacking and sabotage.[16]

Despite these concerns, the U.S. Department of Defense and the militaries of other major powers are proceeding aggressively to employ artificial intelligence in a wide variety of military systems. Its growing importance will be evident in many of the technologies discussed below, but especially in the development of autonomous weapons systems.

Autonomous Weapons Systems

Autonomous weapons systems combine AI software and combat platforms of various sorts—tanks, planes, ships, and so on—to identify, track, and attack enemy assets on their own. As defined by the U.S. Defense Department, such a device is "a weapons system that, once activated, can select and engage targets without further intervention by a human operator."[17] Typically, weapons of this sort are only enabled to conduct these activities within certain parameters programed into the software, such as the geographical space within which they can operate or the types of targets they can engage.[18]

At present, the U.S. military, and those of the other major powers, are developing—and in some cases fielding—unmanned aerial vehicles (UAVs), unmanned surface vessels (USVs), unmanned underwater vessels (UUVs), and unmanned ground vehicles (UGVs). In its budget request for FY 2023, for example, the U.S. Department of Defense requested $2 billion for the development and procurement of a carrier-based UAV, the MQ-25A Stingray, along with $400 million for development work on prototype USVs and UUVs plus an additional $116 million for the development of UGVs.

Russia and China are also known to be developing and deploying autonomous systems of these types. Russia, for example, has developed a family of robotic tanks, including the Uran-6 and Uran-9, some of which reportedly saw service in Syria and Ukraine. China, for its part, has developed a family of combat UAVs, and deployed some in flights across the median line in the Taiwan Strait between China and Taiwan.

The development and deployment of fully autonomous weapons systems like these raise significant moral and legal challenges for the countries involved and the international community. In essence, such weapons are being empowered to employ lethal force against enemy targets, potentially including human beings, without substantial human oversight—moves that run counter to the widely-shared moral and religious principle that only humans can take the life of another human, and only under certain highly constrained circumstances. Although proponents of autonomous weapons contend that humans do bear ultimate responsibility for the actions of such systems (by inserting limiting conditions into the weapons' software), many critics find such claims insufficient and argue that they be banned altogether.[19]

Even putting aside the moral objections to such devices, many critics also contend that they will not be able to abide by the laws of war and international humanitarian law, as spelled out in the Hague Conventions (1899 and 1907) and Geneva Convention (1949). As will be explained further in Chapter 2, these "conventions," or treaties, require signatory states to distinguish between civilians and combatants on the battlefield and, to the greatest degree possible, avoid unnecessary injury to the former. Critics of autonomous weapons avow that they will never be able to distinguish between combatants and noncombatants on a chaotic urban battlefield, and so have joined in calls for their prohibition.[20]

Given the magnitude of these concerns, the development of autonomous weapons systems has attracted more attention from policymakers and arms control advocates than most of the emerging technologies. As will be discussed in Chapter 2, the signatories to the Convention on Certain Conventional Weapons have convened several expert groups to consider possible limitations on the production and deployment of such systems, and several dozen states—along with representatives of civil society—have called for an international ban on their use.

Hypersonic Weapons

Hypersonic weapons are usually defined as missiles than can travel at more than five times the speed of sound (Mach 5). Most traditional ballistic missiles, including all intercontinental ballistic missiles (ICBMs), fly at hypersonic speeds, whereas most traditional cruise missiles fly at subsonic (less than Mach 1) or supersonic speeds (Mach 1 to 5). In practice, and for the purpose of this report, "hypersonic weapons" will refer to missiles that fly at lower altitudes than ICBMs and greater altitudes than traditional cruise missiles.[21]

At present, the United States, China, and Russia (along with a number of other countries) are engaged in the development and fielding of two types of hypersonic weapons, both of which can be armed with either nuclear or conventional warheads: hypersonic glide vehicles (HGVs), or unpowered projectiles that "glide" along the Earth's outer atmosphere after being released from a booster rocket, and hypersonic cruise missiles (HCMs), or missiles powered by high-speed air-breathing engines, called "scramjets."[22]

Weapons of these types possess several capabilities that make them attractive to defense planners. Because

of their high speed and superior maneuverability, hypersonic missiles can be used early in a conflict to attack critical enemy assets, such as air-defense radars, missile batteries, and command-and-control (C2) facilities; they can also be used to strike mobile assets, such road-mobile missiles and ships in port. Because they fly closer to the Earth than ICBMs and are highly maneuverable, such missiles may be able to evade anti-missile systems designed to work against other offensive weapons.[23]

As will be further discussed in Chapter 3, the major powers are being motivated by several factors to acquire weapons of these types. President Vladimir Putin, for example, has claimed that Russia must install hypersonic glide vehicles on some of its ICBMs to ensure Moscow's capacity to execute a second-strike retaliatory attack in the event of a U.S. nuclear strike, even in the face of enhanced U.S. ballistic missile defenses. Although Chinese officials have not been as forthright in explaining their motives for acquiring hypersonic weapons, some Chinese analysts have suggested that the Chinese leadership shares Putin's concerns about the need to overcome future U.S. missile defenses when conducting a retaliatory second strike. But whereas Russian and Chinese leaders tend to stress the role of hypersonic weapons in strategic nuclear encounters, U.S. officials have tended to emphasize their utility in a regional, non-nuclear context, saying they are needed to overcome Chinese and Russian threats to U.S. combat forces.[24]

Spurred by these, and related considerations, the three major nuclear-armed powers have all invested in the development of multiple types of hypersonic weapons and, in some cases, have begun to deploy them. Russia, for example, has deployed the Avangard HGV on a number of its SS19 Stiletto ICBMs and is expected to install additional numbers on the Sarmat extra-heavy ICBM when it becomes operational in late 2022. Russia has also fielded the Kinzhal ("Dagger"), a maneuvering air-launched ballistic missile, reportedly

A missile carrying a common hypersonic glide body launches from the Pacific Missile Range Facility in Hawaii on March 19, 2020. (Photo by U.S. Department of Defense)

firing some on targets in western Ukraine.[25] China has tested a number of hypersonic weapons, including the Dongfeng-17 (DF-17), a road-mobile medium-range ballistic missile fitted with a "dual-capable" (either nuclear or conventional) HGV warhead.[26]

The United States has developed and is testing a variety of conventionally-armed hypersonic weapons, with each of the military services seeking to acquire some for their own specific military purposes. The Air Force, stressing the potential use of hypersonic weapons in attacking "time-sensitive" targets such as mobile ballistic missiles, has pursued the development of two such munitions: the AGM-183 Air-Launched Rapid Response Weapon (ARRW), which is slated to be the first U.S. hypersonic weapon to enter service, and the hypersonic attack cruise missile (HACM). The Army and Navy, citing the threat to their conventional forces posed by growing numbers of Chinese and Russian medium-range ballistic missiles, are working jointly on a common hypersonic boost-glide vehicle for use by both services along with booster rockets to carry the HGV into the outer atmosphere. These initiatives include the Navy-funded Conventional Prompt Strike (CPS) program and the Army's Long-Range Hypersonic Weapon (LRHW). To sustain all these programs, the Department of Defense requested $4.7 billion for hypersonic research in FY 2023, a 24% increase over the FY 2022 request of $3.8 billion.[27]

Although most of these weapons programs are still in the development or early deployment stage, they have already raised concerns among policymakers and arms control advocates regarding their potential impact on escalatory dynamics and strategic stability. Analysts worry, for example, that the use of hypersonic weapons early in a conventional engagement to subdue an adversary's critical assets could be interpreted as the prelude to a nuclear first-strike, prompting the target state to keep its nuclear arms on a high-alert status and to launch them quickly if unsure of its attacker's intentions.[28]

Many analysts are also troubled by the fact that the major powers are rushing to acquire these new hypersonic missiles without having a clear concept of how they will be used in battle but simply out of concern that their rivals may deploy such weapons ahead of them. Indeed, the commander of the Joint Global Strike Operations Center, Maj. Gen. Mark Weatherington, disclosed in 2020 that the Air Force had yet to settle on a combat role for the various hypersonic weapons it was developing. Among the questions that remained unresolved, he noted, were: "How are we going to employ hypersonic weapons? What do they bring to the battlefield? What are our considerations for planning and executing and integrating them in a fight?"[29] Meanwhile, Michael Griffin, the former undersecretary of defense for research and engineering, has stated that the United States needs to develop such weapons in order "to allow us to match what our adversaries are doing."[30] This sort of thinking, analysts fear, could spur an arms race in hypersonics, long before the consequences of their widespread deployment are fully understood.

Given the potential risks posed by the deployment of hypersonic weapons, many arms control advocates believe that such munitions need to be regulated in some fashion, as have other major weapons systems. There is considerable debate and uncertainty, however, as to how this might be accomplished. Hypersonic warheads fitted on the ICBMs of the U.S. and Russia, such as Avangard, are limited by the New Strategic Arms Reduction Treaty (New START), which expires in February 2026. However, none of the other hypersonic missiles now in development by the major powers are covered by this, or other treaties, and it is unclear how they might be brought under some form of international control. Various strategies to achieve this outcome have been proposed by experts in the field, and these will be given close attention in Chapter 3.

Cyberattack and Nuclear C3

Cyberspace, or the global web of information streams linked to the internet, is a remarkable product of human engineering that permits complex interactions among peoples, companies, organizations, and governments. But while an extraordinary tool for many purposes, the internet is also vulnerable to attack by hostile intruders—whether to spread misinformation, disrupt vital infrastructure, or steal valuable data. Most of those malicious activities are conducted by individuals or groups of individuals seeking to enrich themselves or sway public opinion, but the governments of certain countries, including China, Iran, Israel, North Korea, Russia, and the United States, have also engaged in such endeavors for their own strategic purposes.[31]

Cyberspace has proven to be an attractive arena for great-power competition because it encompasses so many important functions yet is vulnerable to a wide variety of malicious and hostile actions. At one end of the spectrum of possible operations is cyberespionage, intended to penetrate an adversary's military and scientific data systems and steal valuable data about military dispositions, combat plans, and weapons designs. China, for example, has been accused of stealing extensive technological data from U.S. universities and defense contractors in this fashion.[32] Hostile actors may also seek to secretly plant malicious software ("malware") in the operating systems of critical infrastructure, such as energy and financial networks, for activation at some future point—say at the onset of a conflict, or to precipitate

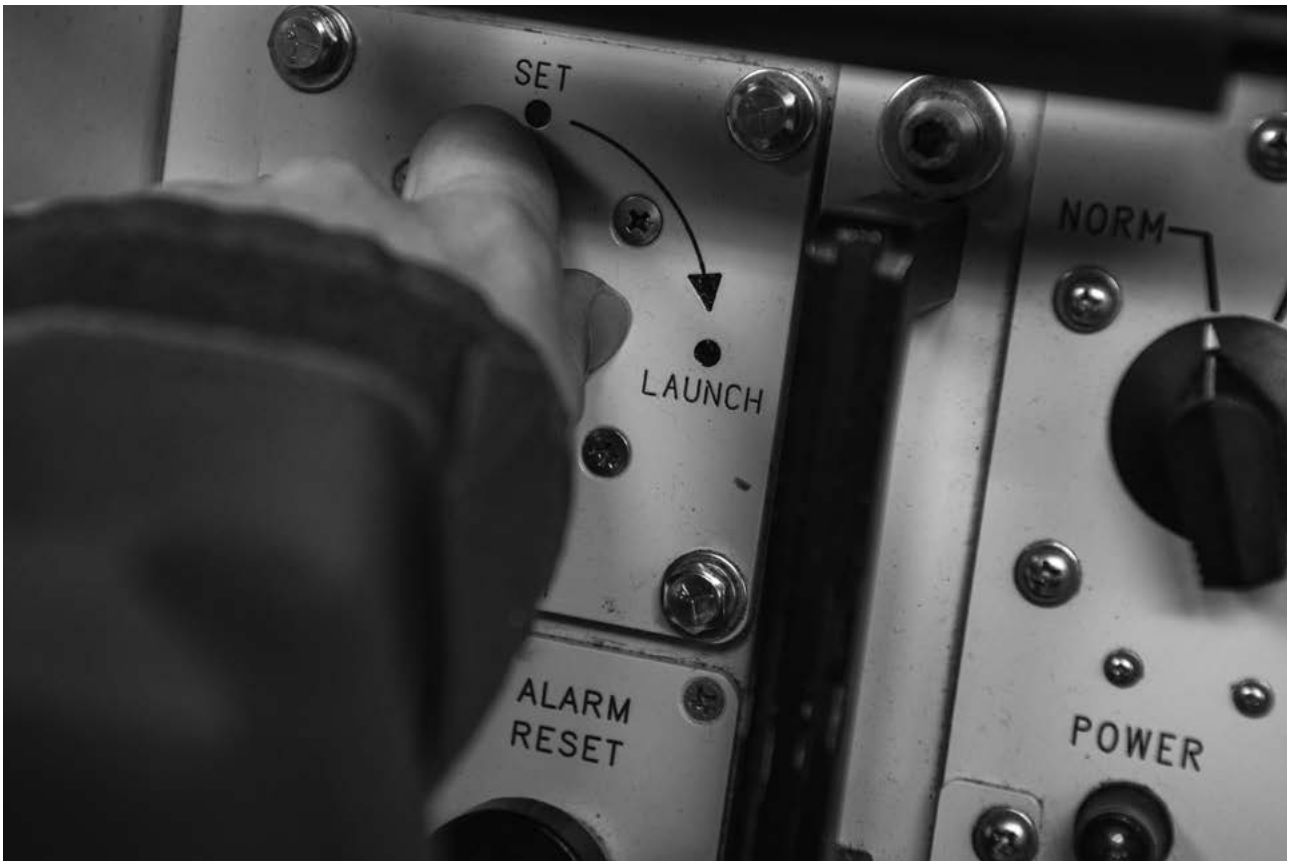
Russian President Vladimir Putin (5L) visits the national defence control centre to oversee the test launch of the Avangard hypersonic missile, Moscow, December 26, 2018. Russian Defence Minister Sergei Shoigu told President Vladimir Putin on December 27, 2019 that the country's first Avangard hypersonic missiles have been put into service, an official statement said. (Photo by Mikhail Klimentyev/SPUTNIK/AFP via Getty Images)

a political crisis of some sort. Russia is said to have mounted attacks of this sort against Ukraine prior to and following its February 2022 invasion.[33]

Cyberoperations are also expected to play a major role in any active conflict between the major powers. Like so many other complex activities, military operations are heavily reliant on digitalized communications and the internet, and these electronic operations are vulnerable to hacking and sabotage. Hence, when a conflict breaks out, the militaries of the major powers are expected to employ their cybertools in efforts to discern enemy moves and intentions, plant false and confusing information, and disable radar, communications, and weapons delivery systems.

To enable military-related cyberoperations of this sort, the "cyberwarriors" of the major powers are believed to devote enormous effort to planting malware in the command, control, and communications (C3) systems of their adversaries. For the most part, such operations are intended to degrade the conventional fighting capabilities of the opposing side—its air, ground, and sea units, and the C3 networks connecting them to radar stations, missile batteries, and the like. The side best able to conduct (and defend against) such activities, it is widely believed, will possess a distinct advantage in future conflicts, as it will be able to fight with a better grasp of battlefield dynamics.

Many analysts worry, however, that such operations might also be aimed at an adversary's strategic nuclear C3 (NC3), so as to impair its functioning in the event of a major-power war. In such a scenario, one side or the other—fearing that a nuclear exchange is imminent—might choose to minimize the danger it can expect (and/or enhance its own nuclear assault) by disabling its adversary's NC3 systems. Attacks of this sort could, in theory, be undertaken without necessarily disclosing their source or, indeed, the fact that they have occurred at all. Given the potential appeal of such measures, it is widely assumed that all of the major powers have pursued such options.[34]



First Lt. Paul Lee, the 321st Missile Squadron missile combat crew commander, performs a simulated key turn of the Minuteman III weapon system during a Simulated Electronic Launch-Minuteman test inside the launch control center at a missile alert facility in the 90th Missile Wing's missile complex, Neb., April 11, 2017. During a SELM, the missileers in the LCC are responsible for sending commands to the Minuteman III ICBMs in the launch facility. (U.S. Air Force photo/Staff Sgt. Christopher Ruano)

While it is easy to grasp the appeal of such endeavors, analysts warn that a cyberattack on an adversary's NC3 systems in the midst of a major crisis or conventional conflict could prove highly destabilizing. Upon detecting interference in its critical command systems, the target state might well conclude that it was facing a pre-emptive nuclear strike by its adversary and so launch its own nuclear weapons, rather than risk their loss to the other side. Even if the attacker was not seeking to provoke a nuclear exchange but was simply probing its adversary's weapons dispositions, the utilization of such tools might be sufficient to provoke a nuclear response by the target state.[35]

Even if not aimed intentionally at nuclear C3, a cyberattack on an adversary's command-and-control systems could prove destabilizing in cases where a state's nuclear and conventional C3 facilities are "co-located" or "entangled," as is often the case. An attacker may seek merely to impair an adversary's conventional C3 systems for tactical battlefield gains, but inadvertently disrupts NC3 systems employing the same digital networks—causing the target state to conclude it faces a nuclear rather than conventional attack, and respond accordingly. This danger, like that arising from a deliberate attack on an adversary's nuclear C3, has led to calls for the adoption of international restrictions on the use of cyberweapons against NC3 systems.[36]

As is true of artificial intelligence and autonomy, the utilization of cyberspace for military purposes poses tough new challenges for arms control. Cyberweapons cannot be detected or tallied by existing means of inspection and verification, and their very existence is often hard to prove. Nor do the major powers have any incentive to discuss what constitutes some of their most secret undertakings. But the proliferation of cyberweapons is creating new and severe threats to strategic stability, so it will be incumbent upon policymakers and arms control advocates to explore methods for devising and adopting controls on their future use.

The Evolving Arms Control Agenda

Even from this brief outline, it should be evident that the weaponization of emerging technologies poses new

and significant threats to strategic stability. In each area covered—artificial intelligence, autonomous weapons systems, hypersonic missiles, and cyberweapons—we see indications that the use of such systems in a major-power conflict could result in uncertainty about an attacker's intentions and so trigger accidental or inadvertent nuclear escalation. At the same time, we observed that existing arms control and regulatory measures do not easily apply to the new technologies, given their distinctive features. Therefore, those existing measures will require modification in some fashion, or new types of controls must be devised to regulate the development, deployment, and use of these new technological capabilities.

On the whole, experts in the field are highly skeptical about the likelihood of the major powers negotiating and signing new arms control agreements of the sort once contrived between the United States and the Soviet Union, and later Russia. However, they suggest that whatever existing measures remain in place be extended wherever possible to incorporate emerging technologies. For example, in negotiating an extension of the New START Treaty beyond February 2026, the U.S. and Russia might agree to incorporate hypersonic weapons (or some types of them) in their slate of weapons to be curtailed. Similarly, the "Strategic Stability Dialogue" held on several past occasions between top U.S. and Russian officials could, in future sessions, devise bilateral restrictions on especially destabilizing cyberweapons.

At the same time, experts agree, it will be necessary to devise new or novel types of control measures. These might include unilateral steps taken by the major powers to reduce their own contribution to global risk. For example, the National Security Commission on Artificial Intelligence, in its Final Report, called on the U.S. government to issue a public statement affirming that "decisions to authorize nuclear weapons employment must only be made by humans, not by an AI-enabled or autonomous system."[37] Unilateral steps of this sort have also been proposed for the cyber field, involving commitments to refrain from attacks on an adversary's NC3 systems.[38]

These are only some of the strategies being considered to control the development, deployment, and battlefield use of emerging technologies. In the chapters below, we will explore these options more closely and examine others that have been proposed for this role. But it should be apparent that despite the unique challenges posed by these technologies, policymakers and arms control advocates are not wanting for ideas on how these challenges might be overcome. In Chapter 6, we summarize these ideas in a "framework strategy" for reducing the escalatory dangers of emerging technologies.

Chapter 2:
Autonomous Weapons Systems and the Laws of War

Envisioning a time when the U.S. combat fleet will be composed by as many "unmanned" warships as traditional, crewed vessels, the Navy in April 2021 conducted its first ever maritime exercise comprised almost entirely of unmanned surface vessels (USVs) and unmanned undersea vehicles (UUVs, or drone submarines). Known as the Unmanned Integrated Battle Problem 2021 (UIBP-21), the exercise was conducted in waters off San Diego and included participation by two prototype medium-displacement USVs, *Sea Hunter* and *Sea Hawk* and the experimental Triton UUV, along with several unmanned aerial vehicles (UAVs).

Equipped with advanced sensors and computing gear, the autonomous air and naval systems were set loose to locate simulated enemy warships and relay this information to manned warships for live missile strikes on the mock targets. "This integrated battle problem provides an operational approach to integrating and adapting unmanned technology with our manned fleet," said the exercise's commander, Rear Adm. James Aiken.[39]

The development of unmanned surface and undersea warships and their integration into the Navy's combat fleets has become a major Pentagon objective as U.S. defense planners seek to counter growing Chinese and Russian naval capabilities in a timely and affordable fashion. Ordinarily, the preferred U.S. response to such a threat would be the construction of additional manned vessels—aircraft carriers, cruisers, destroyers, and so on. But large ships of this sort have become exceedingly expensive and, at the same time, have become increasingly vulnerable to adversary anti-ship missiles. In response to this predicament, Navy strategists have developed the strategy of "Distributed Maritime Operations," under which fewer numbers of large, crewed vessels will be accompanied by scores of less-costly unmanned ships—whose loss, in some future battle, would not cause as much pain and dismay as would the loss of major crewed vessels. As suggested by former Secretary of Defense Mark Esper in October 2020, unmanned vessels "will add significant offensive and defensive capabilities to the fleet at an affordable cost in terms both of sailors and dollars."[40]

Adding to the appeal of this approach, future unmanned vessels will be equipped with advanced sensors and computer systems enabling them to scour large areas of the ocean on their own, collect data on enemy ship positions, and relay this information to manned warships for possible missile strikes—or, in some scenarios, conduct independent attacks using their own onboard missile systems. "Unmanned platforms play a vital role in our future fleet," the Chief of Naval Operations, Adm. Michael Gilday, affirmed in 2021. "They will expand our intelligence, surveillance, and reconnaissance advantage, add depth to our missile magazines, and provide additional means to keep our distributed force provisioned."[41]

At this point, the Navy has yet to deploy a purpose-built unmanned combat vessel or perfected the algorithms needed to enable USVs and UUVs to operate on the high seas autonomously. However, as demonstrated by UIBP-21, they have developed several prototypes of a medium-displacement-unmanned surface vessel, represented by the *Sea Hunter* and *Sea Hawk*, and undertaken elaborate maneuvers to test and refine the necessary software. The aim of UIBP-21, Aiken indicated, "is to evaluate these unmanned systems and how they can actually team with manned systems."[42]

Based on this and other such exercises, the Navy plans to gradually integrate purpose-built USVs and UUVs into its combat fleet in the coming years. As of late 2021, it had awarded contracts for the construction of one deployable (i.e., combat-ready) medium unmanned surface vehicle (MUSV) plus two prototype (or test) MUSVs, four prototype large USVs (LUSVs), and five deployable Extra-Large Unmanned Undersea Vehicles (XLUUVs). The first purpose-built MUSV and XLUUV are expected to join the fleet by 2024 and, if Congress approves, serial production of

Medium displacement unmanned surface vessel *Sea Hunter* sails in formation during Rim of the Pacific (RIMPAC) on July 28, 2022. (U.S. Navy photo)

all three types of unmanned vessels will commence after that. By 2035, the Navy predicts, as much as one-third of its combat fleet will be composed of unmanned vessels of these types.[43]

Initially, these uncrewed ships will engage in what might be termed combat-support missions: tracking and surveillance of enemy vessels, mine and countermine operations, electronic warfare, and so on. As the military gains experience in autonomous operations, however, they will be empowered to conduct offensive attack missions, as well. In its *Unmanned Campaign Framework*, the Navy describes the LUSV as an "adjunct magazine," or floating combat vessel capable of autonomously launching numerous ballistic missiles at enemy ships and land targets.[44]

The Navy is not alone among U.S. armed services in seeking to increase its reliance on autonomous weapons systems in future operations, and the United States is not the only major power championing the development of unmanned systems for military use. The U.S. Air Force and the U.S. Army are also engaged in such endeavors, as are the militaries of China, Russia, and other technologically advanced powers. All of these actors are developing—and in some cases fielding—unmanned combat systems intended to satisfy their distinctive strategic requirements.

The top priority for the U.S. Air Force, for example, is the development of a "loyal wingman"—an unmanned aerial vehicle that can accompany crewed aircraft on missions in contested airspace over enemy territory and conduct vital missions that would place a piloted aircraft at high risk. Such missions might include, for example, intercepting enemy fighter planes or attacking heavily defended anti-aircraft radar stations; they could also be used to strike high-value, heavily-defended targets such as missile batteries and command centers located deep within enemy territory.[45] To advance this concept, the Air Force is testing a prototype "drone wingman," the XQ-58 Valkyrie, and a sophisticated software system called "Skyborg" to control such aircraft when operating on their own.

Skyborg—or, more formally, the Skyborg Autonomous Control System (ACS)—is still in development, but the Air Force has already conducted tests in which it has assumed the role of a human pilot in actual flight operations. On April 29, 2021, the Skyborg ACS took control of an uncrewed military aircraft, the Kratos Unmanned Tactical Aerial Platform (UTAP-22), for the first time. On this occasion, and during a second test held on June 24, 2021, the ACS conducted basic flight maneuvers on its own (albeit while being supervised by human controllers on the

ground). Eventually, Skyborg is intended to control multiple drone aircraft simultaneously and allow them to operate in "swarms," coordinating their actions with one another with minimum oversight by human pilots.[46]

Drawing on this experience, the Air Force plans to award contracts for the design and production of a "loyal wingman" type UAV beginning in fiscal year 2024. As envisioned by Air Force officials, the proposed drone would be designed to accompany F-35 and future manned aircraft on high-risk missions over enemy-controlled territory. "The expectation is that these aircraft can be designed to be less survivable and less capable [than manned aircraft], but still bring an awful lot to the fight in a mixture that the enemy has a very hard time sorting out and dealing with," said Air Force Secretary Frank Kendall in September 2022.[47]

A similar philosophy is guiding the U.S. Army's approach to the development of autonomous ground combat systems. Anticipating a future battlefield in which individual soldiers and human-crewed gun systems will prove increasingly vulnerable to enemy fire, the Army seeks to create a family of Robotic Combat Vehicles (RCVs) that can engage enemy forces "out on the edge," allowing their human overseers to remain protected from the heaviest fighting.[48]

At present, the Army is testing two potential RCV types: the RCV-Light, an unmanned scout vehicle for identifying enemy positions in contested areas; and the RCV-Medium, an unmanned gun platform designed to engage enemy strongpoints and lightly-armored vehicles. It also envisions a third type, the RCV-Heavy, essentially an unmanned tank. Prototypes of the first two types were field tested in 2021, with modified M-113 Bradley armored personnel carriers standing in for the proposed RCV-Heavy in simulated combat operations.[49] The Army is also proceeding with the development of what it calls the Optionally Manned Fighting Vehicle (OMFV), a proposed successor to the M-113 that would be capable of unmanned operations in high-risk combat zones. Initial production of the OMFV is scheduled for 2027.[50]

For the Department of Defense, the development and deployment of autonomous weapons systems like these is viewed as a critical objective if the United States is to retain military superiority over its principal rivals while avoiding excessive risk to its combat personnel and also keeping weapons costs under control. Similar considerations have propelled the autonomous weapons programs of other major powers, especially Russia and China.

Like the United States, Russia is pursuing the concept of a "loyal wingman" for its manned combat planes. It has developed an advanced UAV, the S-70 Okhotnik ("Hunter") strike drone, intended to accompany its most capable fighter, the Sukhoi Su-57, on combat missions over enemy territory. Said to possess stealth characteristics, the Okhotnik has been flown on test flights with the Su-57 and was expected to enter service in 2022. The Russians have also developed an array of surveillance and target-acquisition drones, some of which were employed during the fighting in Syria and Ukraine. And, just as the U.S. Army seeks to reduce the risks to its military personnel by fielding robotic combat vehicles, Russia's ground forces plan to place greater reliance on such systems in the future. Some of its prototype RCVs, including the Uran-6 and Uran-9, also saw service in Syria and Ukraine.[51]

China, too, has been developing such systems. It has deployed a number of large and medium UAVs with branches of the People's Liberation Army (PLA), including the BZK-005 and BZK-007 reconnaissance drones and the GJ-1 and GJ-2 armed UAVs—some of which reportedly have been flown on missions across the median line in the Taiwan Strait between China and Taiwan. In October 2019, at a parade marking the 70th anniversary of the founding of the People's Republic, the PLA displayed mockups of two advanced UAVs, the GZ-11 "Sharp Sword" stealth combat drone and the WZ-8 hypersonic reconnaissance drone. The Chinese also used that occasion to display an unmanned undersea vessel, the HSU-001.[52]

For advocates of such systems, whether in the American, Chinese, or Russian militaries or those of other countries, the development and deployment of autonomous weapons systems offer undeniable advantages in combat. Cheaper to build and maintain than crewed systems and able to operate 24 hours a day without tiring, robotic warriors supposedly would help reduce friendly casualties while enabling high-risk operations in contested areas. As suggested by the U.S. Navy in its 2021 *Unmanned Campaign Framework,* "Autonomous systems provide additional warfighting capability and capacity to augment our traditional combatant force, allowing the option to take on greater operational risk while maintaining a tactical and strategic advantage." When equipped with advanced sensors and AI, autonomous weapons can also be trained to operate in coordinated swarms, or "wolfpacks," overwhelming enemy defenders and affording a speedy victory.

Although the rapid deployment of such systems appears highly desirable to many military officials, their development has generated considerable alarm among diplomats, human rights campaigners, arms control advocates, and others who fear that deploying fully autonomous weapons in battle would severely reduce human oversight of combat operations, possibly resulting in violations of international law, and could weaken barriers that restrain escalation from conventional to nuclear war. For example, it

Major U.S. Autonomous Weapons Systems

Weapon System	Type	Intended Use	Status
MQ-1B Predator / MQ-1C Gray Eagle	UAV	Medium-altitude, long-endurance drone intended for battlefield surveillance and strike missions; MQ-1B is USAF version, MQ-1C is US Army version	Entered service in 1995; widely employed for combat missions in in Afghanistan, Iraq, and elsewhere. $140 million sought in FY 2021 for procurement of 11 MQ-1Cs for US Army
MQ-4C Triton / RQ-4 Global Hawk	UAV	MQ-4C is the USN version of the USAF RQ-4 Global Hawk and is intended for wide-area maritime surveillance	$465 million requested for MQ-4C R&D in FY 2021–23 plus $1.5 billion for procurement of 6 MQ-4s
MQ-8B Fire Scout	UAV	Provides wide-area surveillance and target acquisition for USN Littoral Combat ships and other vessels	In service with the USN
MQ-9 Reaper	UAV	Remotely-piloted long-endurance surveillance and attack drone	Entered service in 2007; widely used for combat missions in Iraq, Afghanistan, and elsewhere. $1.4 billion requested in FY 2021–23 for 23 MQ-9s for the USAF and USMC
MQ-25A Stingray	UAV	USN carrier-based aerial refueling and surveillance drone	USN plans to purchase 72 MQ-25As for $13 billion; first operational MQ-25A expected to join fleet in FY 2025
RQ-170 Sentinel	UAV	Remotely-piloted stealth drone intended for secretive ISR operations	Operated by the 432nd Air Expeditionary Wing, based at Creech AFB, Nev.; reportedly employed over Iran, Pakistan, and Afghanistan
Optionally Manned Fighting Vehicle (OMFV)	UGV	A replacement for the M-113 Bradley Fighting Vehicle intended for crewed or unmanned operation	Five companies awarded a total of $300 million in July 2021 to develop prototypes for testing in FY 2023
Robotic Combat Vehicle Light (RCV-Light)	UGV	Lightly-armed unmanned scout vehicle	$116 million sought for RCV R&D in FY 2023. Up to five companies expected to be chosen for competitive testing of RVC-L candidates in FY 2024 with one selected for prototype development in FY 2026. Development of a more powerful UGV, the RCV-Heavy, is expected to follow.
Robotic Combat Vehicle Medium (RCV-Medium)	UGV	Unmanned combat vehicle designed to engage enemy strongpoints and armored vehicles	
Medium Unmanned Surface Vessel (MUSV)	USV	Envisioned as a low-cost, high-endurance maritime surveillance ship with an estimated displacement of around 500 tons	Two MUSV prototype vessels, *Sea Hunter* and *Sea Hawk,* engaged in simulated combat exercises in 2021. $743.1 million sought for MUSV/LUSV R&D in FY 2021–23
Large Unmanned Surface Vehicle (LUSV)	USV	Envisioned as a reconfigurable combat vessel of approximately 1,000–2,000 tons displacement designed to carry various modular payloads, including anti-ship and land-attack missiles	Two LUSV prototype vessels, *Nomad* and *Ranger*, have been deployed and two additional LUSV prototypes were scheduled for delivery in FY 2022. $743.1 million sought for MUSV/LUSV R&D in FY 2021–23
Orca Extra-Large UUV (XLUUV)	UUV	Intended for use in ASW and antiship operations; to be launched from piers or manned vessels	Boeing awarded contract in 2019 for initial work on 5 XLUUVs. $328 million requested in FY 2022 for Orca program, with first XLUUV scheduled for delivery in late 2022

Major Chinese Autonomous Weapons Systems

Weapon System	Type	Intended Use	Status
BZK-005	UAV	High-altitude, long-endurance reconnaissance drone capable of launching bombs or missiles	First displayed in 2006. In service with all branches of PLA. Reportedly deployed by PLAAF in missions across median line of Taiwan Strait in 2022
BZK-007	UAV	High-altitude, long-endurance reconnaissance drone	In service with PLA Army, PLAN
BZK-008	UAV	Medium-range reconnaissance UAV; considered the Chinese equivalent of the U.S. RQ-4 Global Hawk	In service with PLA Army
CH-4	UAV	Medium altitude, long endurance UAV intended for ISR and strike missions; considered an equivalent of U.S. MQ-9 Reaper	Reportedly deployed by PLAAF in missions across median line of Taiwan Strait in 2022
EA-3 Xianglong	UAV	High-altitude, long endurance UAV intended for ISR missions	First introduced in 2006; in service with PLAAF
GJ-1 Wing Loong	UAV	Medium altitude, long-endurance UAV intended for ISR and strike missions; considered an equivalent of the U.S. MQ-1 Predator	First displayed in 2010; in service with PLAAF
GJ-2 Wing Loong II	UAV	Medium altitude, long-endurance UAV intended for ISR and strike missions; considered an equivalent of the U.S. MQ-9 Reaper	First displayed in 2015; in service with PLAAF
GJ-11 Sharp Sword	UAV	Long-endurance stealth UAV intended for ISR and attack missions; reportedly a clone of the U.S. RQ-170	First displayed at China's National Day parade, Beijing, Oct. 1, 2019.
TB-001	UAV	High-altitude, long-endurance UAV intended for ISR and strike missions	Reportedly deployed by PLAAF in missions across median line of Taiwan Strait in 2022
WZ-7 Soaring Dragon	UAV	High-altitude, long-endurance UAV intended for wide-area surveillance; considered a Chinese equivalent of the U.S. MQ-4.	In service with PLAAF since 2018. Reportedly deployed by PLAAF in missions across median line of Taiwan Strait in 2022
WZ-8	UAV	Hypersonic surveillance drone intended for launching by a "mother ship" aircraft at a high altitude	First displayed at China's National Day parade, Beijing, Oct. 1, 2019.
Sharp Claw II	UGV	Small tracked UGV intended for infantry-support missions; rear storage area can accommodate a mini-UGV, Sharp Claw I	Reportedly deployed by PLA Army in 2021 in Tibet and along Indo-Chinese border
HSU-b 001	UUV	Drone submarine intended for long-range ISR patrols; its flat nose suggests it houses a large sonar for detecting underwater targets	First displayed at China's National Day parade, Beijing, Oct. 1, 2019.

Major Russian Autonomous Weapons Systems

Weapon System	Type	Intended Use	Status
Forpost-R	UAV	Licensed-produced Russian version of Israeli Searcher UAV; intended for reconnaissance and strike missions	Reportedly used to attack Ukrainian weapons systems in 2022
Kronstadt Orion	UAV	Family of medium-range, long-endurance UAVs intended for surveillance and strike missions	First flown in 2016. Reportedly used in for attacks on Ukrainian ground vehicles in 2022
Sukhoi S-70 Okhotnik-B	UAV	Armed stealth UAV intended as a "wingman drone" to accompany the Su-75 fighter jet in contested airspace	First flown in 2019; reportedly test-fired guided missiles in 2022
Orlan-10	UAV	Medium-range UAV used for reconnaissance and target acquisition	Reportedly used in Ukraine in 2022 to select targets for artillery strikes
Orlan-30	UAV	Improved version of Orlan-10 with greater range	Reportedly used in Ukraine in 2022 to select targets for artillery strikes
Tu-243 Reis-D	UAV	Medium-range UAV used for reconnaissance and target acquisition	In production since 1994. Reportedly used in Ukraine in 2022 to select targets for artillery strikes
Uran-6	UGV	Robotic combat vehicle intended for infantry-support operations, especially mine clearance.	Reportedly saw wide use in Syria and used in Ukraine for mine clearance
Uran-9	UGV	Robotic combat vehicle intended for offensive operations alongside tanks and infantry fighting vehicles	Entered service in 2019. Reportedly used in Syria.

Abbreviations:

ASW = anti-submarine warfare

FY = fiscal year

ISR = intelligence, surveillance, and reconnaissance

PLA = People's Liberation Army

PLAAF = People's Liberation Army Air Force

PLAN = People's Liberation Army Navy

R&D = research & development

UAV = unmanned aerial vehicle

UGV = unmanned ground vehicle

USAF = U.S. Air Force

USN = U.S. Navy

USV = unmanned surface vessel

UUV = unmanned subsea vessel

Autonomy is a matter of degree, with machines being granted ever-increasing capacity to assess their surroundings and decide what to strike and when.

seems reasonable to ask whether the Army's proposed RCV, if deployed in a crowded urban area, would be able to distinguish between enemy combatants and civilian residents, as required by international law? Likewise, could a wolfpack of sub hunters, hot on the trail of an enemy submarine carrying nuclear-armed ballistic missiles, provoke the captain of that vessel to launch its weapons to avoid losing them to a presumptive U.S. pre-emptive strike?

These and other such questions have sparked a far-ranging inquiry into the legality, morality, and wisdom of deploying fully autonomous weapons systems. In October 2022, for example, a group of 70 nations, including the United States, delivered a joint statement to the UN General Assembly raising such concerns and calling for unilateral and multilateral steps to address them. "The introduction of new technological applications, such as those related to autonomy in weapon systems…raise serious concerns from humanitarian, legal, security, technological and ethical perspectives," the statement reads. "We therefore see an urgent need for the international community to…address these risks and challenges by adopting appropriate rules and measures."[53]

Ever-Increasing Degrees of Autonomy

Autonomous weapons are lethal devices that have been empowered by their human creators to survey their surroundings, identify potential enemy targets, and, under certain conditions, independently choose to attack those targets on the basis of sophisticated algorithms incorporated into their operating systems. Such devices require the integration of several core elements: a mobile combat platform, such as a drone ship, aircraft, or ground vehicle; sensors of various types to scrutinize the platform's surroundings; processing systems to classify objects discovered by the sensors; and algorithms directing the platform to initiate attack when an allowable target is detected within a certain prescribed area. The U.S. Department of Defense describes an autonomous weapons system as a "weapons system that, once activated, can select and engage targets without further intervention by a human operator."[54]

Few weapons in active service presently exhibit all of these characteristics. Some militaries employ close-in naval defense weapons such as the U.S. Phalanx gun system, which can fire autonomously when a ship is under attack by enemy planes or missiles. However, the Phalanx cannot independently search for and strike enemy assets on its own, and human operators are always present to assume control if needed. Many aerial drones are able to attack human-selected ground targets, such as tanks or armed combatants, but cannot hover over an area to identify and attack potential threats on their own. Increasingly, however, UAVs are being endowed with such capabilities, as shown by Israel's Harpy airborne anti-radiation drone, which can loiter for several hours over a pre-determined area to search for and destroy enemy radars.[55]

Autonomy, then, is a matter of degree, with machines being granted ever-increasing capacity to assess their surroundings and decide what to strike and when. As described by the Congressional Research Service, autonomy is "the level of independence that humans grant a system to execute a given task.… [It] refers to a *spectrum of automation* in which independent decisionmaking can be tailored for a specific mission, level of risk, and degree of human-machine teaming."[56] Put differently, autonomy refers to the degree to which humans are taken "out of the loop" of decision-making, and AI-enabled systems are invested with responsibility for critical battlefield decisions.[57]

This emphasis on the "spectrum of automation" is important because, for the most part, nations have yet to deploy fully autonomous weapon systems on the battlefield. Under prevailing U.S. policy, as enshrined in a November 2012 Defense Department directive, "autonomous and semi-autonomous weapons systems shall be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force."[58] In their official statements, U.S. military leaders regularly assert that this dictum continues to govern Pentagon policy on autonomous weapons. Yet this country, like others, is developing and testing weapons that would allow for ever-diminishing degrees of human control over their future use.

This is evident, for example, in the U.S. Navy's approach to autonomous weapons systems. The first generation of USVs, it has been noted, will contain modest accommodations for a small detachment of personnel to oversee operations that AI systems are not yet deemed capable of performing, such as refueling at sea. But the Defense Advanced Research Projects Agency (DARPA) is developing a future unmanned warship called NOMARS, for "no mariners," that will have no crew space at all and will be designed to operate entirely autonomously.[59]

The U.S. Army is testing the Squad Multipurpose Equipment Transport vehicle, designed to unburden infantry personnel from carrying supplies. Future versions may feature more autonomy and front-line capabilities. (Image: U.S. Army)

The Air Force and Army, as we have seen, are proceeding along similar lines, initially fielding unmanned planes and guns that will operate under the oversight of human commanders while at the same time developing AI systems like Skyborg that will enable those systems to operate with ever-increasing degrees of autonomy. A similar evolutionary process is evident in the development and deployment of unmanned weapons by Russia, China, and other nations.

An Arms Race in Autonomy?

In developing and deploying these weapons systems, the United States and other countries appear to be motivated largely by the aspirations of their own military forces, which see various compelling reasons for acquiring robotic weapons. For the U.S. Navy, it is evident that cost and vulnerability calculations are leading the drive to acquire unmanned surface and subsea vessels. Naval analysts believe that it might be possible to acquire dozens of USVs for the price of just one manned destroyer, while simultaneously reducing the threat to human crews. The ground forces of both the U.S. and Russia are proceeding along similar lines, seeking to substitute unmanned combat systems for human-crewed ones in future high-intensity battles.

These institutional considerations, however, are not the only drivers for developing autonomous weapons systems. Senior officers in China, Russia, and the U.S. are fully aware of the technological ambitions of their competitors and are determined to prevail in what might be called an "autonomy race," wherein all of the major powers are rushing the development and deployment of ever-more sophisticated autonomous weapons lest their adversaries deploy such devices first, and so gain a presumptive battlefield advantage. Pentagon officials regularly speak of China's and Russia's gains in robotic weapons when asking Congress for increased funding for their own such projects, often intimating (without providing any evidence) that the U.S. lags behind those countries in the autonomy field.[60] By the same token, what is known of Chinese and Russian autonomous weaponry suggests a drive to duplicate the strides achieved by the United States in this area: many Chinese UAVs, for example, appear to be variants or imitations of U.S. models.[61]

Arms racing behavior is a perennial concern for the great powers, because efforts by competing states to gain a technological advantage over their rivals (or to avoid falling behind them) often lead to excessive and destabilizing arms buildups. A race in autonomy

poses a particular danger because the consequences of investing machines with increased intelligence and decision-making capacity are largely unknown and could prove catastrophic. In their haste to match the presumed progress of likely adversaries, states might field robotic weapons with considerable autonomy well before their abilities and limitations have been fully determined, resulting in unintended fatalities or uncontrolled escalation.[62]

Supposedly, these risks will be minimized by maintaining some degree of human control over all such machines, but the race to field increasingly capable robotic weapons could result in ever-diminishing human oversight. Analysts at the CRS foresaw this in a 2018 assessment of the Army's plans for robotic combat vehicles. "Despite [the Defense Department's] insistence that a 'man in the loop' capability will always be part of [RCV] systems," they wrote, "it is possible if not likely, that the U.S. military could feel compelled to develop…fully autonomous weapon systems in response to comparable enemy ground systems or other advanced threat systems that make any sort of 'man in the loop' role impractical.[63]

Assessing the Risks

Given the likelihood that China, Russia, the U.S., and other nations will deploy increasingly autonomous robotic weapons in the years ahead, policymakers must identify and weigh the potential risks of such deployments. These include not only the potential for accident and malfunctioning, as would be the case with any new weapons that are unleashed on the battlefield, but also a wide array of moral, ethical, and legal concerns arising from the diminishing role of humans in making life-and-death decisions.

The potential dangers associated with the deployment of AI-empowered robotic weapons begin with the fact that much of the technology involved is new and untested under the conditions of actual combat, where unpredictable outcomes are the norm. For example, it is one thing to test AI-equipped self-driving cars under controlled roadway conditions with constant human oversight; it is another to let such vehicles loose on busy highways. Recent accidents involving Tesla's "Autopilot" self-driving feature suggest that even after years of testing and refinement, such devices can fail when encountering unfamiliar objects or conditions.[64] Consider, then, if that inherently flawed self-driving vehicle is covered with armor, equipped with a gun, and released on a modern battlefield as a robotic combat vehicle. Most experts agree that algorithms can never anticipate all the hazards and mutations of combat, no matter how well "trained" the algorithms governing a given weapon's actions may be. In war, accidents and mishaps—some potentially catastrophic—are almost inevitable.[65]

Although data on the reliability of fully autonomous weapons under wartime conditions is relatively scarce (given that few such systems have yet been deployed), extensive laboratory testing of AI image-classification algorithms has shown that such systems can easily be fooled by slight deviations from standardized representations. In one experiment, for example, a turtle was repeatedly identified as a rifle. Algorithms of this sort are also vulnerable to trickery, or "spoofing," as well as hacking by adversaries.[66]

These dangers are becoming ever more severe as autonomous weapons systems are accorded ever-greater authority to make decisions on the use of lethal force in battle. Although U.S. authorities insist that human operators will always be involved when life-and-death decisions are made by armed robots, the trajectory of technology is leading to an ever-diminishing human role in that capacity, heading eventually to a time when humans are uninvolved entirely. This could occur as a deliberate decision, such as when a drone is set free to attack targets fitting a specified appearance ("adult male armed with gun"), or as a situational matter, as when drones are empowered to fire at their discretion if they lose contact with human controllers. It might be argued that a human operator is somehow involved, simply by launching the drones on such missions, but no human is ordering the specific lethal attack.

This erosion in the degree of human control is especially concerning when we consider the escalatory potential of advanced autonomous weapons. As noted above, the U.S. Navy and Air Force are testing unmanned ships and planes that will be equipped with advanced sensors and missile systems, allowing them to strike high-value targets, including command-and-control facilities located deep within enemy territory. Should USVs and UAVs of this type lose contact with their human controllers and their AI systems determine that circumstances require the launch of their weapons, they could provoke a major enemy retort resulting in an unintended escalatory spiral.

Packs of such weapons, operating in self-coordinated "swarms," might also be used to track down enemy ballistic-missile submarines and mobile ICBMs, eliminating the presumed invulnerability of such weapons and making a nuclear first strike appear more viable to states possessing such capabilities. Simply by suggesting the potential for such an assault, the development or fielding of such capabilities could prompt the nuclear powers to place their atomic weapons on a high level of alert, thereby making an accidental or inadvertent nuclear war far more likely.[67]

Maintaining Ethical and Legal Norms

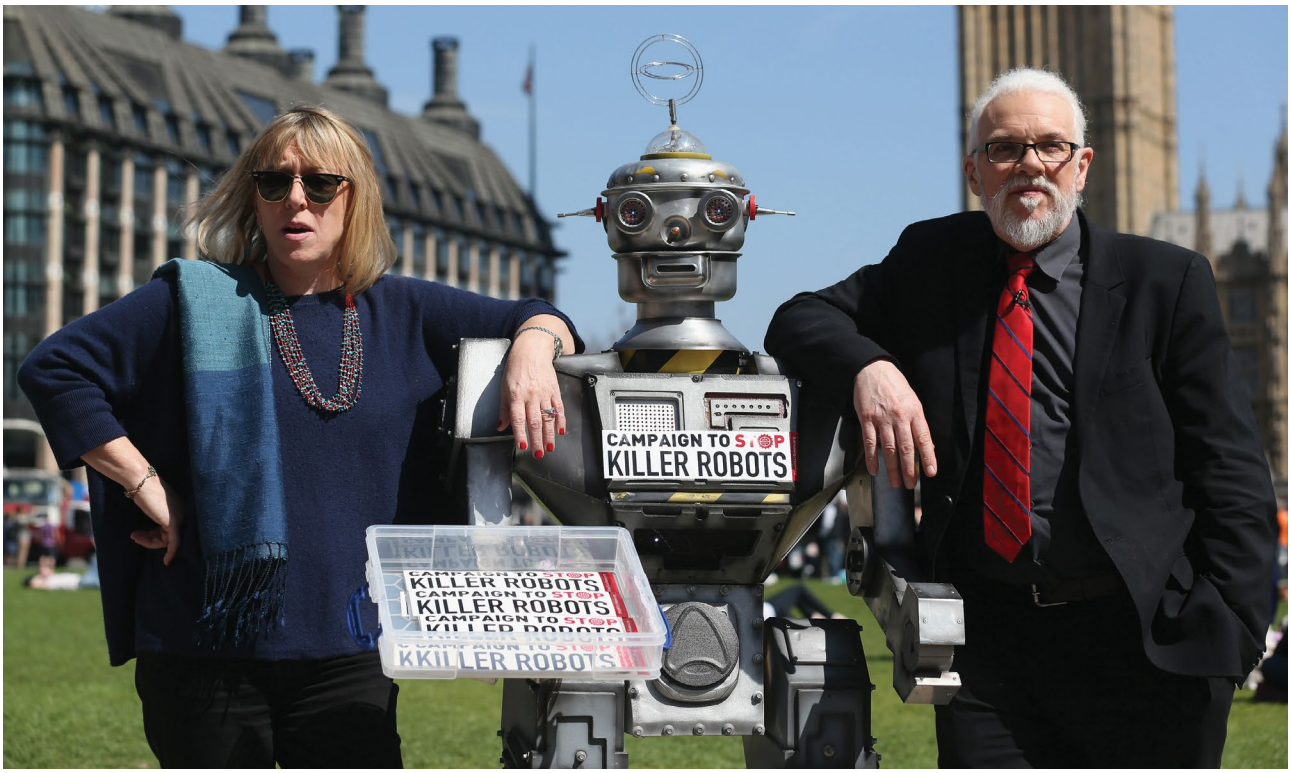
The trend towards diminishing human control over autonomous weapons poses obvious challenges

because virtually all human ethical and religious systems view the taking of a human life, whether in warfare or not, as a supremely moral act requiring some valid justification. Humans, however imperfect, are expected to abide by this principle, and most societies punish those who fail to do so. Faced with the horrors of ever-more destructive warfare, human societies have, over time, sought to limit the conduct of belligerents in wartime and to prevent cruel and excessive violence.

Beginning with the Hague Convention of 1899 and in subsequent agreements forged in Geneva after World War I, international jurists have devised a range of rules—understood, collectively, as the laws of war—proscribing certain behaviors in armed conflict, such as the use of poisonous gas. Following World War II and revelations of the Holocaust, diplomats adopted additional protocols to the Hague and Geneva conventions intended to better define the obligations of belligerents in protecting civilians from the ravages of war—measures generally known as international humanitarian law. So long as humans remain in control of weapons, they can, in theory, be held accountable under those laws for any violations committed when using those devices. But what happens when a machine makes the decision to take a life, and questions arise over the legitimacy of that action? Who is accountable for any crimes deemed to have occurred, and how can a chain of responsibility be determined?

These questions arise with particular significance regarding two key aspects of international law: the requirement for *distinction* and *proportionality* in the use of force against enemy troops interspersed with civilian populations. Distinction requires warring parties to discriminate between armed combatants and civilians during the course of combat and to spare the latter from harm to the greatest extent possible. Proportionality requires attacking forces to apply no more force than is needed to achieve the intended military objective, while sparing civilian personnel and property from unnecessary collateral damage.[68]

These principles pose a particular challenge to fully autonomous weapons because they require a capacity to make fine distinctions in the heat of battle. It may be relatively easy, in a large tank-on-tank battle, for such systems to distinguish military from civilian vehicles; in many recent conflicts, however, enemy combatants have installed guns and rocket launchers on ordinary pickup trucks and covered them with tarpaulins, making them almost indistinguishable from civilian vehicles. Perhaps



Jody Williams (left), a Nobel Peace Laureate, and Noel Sharkey, the chair of the International Committee for Robot Arms Control, called for a ban on fully autonomous weapons in Parliament Square in London on April 23, 2013. The 'Campaign to Stop Killer Robots' is calling for a pre-emptive ban on lethal robot weapons that could attack targets without human intervention. (Photo by Oli Scarff/Getty Images)

a hardened veteran could spot the difference, but an intelligent robot? Unlikely. Similarly, how does one gauge proportionality when attempting to attack enemy snipers ensconced in civilian-occupied tenement buildings? For robots, this could prove an insurmountable challenge.

Advocates and critics of autonomous weaponry disagree over whether such systems can be equipped with algorithms sufficiently adept to distinguish between legitimate and illegitimate targets in order to satisfy the laws of war. While champions of robotic weaponry insist that such precision is within technological reach, many human rights advocates argue otherwise. "Humans possess the unique capacity to identify with other human beings and are thus equipped to understand the nuances of unforeseen behavior in ways that machines, which must be programmed in advance, simply cannot," analysts from Human Rights Watch and the International Human Rights Clinic of Harvard Law School wrote in 2016.[69]

Critics of fully automated weapons systems also argue that it is fundamentally immoral to endow machines with the capacity to make decisions of life and death on their own. This outlook holds that international law and common standards of ethical practice ordain that only humans possess the moral capacity to justify taking another human's life, and that machines must never be endowed with that power. Proponents of this approach point to the Martens clause of the Hague Convention of 1899 (also inscribed in Additional Protocol I of the Geneva Conventions), stating that even when not covered by other laws and treaties, human populations "remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity, and from the dictates of human conscience." Opponents of fully autonomous weapons systems claim that such devices, by removing humans from life-and-death decisions, are inherently contradicting "principles of humanity" and "dictates of human conscience," and so should be banned.[70]

Strategies for Control

Since it first became evident that strides in AI would permit the deployment of increasingly autonomous weapons systems and that the major powers are seeking to exploit those breakthroughs for military advantage, analysts in the arms control and human rights communities, joined by sympathetic diplomats and others, have sought to devise strategies for regulating the development and battlefield use of such systems, or for banning them entirely.

A major part of that effort has involved efforts by parties to the Convention on Certain Conventional Weapons (CCW) to consider the adoption of a legally binding prohibition of the deployment and use of fully autonomous weapons. The CCW, a 1980 treaty restricting or prohibiting the use of particular types of weapons that are deemed to cause unnecessary suffering in war or to harm civilians indiscriminately, allows for the adoption of additional protocols addressing specific weapons not envisioned in the original treaty—as occurred in 1995, with the adoption of a ban on blinding laser weapons, and in 1996, with a measure restricting the use of mines, booby traps, and other such devices.[71] Citing these examples, several dozen states, along with civil society groups such as the Campaign to Stop Killer Robots, have called for negotiating an additional protocol banning autonomous combat systems.[72]

Proponents of such a measure say that it is the only way to avoid inevitable violations of international humanitarian law. Opponents of a ban argue that autonomous weapons systems can be made intelligent enough to overcome concerns regarding international humanitarian law, so no barriers should be placed on their continued development. In line with CCW practice, state parties to the CCW have convened a group of governmental experts to consider these and other perspectives on autonomous weapons and their regulation. These meetings have generated a wide spectrum of possible control measures, ranging from a total ban to assorted voluntary restrictions. However,

Ambassador Amandeep Singh Gill (center), chair of the Governmental Group of Experts on Lethal Autonomous Weapons Systems, speaks at a press conference in Geneva August 27, 2018. The group was established by state parties to the Convention on Certain Conventional Weapons to evaluate the risks of autonomous weapons systems and to develop regulatory strategies. (Photo: Violaine Martin/ United Nations)

as deliberations under the CCW are governed by consensus, a handful of states with advanced robotic projects—notably Russia and the United States—have blocked consideration of a legally-binding protocol.

Given that signatory states of the CCW are unlikely to reach consensus on the adoption of a protocol banning fully autonomous weapons, some states—urged on by the Campaign to Stop Killer Robots and other civil-society groups—are exploring alternative routes to such a prohibition. One such path being considered is a drive to persuade members of the UN General Assembly (where measures are adopted by majority vote, not consensus) to adopt a ban of this sort akin to the 2017 Treaty on the Prohibition of Nuclear Weapons (TPNW).[73]

Another approach, advanced by representatives of France and Germany at the CCW expert group's meetings, would be the adoption by key states of a political declaration affirming the principle of human control over weapons of war, accompanied by a nonbinding code of conduct. Such a measure, possibly in the form of a UN General Assembly resolution, would require human responsibility over fully autonomous weapons at all times to ensure compliance with the laws of war and international humanitarian law. The code would establish accountability for states committing any misdeeds with autonomous weapons systems in battle and require that these weapons retain human oversight to disable the device if it malfunctions.[74]

Yet another approach, favored by the United States and several other countries, would be the adoption by states of unilateral measures limiting the use of autonomous weapons by their own military forces, and, in the process, setting an example for other countries to follow. The National Security Commission on Artificial Intelligence, in its Final Report, specified a range of such measures, including a requirement for rigorous testing of prototype robotic weapons under simulated combat conditions to detect any flaws in their software before being deployed on the battlefield.[75]

The U.S. military, and those of other nations, are also being pressured by elements of civil society, including figures in the tech industry, to adopt ethical principles for the use of AI and autonomy in combat systems. Reflecting its awareness of these concerns, in February 2020 the Department of Defense adopted a set of "ethical principles for artificial intelligence" to govern its use by the military services. These include a requirement that AI-empowered systems "be subject to testing and assurance . . . across their entire life-cycles" and that they possess "the ability to detect and avoid unintended consequences."[76]

The construction and adoption of these and other such control measures will become ever more essential as the major powers accelerate the acquisition of unmanned combat systems and these devices are accorded ever greater autonomy. Without such controls, human commanders will experience ever-diminishing control over the conduct of battlefield operations, potentially resulting in unintended human slaughter and accidental or inadvertent nuclear escalation.

Chapter 3:

An 'Arms Race in Speed': Hypersonic Weapons and the Changing Calculus of Battle

Speed. Since nations first went to war, speed has been a key factor in combat, particularly at the very onset of battle. The rapid concentration and employment of force can help a belligerent overpower an opponent and avoid a costly war of attrition—an approach that underlaid Germany's blitzkrieg (lightning war) strategy during World War II and America's "shock and awe" campaign against Iraq in 2003.

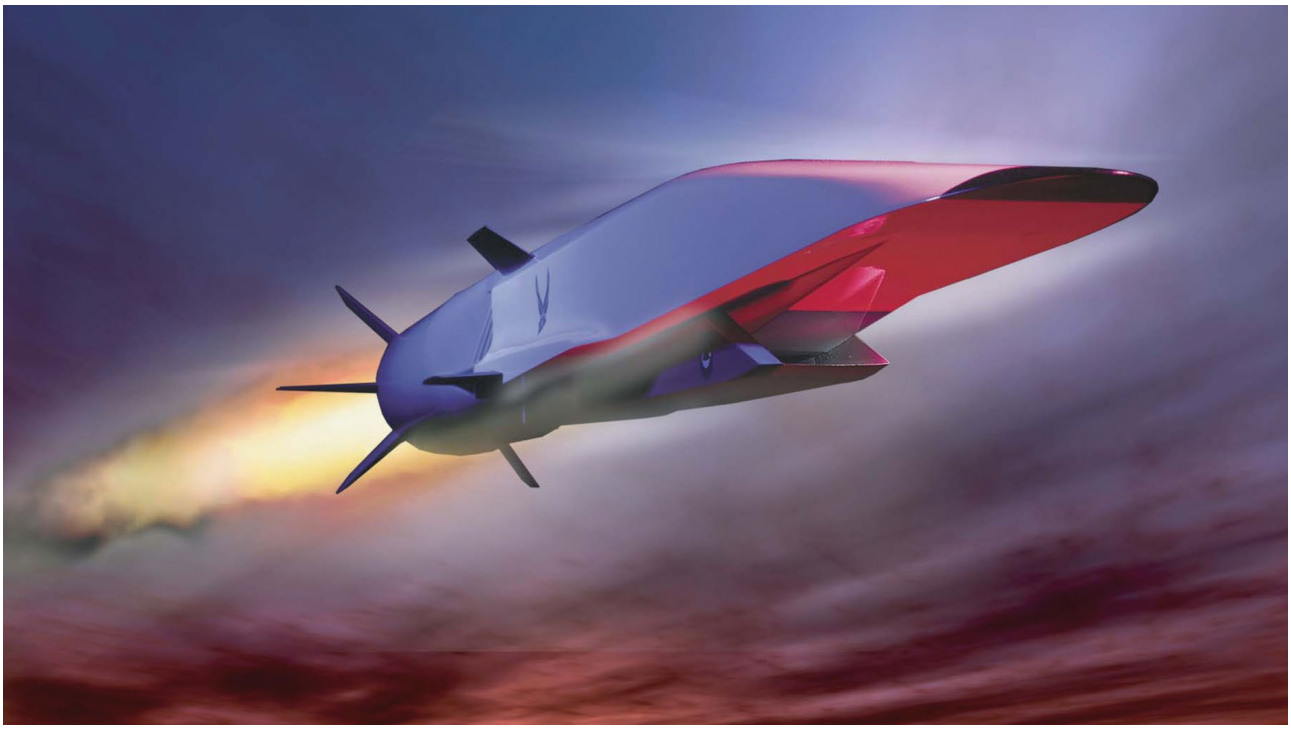
Speed is also a significant factor in the nuclear attack and deterrence equation. Following the advent in the 1950s of intercontinental ballistic missiles (ICBMs), which reduced to mere minutes the time between a launch decision and catastrophic destruction on the other side of the planet, nuclear-armed states have labored to deploy early-warning and command-and-control systems capable of detecting a missile launch and initiating a retaliatory strike before their own missiles could be destroyed. Preventing the accidental or inadvertent onset of nuclear war thus requires enough time for decision-makers to ascertain the accuracy of reported missile launches and choose appropriate responses. This is an imperative reinforced by several Cold War incidents in which launch detection systems provided false indications of such action, but human operators intervened to prevent unintended retaliation.

Today, speed will alter the calculus of combat and deterrence even further with the widespread deployment of hypersonic weapons—maneuverable projectiles that fly at more than five times the speed of sound (Mach 5 and higher). China, Russia, and the United States are now testing and deploying several types of hypersonic weapons to enhance their strategic nuclear deterrence capabilities and acquire additional conventional strike options. (ICBM reentry vehicles also travel at those superfast speeds, but the hypersonic glide vehicles now in development are far more maneuverable, making their tracking and interception exceedingly difficult.)

Both Russia and China have developed hypersonic warheads for some of their ICBMs with the evident intention of overcoming the defense systems being installed by the United States to intercept and destroy incoming enemy missiles. Hypersonic warheads, capable of carrying either nuclear or conventional payloads (and so termed "dual-use"), are also being fitted on missiles intended for use in a regional context, say, in a battle erupting in Europe or the area around Taiwan. With the time between launch and arrival on target dwindling to ten minutes or less, the introduction of these weapons will introduce new and potent threats to global stability.[77]

Hypersonic weapons are said by proponents to be especially useful at the onset of battle, when they can be used to attack an opponent's high-value, heavily defended assets, such as air-defense radars, fighter bases, and command-and-control (C2) facilities. The incapacitation of those facilities at an early stage in the conflict could help smooth the way for follow-on attacks by regular air, sea, and ground forces. Yet, as the same facilities are often tied into a nuclear-armed country's strategic warning and C2 systems, attacks against them could be interpreted by the target state as the prelude to a nuclear first strike, and so trigger the early use of its own atomic weapons.

The rapid development of hypersonic weapons and the escalatory dangers they present obviously raise a number of significant issues for arms control. Under the Intermediate-Range Nuclear Forces (INF) Treaty of 1987, the U.S. and the Soviet Union (and later Russia) agreed to eliminate all nuclear and conventional ground-based ballistic and cruise missiles with a range of between 500 and 5,500 kilometers—a span that encompasses most of the hypersonic weapons now in development. However, that accord was nullified in 2019 when the United States withdrew from the treaty and Russia soon followed suit. Thus, except for any hypersonic warheads affixed upon ICBMs covered under the New Strategic Arms Reduction Treaty (New



The X-51A, shown as an artist's concept, is an experimental, scramjet-powered hypersonic aircraft that achieved speeds of over Mach 5 in a 2013 test. (Graphic: U.S. Air Force)

START) between the U.S. and Russia, which will remain in effect until 2026, weapons of this type are not subject to any arms control agreements.

Both U.S. and Russian officials have spoken of their interest in discussing possible limitations on new military technologies with strategic effects, possibly including hypersonic weapons, in any future talks on a successor to New START, but no specific proposals along these lines have yet been advanced. The Biden administration has also expressed its desire to discuss such limits with Chinese officials, but Beijing has yet to agree to such talks. Accordingly, at present there are no formal restraints on the deployment or use of hypersonic weapons, despite the escalatory risks they pose.[78]

The rush to develop and deploy hypersonic weapons without fully considering their potential impacts or devising meaningful controls on their use is yet another aspect of the speed associated with these munitions. Given the escalatory dangers of deploying hypersonic weapons, it is essential that they receive closer attention from policymakers, arms control analysts, and the general public.

Hypersonic Developments

During the Cold War, the United States and the Soviet Union conducted extensive research on the technologies associated with hypersonic weapons, including the notion of mounting maneuverable reentry vehicles on ICBMs. Yet it was only at the onset of the 21st century that the major powers began exploring the application of these technologies to a wide variety of missile types. As this process has advanced, these states have largely focused on two types of weapons: hypersonic boost-glide vehicles (HGVs) and hypersonic cruise missiles (HCMs).[79]

Hypersonic glide vehicles employ a booster rocket to carry the glide vehicle (and its encased warhead) into the outer atmosphere. Once reaching that height, between 40 and 100 miles above the earth's surface, the glide vehicle separates from the booster and, propelled solely by its kinetic momentum and kept aloft by its aerodynamic shape, skims along the atmosphere's outer boundary for considerable distances. Although unpowered, the vehicle can maneuver in flight, using satellite guidance to strike its intended target with high precision.

The U.S. Department of Defense, as part of its prompt global-strike program, initially considered launching conventionally-armed hypersonic glide vehicles from repurposed Minuteman ICBMs and placing similar warheads on a small number of intercontinental Trident submarine-launched ballistic missiles (SLBMs). Later, under pressure from Congress, the Pentagon largely abandoned that approach, largely out of concern that such systems could be confused for the nuclear-armed versions of those missiles and unintentionally trigger a nuclear

response. More recently, the Pentagon has pursued medium-range systems employing assorted rockets to boost the glide vehicle into space. Russia and China, however, are continuing to test and deploy ICBM-launched hypersonic glide vehicles, such as the Russian Avangard and Chinese DF-17.

Hypersonic glide vehicles are believed by their proponents to offer several advantages over existing ballistic missiles, whether ICBMs or shorter-range types. By definition, ballistic missiles fly on a parabolic course, rising far into space before reaching their peak altitude and then descending toward Earth on a primarily predetermined trajectory. Once such projectiles are detected by a country's early-warning radars, during the extra-atmospheric portion of their flight, it is possible to determine their intended target and, where missile defense technology (with its limited current success rate) permits, to intercept and destroy them with ballistic missile interceptors.

HGVs, by contrast, coast along the atmosphere's outer edge, below the range of early warning radars scanning for a ballistic trajectory, and so are harder to detect while in flight. HGVs are also assumed to be highly maneuverable, and so can more easily elude enemy missile interceptors. Some analysts have argued, however, that HGVs will surrender some of their velocity during their atmospheric flight due to drag from the surrounding air and so will be more susceptible to point defenses when nearing their intended target.[80]

Hypersonic cruise missiles, unlike glide vehicles, fly within the atmosphere and can be launched by ships or planes, or from land-based systems. To attain Mach 5 and above, they employ advanced, air-breathing jet engines called scramjets, for supersonic combustion ramjets. Because the missiles must carry their fuel, they possess less range than glide vehicles and so must be launched from sites closer to their target. The U.S. Air Force is pursuing an air-launched HCM, the Hypersonic Attack Cruise Missile (HACM), and the Defense Advanced Research Projects Agency is also conducting research on such systems. In January 2023, Russia deployed the Tsirkon HCM, which can be launched from ships and submarines.

China, Russia, and the United States are all working on variants of these weapons types and the necessary supporting technologies. In the U.S., each of the military services has pursued its own hypersonics development effort or collaborated in joint projects with one of the other services. The Air Force, along with its hypersonic cruise missile program, is developing a hypersonic projectile called the Air-Launched Rapid Response Weapon (ARRW), scheduled to be the first U.S. hypersonic missile to enter active service, in fiscal year 2023. The Army is proceeding with development of several hypersonic weapons simultaneously: the Precision Strike Missile (PrSM), with an intended range of 300 to 500 miles, the Long-Range Hypersonic Weapon (LRHW), with a range of 1,725 miles or more, and the Mid-Range Capability (MRC), falling somewhere in between. Not to be outdone, the Navy, under its Conventional Prompt Strike (CPS) program, is developing a booster rocket that could be fired from submarines or surface ships and launch the hypersonic glide vehicle it is developing jointly with the Army, which plans to install it on its LRHW system. The Defense Department asked for $3.8 billion for development work on these and related projects in its fiscal year 2022 budget request and $4.7 billion in fiscal year 2023, with far larger amounts expected in future budgets as serial production of these weapons begins.[81]

In addition to their work on HGVs intended for long-range strike missions, such as the Avangard and DF-17, Russia and China have also been developing hypersonic weapons for battlefield use, similar to the U.S. ARRW and PrSM. These include, for example, Russia's Tsirkon (or Zircon), a sea-launched HCM with an estimated range of 300-700 miles, and its Kinzhal ("Dagger"), an air-launched HGV with a range of 1,200 miles. China is believed to be developing similar types, but little information on these is available.[82]

For the most part, work on hypersonic weapons is focused on their use as *offensive* systems—whether for theater battlefield use or to attack an enemy's cities and industrial zones as part of a retaliatory nuclear strike. However, the U.S. Department of Defense has also awarded $61 million for preliminary design work on a *defensive* hypersonic missile, the Glide Phase Interceptor (GPI), intended for use in attacking an enemy's hypersonic glide vehicles while in the midcourse, unpowered stage of their flight. In conjunction with the GPI (which is expected to be mounted on surface ships), the Pentagon plans to deploy a new family of satellites in low-Earth orbit to detect and track enemy glide vehicles.[83]

Strategic Rationales

All three major powers have explored similar applications of hypersonic technologies, but their strategic calculations in doing so appear to vary, with the United States primarily seeking weapons for use in a regional, non-nuclear conflict, and both China and Russia emphasizing the use of hypersonic weapons for nuclear, as well as conventional applications. Whatever the case, leaders of all three countries believe that hypersonic weapons provide significant—even "game-changing"—advantages in speed and maneuverability as well as perceived invulnerability to existing defensive systems.

The United States first considered development of hypersonic weapons so as to be able to attack an

The X-60A is a test vehicle intended to develop U.S. hypersonic missile technology. (Graphic: Generation Orbit)

enemy's high-value targets, including C2 systems and mobile missile batteries, without using nuclear warheads or relying on forward-based forces. This was the premise of the original conventional prompt global-strike mission (not to be confused with the Navy's CPS program), first announced by the Bush administration in 2003. Over time, however, the Pentagon's pursuit of hypersonic weaponry has focused more on conventionally-armed, intermediate-range weapons that might be used in a regional context to degrade an enemy's defenses at the onset of battle, thereby easing the way for follow-on air, sea, and ground forces. Despite this shift, speed of attack has remained a consistent aim of the Pentagon's hypersonic endeavors. As noted by the Congressional Research Service in a January 2019 review of these efforts, "Analysts have identified a number of potential targets that the United States might need to strike promptly," such as an enemy's C2 facilities as well as "air defense or anti-satellite weapons that could disrupt the U.S. ability to sustain an attack."[84]

Such a capacity would be particularly useful, U.S. strategists believe, in any future engagement with Russian forces in Europe or Chinese forces in the Asia-Pacific region, such as in the South China Sea or the area around Taiwan. Russia, it is claimed, has deployed a powerful array of defensive weapons—collectively, anti-access/area denial (A2/AD) systems—on its western borders, facing the NATO countries. Likewise, China is said to have deployed numerous short- and medium-range ballistic missiles aimed at U.S. warships and air bases in the western Pacific. A U.S. preemptive strike on such capabilities using hypersonic weapons at the onset of a conflict could help safeguard key U.S. assets and pave the way for subsequent attacks by main force units.

"Our potential adversaries have created the A2/AD environment," explained Lt. Gen. Neil Thurgood, director of the Army's Rapid Capabilities and Critical Technologies Office, in a February 2020 interview. "In order to move forces into that, you've got to create lines of penetration. Hypersonics is a strategic weapon that does that."[85]

When discussing the potential combat uses of hypersonic weapons, U.S. military officials typically speak of their utility in conventional warfare—to overcome enemy A2/AD capabilities and otherwise degrade enemy defenses. However, some analysts have suggested that they could also be used to attack an enemy's mobile missiles (some assumed to be dual-capable) and other highly sensitive targets, such as satellite communications systems and underground command centers. Even if the intent in such cases is to ensure success in a conventional conflict, a hypersonic missile barrage directed against such systems might be interpreted as the prelude to a nuclear attack, and trigger the early use of nuclear weapons.[86]

Russia and China seem to have pursued a somewhat different path in their development of hypersonic weapons. Ever since the U.S. withdrew from the Anti-Ballistic Missile (ABM) Treaty in June 2002, Chinese and Russian leaders have worried that a future U.S. first strike on their strategic nuclear forces might leave few of their ICBMs operational, and that, once launched, their remaining missiles could be intercepted by U.S. anti-missile batteries, thereby eliminating their second-strike retaliatory capability. By equipping their ICBMs with maneuverable hypersonic re-entry vehicles, however, they evidently hope that their surviving missiles will be able to evade any conceivable U.S. defenses, thus preserving their deterrent capability.

"After the United States withdrew from the Anti-Ballistic Missile Treaty," Russian Foreign Minister Sergey Lavrov said as recently as May 2022, "we had no choice but to work on hypersonic weapons because we knew perfectly well that the U.S. missile defense system would not be aimed at North Korea and Iran but against Russia and then China. We needed weapons that were guaranteed to overpower missile defenses."[87]

This, it appears, was the motive for development of Russia's nuclear-armed Avangard HGV: with its speed and maneuverability, Avangard is designed to evade any existing or future U.S. anti-missile systems, thereby ensuring the integrity of Russia's strategic deterrent. "I will speak about the newest systems of

Russian strategic weapons that we are creating in response to the unilateral withdrawal of the United States of America from the Anti-Ballistic Missile Treaty," Russian President Vladimir Putin said in March 2018 when describing Avangard and several other new weapons systems. These new weapons, he declared, are intended to "neutralize the threats posed by the deployment of the U.S. global missile defense system."[88] Similar reasoning appears to underlie China's August 2021 test of a hypersonic glide vehicle that reportedly circled the globe before striking its intended target.[89]

Although Russia and China appear to have placed their primary emphasis on the development of hypersonic vehicles for emplacement on ICBMs to evade U.S. anti-missile defenses, they have also pursued such weapons for theater use, presumably to target key enemy assets—warships, air bases, logistical hubs, and communications facilities—in the event of a conflict arising in Europe or the western Pacific. Russia's Kinzhal, for example, is thought to be intended for attacks on land- and ship-based missile defense systems, while Tsirkon is believed to be designed to target carrier battle groups and key land-based assets, such as C2 facilities.[90] During the war in Ukraine, Russia reportedly fired Kinzhal missiles at Ukrainian arms depots and port facilities.[91]

Arms Racing Behavior

Each of these countries initiated its pursuit of hypersonic weapons for unique strategic purposes, but all seem to have accelerated their efforts partly to overtake progress made by their rivals—behavior that has all the earmarks of a classic arms race. In the United States, at least, hypersonic advances by China and Russia are often cited by military officials to generate alarm among policymakers and garner support for comparable endeavors on the U.S. side.

"China's hypersonic weapons development outpaces ours … we're falling behind," Admiral Harry Harris, then commander of the U.S. Indo-Pacific Command and later ambassador to South Korea, told Congress in 2018. "We need to continue to pursue that and in a most aggressive way to ensure that we have the capabilities to both defend against China's hypersonic weapons and to develop our own offensive hypersonic weapons," he added.[92] More recently, U.S. Air Force Secretary Frank Kendall told Reuters that the U.S. and China are competing to develop the most capable hypersonic weapons. "There is an arms race, not necessarily for increased numbers, but for increased quality," he declared. "It's an arms race that has been going on for quite some time."[93]

Whether China or Russia has overtaken the United States in hypersonic weaponry is a matter of debate. Both assert they are ready to deploy hypersonic weapons, but it is unclear if those munitions are truly as capable as is claimed. The much-ballyhooed Chinese HGV test of August 2021, for example, is said to have missed its intended target by 24 miles, whereas a recent U.S. hypersonic vehicle test (admittedly following a shorter trajectory) missed its target by a mere six inches.[94] Furthermore, with each of these countries driven by their specific goals, the United States likely enjoys significant technological advantages in the hypersonic weapons types it seeks for its own arsenal. It would be misleading, therefore, to claim that the United States has fallen behind in a hypersonic arms race.

Whatever the case may be in this regard, the arms racing behavior described by Secretary Kendall has resulted, in some cases, in the rushed development of new hypersonic missiles before their strategic functions have been fully thought through. "The target set that we would want to address, and why hypersonics are the most cost-effective weapons for the U.S., I think it's still, to me, somewhat of a question mark," Kendall remarked in September 2021. "I haven't seen all the analysis that's been done to justify the current program."[95] This observation appears to be vindicated by the U.S. military's current drive to field at least eight new hypersonic weapons by the mid-2020s, not including defensive weapons; even a cursory examination of these programs (see Table 2), suggests a lot of overlap and indeterminate purpose.

The risk of arms racing behavior is being further exacerbated by the U.S. decision to develop new hypersonic missiles specifically for defense against an adversary's offensive hypersonic weapons. At present, three military contractors—Raytheon, Lockheed Martin, and Northrop Grumman—are competing to develop a prototype design for such a weapon, with the winner expected to begin producing combat-ready models later in the decade. No doubt these efforts will induce Russian and Chinese military officials to consider obtaining both additional offensive hypersonic capabilities as well as their own hypersonic defensive systems, triggering a typical "action-reaction" cycle in which advances in offensive weaponry on one side prompts increased defensive investments on the other, leading to countervailing advances in offensive weaponry, and so on, in an endless escalatory spiral.

Nevertheless, the presumed need to ensure a U.S. technological lead in hypersonic weaponry has been underscored by the nation's top defense contractors, many of which expect to benefit from higher spending in this area. "From a pure business perspective, there is a significant opportunity in the hypersonic domain," said former Raytheon Vice President Thomas Bussing at a December 2018 meeting of military contractors. Indeed, the hypersonic weapons

U.S. Hypersonic Weapons Programs

Lead	conventional, nuclear, dual-capable	Description	Speed	Range (in kilometers)	Schedule
AGM-183 Air-Launched Rapid Response Weapon (ARRW)					
Air Force	conventional	an air-launched hypersonic glide vehicle, using Tactical Boost Glide technology and with a tungsten fragmentation warhead (which is limited to soft targets)	Mach 6.5–8	1,600	flight testing through FY 2023
Hypersonic Attack Cruise Missile (HACM)					
Air Force	conventional	a hypersonic cruise missile, using air-breathing technology	Mach 5+*	unknown*	new start program in FY 2022; complete test and development in FY 2027
Long-Range Hypersonic Weapon (LRHW, also called Dark Eagle)					
Army	conventional	the common hypersonic glide body paired with the Navy's booster system on mobile ground platforms; at least the first battery will feature a tungsten fragmentation warhead	Mach 5+*	2,775	prototype deployment in FY 2023
Conventional Prompt Strike (CPS)					
Navy	conventional	the common hypersonic glide body paired with a submarine-launched booster system on Zumwult-class destroyers and Virginia-class submarines; this system may feature the tungsten fragmentation warhead or an alternative warhead	Mach 5+*	unknown*	initial operating capability on Zumwult-class destroyers in FY 2025 and on Virginia-class submarines in FY 2028
Hypersonic Air-Launched OASuW (HALO), also called Offensive Anti-Surface Warfare Increment II (OASuW-2)					
Navy	conventional	an air-launched, long-range hypersonic weapon system likely to be compatible with F/A-18 fighter jet	Mach 5+*	unknown*	new start in FY 2023; deployment in FY 2028
Tactical Boost Glide (TBG)					
DARPA	conventional	a hypersonic boost-glide vehicle; capabilities planned for Air Force and Navy	Mach 7+	tactical	complete third test flight in FY 2023
Operation Fires (OpFires)					
DARPA	conventional	a ground-launched system with TBG technology	Mach 5+*	1,600	program completed in FY 2022; capabilities to be developed for services
MoHAWC, previously Hypersonic Air-Breathing Weapon Concept (HAWC)					
DARPA	conventional	an air-launched hypersonic cruise missile that could be compatible with a variety of launch platforms; capabilities planned for the Air Force; successor program to HAWC	Mach 5+*	unknown*	new start in FY 2023; begin integration and ground testing in FY 2023

*no estimate or information publicly available

Russian Hypersonic Weapons Programs

Program	conventional, nuclear, dual-capable	Description	Speed	Range (in kilometers)	Schedule
Avangard (Project 4202)	nuclear, possibly conventional	a hypersonic boost-glide vehicle launched from an ICBM (SS-19 or Sarmat)	Mach 20+	6,000	deployed in 2019
Kinzhal ("Dagger")	dual-capable	a hypersonic air-launched, short-range ballistic missile; compatible with the MiG-31K interceptor jet and the Tu-22M3 strategic bomber	Mach 10	2,000	reportedly entered trial deployment in 2017 and became operational in 2018
3M22 Tsirkon (or Zircon)	conventional, though may possibly become nuclear capable	a hypersonic cruise missile able to be launched from ship or sea	Mach 5–8	500–1,000	deployed in 2023

Chinese Hypersonic Weapons Programs

Program	conventional, nuclear, dual-capable	Description	Speed	Range (in kilometers)	Schedule
Dongfeng-17 (DF-17)	dual-capable most likely	a hypersonic glide vehicle on a road-mobile, medium-range ballistic missile	Mach 5–10	1,800–2,500	some reports indicate a deployment in 2020
Xing Kong-2 (Starry Sky-2)	nuclear	a hypersonic vehicle prototype; also described as a hypersonic waverider vehicle	Mach 6	unknown*	some reports indicate a deployment in 2025

*no estimate or information publicly available

market could be worth "many billions of dollars," said Loren Thompson, a defense analyst who works with Lockheed Martin and other big firms. "We're talking about an entirely new class of weapons and the operating concepts to go with it."[96]

Escalation Risks and 'Entanglement'

Many weapons can be employed for offensive and defensive purposes, but hypersonic weapons, especially those designed for use in a regional context, are primarily intended to be used offensively—to destroy high-value, heavily-defended enemy assets, such as radar stations, missile batteries, and C2 facilities. This raises two major concerns: the risk of rapid escalation from a minor crisis to a full-blown war and the unintended escalation from conventional to nuclear warfare.

That hypersonic weapons are being designed for offensive use at an early stage in a conflict has been evident in U.S. strategic policy from the beginning. Claiming that a major adversary might try to hide or move critical assets at the outbreak of a crisis to protect them from U.S. air and missile strikes, the Pentagon presumed that its prompt global-strike program—once equipped with hypersonic missiles—would enable U.S. forces to attack those targets with minimal warning. "Systems that operate at hypersonic speeds…offer the potential for military operations from longer ranges with shorter response times and enhanced effectiveness compared to current military systems," DARPA has indicated.[97] Most of the hypersonic weapons being developed by the U.S. military, including the Air Force's ARRW and the Army's PrSM, are intended for strikes against key enemy assets at an early stage of conflict, when speed confers a significant advantage. Certain Russian weapons, such as the Kinzhal, also seem intended for this purpose.

Some analysts fear that the mere possession of such weapons might induce leaders to escalate a military clash at the very outbreak of a crisis, believing that

their early use will confer a significant advantage in whatever conflict might ensue, thereby reducing the chances for keeping the fighting limited. It is easy to imagine, for example, how a clash between U.S. and Chinese naval vessels in the South China Sea, accompanied by signs of an air and naval mobilization on either or both sides, might prompt one or another to launch a barrage of hypersonic weapons at all those ships and planes, hoping thereby to minimize their utility in any full-scale engagement that might follow. This might make sense from a military perspective, but would undoubtedly prompt a fierce counterreaction from the injured side and restrict efforts to halt the fighting at a lower level of violence.

A similar scenario could easily emerge in Europe, where U.S./NATO forces face Russian forces along a potential conflict perimeter stretching from the Arctic in the north to the Black Sea in the south. Should an armed encounter erupt at any spot along this perimeter, say in the Baltic states or the Black Sea, either or both sides might be tempted to launch hypersonic missiles at their adversary's key combat assets, so as to ensure success in a full-blown encounter. Indeed, President Putin has warned of such scenarios, saying that any U.S. deployment of offensive missiles in Ukraine would prompt Russia to deploy hypersonic weapons aimed at U.S. and NATO installations. "We would have to create a similar threat for those who are threatening us," he said in November 2021. "And we can do that already now," he added.[98]

The introduction of hypersonic weapons also raises concerns over the escalation from conventional to nuclear warfare. The United States has focused primarily on the development of hypersonic weapons carrying conventional warheads, but there is no fundamental reason why they could not be armed with nuclear weapons in the future. Furthermore, both Russia and China appear to be developing hypersonic weapons with a dual-use capability: Russia's Kinzhal is assumed to be dual-use and its Tsirkon, though initially conventional, may possess that capability in the future; China's DF-17 is also thought to be dual-capable.

This leads to what is called "warhead ambiguity": the risk that a defending nation, aware of an enemy's hypersonic launch and having scant time to assess the warhead type, will assume the worst and launch its own nuclear weapons before they can be destroyed by the incoming warheads. Concern over this risk has led the U.S. Congress to bar funding for the development of ICBM-launched hypersonic glide vehicles, thereby helping to propel the Pentagon's shift away from such systems and toward the development of medium-range weapons more suitable for use in a regional context.[99] Nevertheless, warhead ambiguity will remain a feature of any future conflict among nuclear-armed states involving the deployment of multiple hypersonic weapons, as a defender will never be certain that an enemy's assault is entirely non-nuclear. With as little as five minutes to assess an attack—the time it would take a hypersonic glide vehicle to traverse 2,000 miles—a defender would be understandably hard pressed to avoid worst-case assumptions.[100]

Equally worrisome is the danger of "target ambiguity": the possibility that a hypersonic attack, even if conducted with missiles known to be armed solely with conventional warheads, would endanger the early-warning and C2 systems a defender uses for both its nuclear and conventional forces, leading it to fear the onset of a nuclear attack. This is especially dangerous in light of what James Acton, a security analyst at the Carnegie Endowment for International Peace (CEIP), calls the "entanglement" problem. As he explains, the nuclear and conventional command-and-control systems of the major powers are widely assumed to be interconnected, or "entangled," making it difficult to clearly distinguish one from another. Therefore, any attack on C2 facilities at the onset of crisis, however intended, could be interpreted by the defender as a prelude to a nuclear rather than a conventional attack, and so prompt the defender to launch its own nuclear weapons before they are destroyed by an anticipated barrage of enemy bombs and missiles.[101]

The risk of target ambiguity arises with even greater severity in the case of attacks by conventionally-armed hypersonic missiles on the dual-use mobile missiles of an adversary. Russia and China have fielded dual-use missiles that pose a significant threat to key U.S. assets in Europe and Asia, respectively. As their mobility makes them difficult to track once fighting has commenced, they could be selected for attack with hypersonic weapons in the very first hours of a major U.S. clash with those countries. However, as some of these mobile assets are also viewed by their owners as nuclear retaliatory systems, a U.S. assault on them could be interpreted by the target state as part of a disarming first strike and so trigger its own use of atomic munitions.

All this points to yet another concern related to the impact of emerging technologies on the future battlefield: the risk that nuclear-armed nations, fearing scenarios of just this sort, will entrust more and more of their critical decision-making to machines, fearing that humans will not be able to process the vast amounts of information pouring in from various sources and make reasoned judgments under such enormous time pressures. With hypersonic weapons in the arsenals of the major powers, military leaders may conclude that sophisticated AI systems should be empowered to determine the nature of future missile attacks and select the appropriate

Deputy Secretary of State Wendy R. Sherman meets with Russian Deputy Foreign Minister Sergey Ryabkov at the start of the U.S.-Russia Strategic Stability Dialogue in Geneva, Switzerland on July 28, 2021. (U.S. Mission Geneva Photo)

response, possibly involving highly escalatory actions—a danger we address at length in Chapter 5.

Inserting Speed Bumps

Given the risks posed by hypersonic weapons—especially when their deployment is paired with other technological developments—it is essential that we consider measures for minimizing the dangers they pose to escalation control and strategic stability. Such efforts are especially urgent now, as the major powers rush ahead with the development and initial fielding of many such systems even though they remain largely unproven and the strategic rationale for their deployment has yet to be fully demonstrated. In contrast to the speed with which this is occurring, policymakers need to provide additional time in which to assess the potential utility and escalatory risk of hypersonic missiles as well as any alternative, already-existing capabilities that could fill a similar set of missions.

At present, there are no bilateral or multilateral fora in which officials of the U.S., Russia, and China can meet to discuss formal limits on hypersonic weapons. Although each of these states can and should take unilateral steps to slow their deployment of such systems, joint discussions will be essential to develop a common understanding of the risks inherent in a hypersonic arms race and to develop mutually acceptable restraints. Until formal inter-governmental talks of this sort can be convened, informal conversations on these topics should be conducted among scientists, arms control analysts, and retired military and diplomatic personnel—an approach known as "Track 1.5 Diplomacy." Without broaching classified information, these experts could assess the dangers posed by the unrestrained deployment of hypersonic weapons and share ideas for mitigating these risks.

A possible forum for direct talks between government officials on these topics is the bilateral U.S.-Russian Strategic Stability Dialogue. At a September 2021 meeting in Geneva to discuss the dialogue's future functioning, senior U.S. and Russian officials agreed to establish a "working group on capabilities and actions with strategic effects," and it has been expected that this group will examine the potentially destabilizing impacts of hypersonic weapons, among other emerging technologies.[102] While the dialogue was paused following Russia's February 2022 invasion of Ukraine, the two sides may eventually return to the table as New START's expiration in February 2026 nears with

no replacement agreement in sight. A U.S.-China strategic dialogue, if and when established, would hopefully address similar concerns.

If leaders of the major powers are prepared to discuss constraints on developing and deploying hypersonic weapons, they could adopt a number of approaches. One way to start would be to impose an international moratorium on flight tests of hypersonic weapons, as suggested by some arms control experts. Because the technology for most hypersonic weapons is still largely unproven, a test moratorium would allow time for policymakers to devise multilateral controls on such systems.[103] Assuming that a ban of this sort is unachievable at this time, the parties to such discussions could agree on various confidence-building measures (CBMs) designed to reduce the escalatory dangers of hypersonic deployments or narrow their application. Such measures could include information-sharing on the range and capabilities of proposed weapons and protocols intended to differentiate conventionally-armed hypersonic weapons from nuclear-armed ones, so as to reduce the risk of warhead ambiguity and unintended escalation.

The adoption of more formal, restrictive measures will no doubt prove more difficult, as all the countries involved see a military advantage in deploying new hypersonic systems quickly. Nevertheless, when and if officials of China, Russia, and the U.S. are prepared to discuss such constraints, there are a number of ways they could proceed. One approach would be an outright ban on certain types of weapons—for example, ground-launched missiles with specific range limits, as in the INF Treaty. Such a ban would reduce the risk of attacks on each country's critical assets at the onset of an engagement, preventing rapid escalation of the fighting. Another approach, in the style of New START, would be to limit the number of deployed weapons below a certain threshold, which would eliminate fears of a disarming first strike.[104]

Admittedly, such negotiations appear distant, so Congress should intervene and impose its own speed bumps on the race to deploy hypersonic weapons. Before approving all the funds sought by the Pentagon for hypersonic weaponry, lawmakers should ask: What are these munitions needed for? Do they pose an unnecessary risk of escalation? Are there better alternatives? By raising these questions, Congress would also call into question the utility of similar moves by other countries, thereby facilitating multiparty talks on hypersonic missile deployments.

Chapter 4:

Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation

When the Obama administration issued its Nuclear Posture Review (NPR) in 2010, laying out the nation's nuclear weapons policies, it identified only two permissible uses for nuclear munitions by the United States: to deter their employment by another nuclear power, and to blunt "a massive conventional attack" by a well-armed adversary. The 2010 NPR also envisioned a time when only the first of those uses remained, leaving "deterrence of nuclear attack on the United States or our allies and partners the sole purpose of U.S. nuclear weapons."[105] However, when the Trump administration released its own Nuclear Posture Review in 2018, the pendulum had swung in the opposite direction, with nuclear weapons being accorded more potential uses, not less. These included the revival of a Cold War precept, the deployment of so-called "low-yield" nuclear munitions to deter and, if necessary, retaliate against the use of similar weapons by a potential adversary. The 2018 Trump policy also incorporated an entirely *new* justification for the unilateral use of nuclear weapons by the United States: to counter an enemy cyberattack on the nation's nuclear command, control, and communications (NC3) systems.

Speaking in particular of possible Russian cyberattacks on America's NC3 networks (but employing language that would also apply to China or another future adversary), the 2018 NPR states, "To correct any Russian misperceptions of advantage and credibly deter Russian nuclear or non-nuclear strategic attacks—which could now include attacks against U.S. NC3—the President must have a range of limited and graduated options, including a variety of delivery systems and explosive yields."[106] Or, in plain English, an attack by Russia on American NC3 systems would be sufficient to justify a U.S. nuclear response.

The Pentagon justified the perceived need to threaten the use of nuclear weapons in response to an attack on the nation's nuclear command, control, and communications systems in the 2018 NPR on three grounds: a reliable NC3 system was absolutely essential to the effective functioning of the nation's nuclear deterrence capability; the nation's NC3 networks were becoming increasingly vulnerable to newly-developed cyberweapons; and third, any attempt to disable these networks by such means constituted an assault on the U.S. nuclear deterrent itself.

"The emergence of offensive cyber warfare capabilities has created new challenges and potential vulnerabilities for the NC3 system," the 2018 nuclear policy stated. "Potential adversaries are expending considerable effort to design and use cyber weapons against networked systems," including nuclear command, control, and communications. In light of these threats, it avowed, the U.S. must take action to bolster the safety of its NC3 systems against hostile assault, both by increasing its ability to withstand attack and by raising the costs for future NC3 attackers.[107] Not mentioned—at least not in the unclassified text of the NPR—were extensive U.S. efforts to employ cybertools to infiltrate and potentially incapacitate the NC3 systems of likely adversaries, including Russia, China, and North Korea.[108]

When first promulgated in 2018, the claim that a cyberattack on American NC3 capabilities constitutes sufficient grounds to launch a nuclear attack was seen by many observers as a dangerous shift in policy, greatly increasing the risk of accidental or inadvertent nuclear escalation in a crisis. "The entire broadening of the landscape for nuclear deterrence is a very fundamental step in the wrong direction," said former Secretary of Energy Ernest Moniz. "I think the idea of nuclear deterrence of cyberattacks, broadly, certainly does not make any sense."[109] Nevertheless, this policy was retained throughout the Trump presidency.

Despite this shift in declaratory policy, the link between cyber operations, nuclear command and control systems, and nuclear escalation has been firmly established in the thinking of military planners in the United States and other nuclear-armed

A U.S. F-22 fighter shadows a Russian Tu-95 bomber on May 20, 2019 in international airspace near Alaska. Aircraft and missile detection systems rely heavily on electronic communications, making them potential targets for cyberwarfare. (Photo: NORAD)

states. Most officials now assume that any conflict erupting between the major powers will be preceded or accompanied by cyberattacks on adversary NC3 networks and that each is constantly probing the NC3 defenses of the others in search of vulnerabilities that might be exploited in future such attacks. "We are in a very, very contested domain in cyber," Chairman of the Joint Chiefs of Staff General Mark A. Milley told the Aspen Security Forum in November 2021. "Every day our nation is literally being hacked."[110]

The development and deployment of both defensive and offensive cybertools have thus become a significant feature of military relations among the major powers, raising entirely new sorts of threats to strategic stability. Analysts worry, for example, that efforts by one major power to infiltrate the NC3 systems of another for information-gathering purposes can be interpreted, in a time of crisis, as the prelude to a disarming "counterforce" strike aimed at the target state's nuclear deterrent, conceivably prompting the early or inadvertent use of nuclear weapons. Furthermore, as the nuclear command, control, and communications systems of the major powers are often interwoven with their non-nuclear C3 systems, a cyberattack on the latter network could be misinterpreted as an assault on the former, producing a similar outcome.[111]

As governments and military forces come to rely on computers for an ever-expanding of array of critical tasks, their vulnerabilities to cyberattack will grow—as will the temptation to devise new cyberweapons aimed at their adversaries' vital systems. In this environment, it is essential to assess the impact of cyberattack developments on strategic stability and to consider the enactment of new measures to bolster stability and reduce the risk of inadvertent escalation.

The Cyber-Nuclear Connection

The risks to strategic stability arise from the fact that the NC3 systems of the United States and other nuclear-armed states are heavily dependent on computers and other digital processors for virtually every aspect of their operation and because those systems are highly vulnerable to cyberattack.

Every nuclear force is composed, most basically, of nuclear explosive devices, the delivery systems (planes and missiles) needed to transport these devices to their intended targets, early-warning radars and other systems used to detect enemy attacks, and the presidents and prime ministers empowered to initiate a nuclear exchange. Connecting them all, however, is the NC3 system—an extended network of communications and data-processing systems, all of them reliant on cyberspace. Warning systems, whether ground- or space-based, must constantly watch for and analyze possible enemy missile launches; information on actual threats must rapidly be communicated to decision-makers, who must then weigh possible

responses and communicate their chosen outcomes to air and missile launch facilities, which in turn must provide target data to delivery systems.[112]

Because an effective, reliable NC3 infrastructure is essential to the maintenance of a nuclear-armed state's deterrent capability, it is not surprising that rival nuclear powers view these systems as a promising vector of attack. During peacetime, cyber intrusion allows for one antagonist to probe for details about the nuclear plans, deployments, and capabilities of its rivals (i.e., cyber espionage); during wartime, preemptive cyberstrikes on an enemy's NC3 could theoretically impair its ability to carry out attack missions ordered by senior officials.

"The lure of cyberspace seems almost irresistible," a team of researchers assembled by the Carnegie Endowment for International Peace (CEIP) observed in 2021. "Cyber tools are less expensive to acquire and operate than conventional weapons. They offer huge potential geographic coverage, economies of scale, and force-projection capabilities." Moreover, "cyber operations are typically highly secretive. This avoids the scrutiny associated with other types of operations and presents options for plausible deniability."[113]

The use of cyberspace to gain an advantage over adversaries takes many forms and is not always aimed at nuclear systems. China has been accused of engaging in widespread cyberespionage to steal technical secrets from U.S. firms for economic and military advantages. Russia has been accused of exploiting cyberspace to interfere in the 2016 and 2020 U.S. presidential elections. Criminal groups, including some thought to be allied with state actors—including in Russia and North Korea—have used cyberspace to extort money from banks, municipalities, and individuals.[114] Attacks of these sorts occupy most of the time and attention of the civilian and military cybersecurity organizations charged with thwarting such attacks. Yet, for those who worry about strategic stability and the risks of nuclear escalation, it is the threat of cyberattacks on NC3 systems that provokes the greatest concern.

This concern stems from the fact that, despite the immense effort devoted to protecting NC3 systems from cyberattack, no enterprise that relies so extensively on computers and cyberspace can be made one hundred percent invulnerable to attack. This is so because such systems employ many devices and operating systems of various origins and vintages—most incorporating numerous software updates and "patches" over time—offering multiple vectors for attack. Electronic components can also be modified by hostile actors during production, transit, or insertion, and the software involved can be tampered with or corrupted in some fashion. The experienced "cyberwarriors" of every major power have been working for years to probe for weaknesses in these systems and have devised a vast array of cyberweapons, including tools for breaking into an adversary's computer networks (sometimes described as "delivery systems") as well as malicious software ("malware," also called a "payload") to permit the extraction of vital secrets and/or the disabling of critical infrastructure.[115]

Military officials in the United States and, presumably, the other nuclear powers, have made enormous efforts over time to enhance the invulnerability of their NC3 systems to cyberattacks of these sorts. At the same time, however, they have also increased the scale and sophistication of their NC3 systems, adding ever more computers and communications gear to these networks—and so increasing the number of possible entry points for cyber intrusion. As noted by Herbert Lin, a senior research scholar at Stanford University, "Greater system complexity means a larger attack surface (i.e., more places where flaws can be found), which an adversary can exploit (i.e., vulnerabilities)."[116]

Although activity in cyberspace is much more difficult to detect and track than conventional military operations, enough information has become public to indicate that the major nuclear powers, notably China, Russia, and the United States—along with such secondary powers as Iran and North Korea—have established extensive cyberwarfare capabilities and engage in offensive cyber operations on a regular basis, often aimed at critical military, financial, and energy infrastructure. In the buildup to the war in Ukraine, for example, the Biden administration revealed that it had removed widespread malware from U.S. computer networks thought to have been planted by Russian intelligence agencies in an attempt to hobble critical infrastructure once fighting commenced.[117]

"Cyberspace is a contested environment where we are in constant contact with adversaries," said General Paul M. Nakasone, director of the National Security Agency (NSA) and commander of the U.S. Cyber Command (Cybercom), in February 2019 testimony before the Senate Armed Services. "We see near-peer competitors [i.e., China and Russia] conducting sustained campaigns below the level of armed conflict to erode American strength and gain strategic advantage."[118]

While eager to speak of adversarial threats to U.S. interests, Nakasone was noticeably, but not surprisingly, reluctant to say much about U.S. offensive operations in cyberspace. He acknowledged, however, that Cybercom took action to disrupt possible Russian interference in the 2018 midterm elections. "We created a persistent presence in cyberspace to monitor adversary actions and crafted

tools and tactics to frustrate their efforts," he testified in 2019. According to press accounts, this included a cyberattack aimed at paralyzing the Internet Research Agency, a "troll farm" in St. Petersburg said to have been deeply involved in generating disruptive propaganda during the 2016 presidential elections.[119]

Other press investigations have disclosed two other offensive operations undertaken by the United States. One, called "Olympic Games," was intended to disrupt Iran's drive to increase its uranium-enrichment capacity by sabotaging the centrifuges used in that process by infecting them with the so-called Stuxnet virus. Another, described as a "left of launch" operation to distinguish it from attempts to intercept a missile after it had been fired, reportedly involved cyberattacks designed to cause malfunctions in North Korean missile tests.[120] Although not aimed at either of America's principal nuclear adversaries, those two attacks demonstrated a willingness and capacity to conduct cyberattacks on the nuclear infrastructure of other states.

Efforts by strategic rivals of the United States to infiltrate and eventually degrade U.S. nuclear infrastructure are far less documented but thought to be no less prevalent. Russia, for example, is believed to have planted malware in the U.S. electrical utility grid, possibly with the intent of cutting off the flow of electricity to critical NC3 facilities in the event of a major crisis.[121] Indeed, every major power, including the United States, is believed to have crafted cyberweapons aimed at critical NC3 components of their adversaries and to have implanted malware in enemy systems for potential use in some future confrontation.

Pathways to Escalation

Knowing that the NC3 systems of the major powers are constantly being probed for weaknesses and are probably infested with malware designed to be activated in a crisis, what does this tell us about the risks of escalation from a "nonkinetic" battle—that is, one fought with cyberweapons—to a kinetic one, using conventional weapons at first and then, conceivably, nuclear ones? None of this can be predicted in advance, but analysts who have studied the subject worry about the emergence of dangerous new pathways for escalation. In fact, several such scenarios have been identified.[122]

The first and possibly most dangerous path to escalation would arise from the early use of cyberweapons in a great-power crisis to paralyze the vital command, control, and communications (C3) capabilities of an adversary, many of which serve both nuclear and conventional forces. Given the heavy reliance placed by senior officers on reliable and extensive C3 systems to track enemy actions and oversee countermoves by their own forces, the incapacitation of these networks through cyberattacks

U.S. servicemen conduct a defensive cyberoperations exercise at Ramstein Air Base, Germany, on March 8, 2019. (U.S. Air Force photo by Master Sgt. Renae Pittman)

at the very onset of battle would, presumably, convey an enormous advantage to the attacking side. In the "fog of war" that would naturally ensue from cyberattacks of this sort, the recipient of such an assault might anticipate more punishing follow-up kinetic attacks, possibly including a preemptive strike on its nuclear deterrent capabilities. Fearing the possible loss of those capabilities, the nation under assault might place its nuclear weapons on high alert and, in the worst case, launch them in response to ambiguous signs of attack. This might occur, for example, in a confrontation between NATO and Russian forces in eastern Europe or between U.S. and Chinese forces in the Asia-Pacific region.

Speaking, for example, of a possible confrontation in Europe, James N. Miller Jr. and Richard Fontaine of the Center for a New American Security wrote that "both sides would have overwhelming incentives to go early with offensive cyber and counter-space capabilities to negate the other side's military capabilities or advantages." If those early attacks succeeded, "it could result in [a] huge military and coercive advantage for the attacker." This scenario might induce the recipient of such attacks to back down, affording its rival a major victory at very low cost. Alternatively, however, the recipient might view the attacks on its critical C3 infrastructure as the prelude to a full-scale attack aimed at neutralizing its nuclear capabilities, and so choose to strike first. "It is worth considering," Miller and Fontaine concluded, "how even a very limited attack or incident could set both sides on a slippery slope to rapid escalation."[123]

What makes the insertion of latent malware in an adversary's NC3 systems so dangerous is that it may not even need to be activated to increase the risk of nuclear escalation: simply by their presence, they could sow doubts in the minds of adversary leaders regarding the reliability of their NC3 systems. "The introduction of a flaw or malicious code into nuclear weapons through the supply chain that compromises the effectiveness of those weapons could lead to a lack of confidence in the nuclear deterrent," thereby undermining strategic stability, Page O. Stoutland and Samantha Pitts-Kiefer wrote in a 2018 paper for the Nuclear Threat Initiative. Without confidence in the reliability of its nuclear weapons infrastructure, a nuclear-armed state might misinterpret confusing signals from its early-warning systems and, fearing the worst, launch its own nuclear weapons rather than lose them to an enemy's first strike.[124]

Compounding these dangers, in the view of many analysts, is the widespread integration of nuclear C3 with conventional command, control, and communications systems. For reasons of convenience and economy, the major powers have chosen to rely on the same early-warning and communications

What makes the insertion of latent malware in an adversary's NC3 systems so dangerous is that it may not even need to be activated to increase the risk of nuclear escalation.

links to serve both their nuclear and conventional forces—a phenomenon described by James Acton of CEIP as "entanglement." In the event of a great-power conflict, one side or the other might employ its cyberweapons to confuse or disable its adversary's conventional C3 in the opening stages of a nonnuclear assault; but the recipient of such attacks, not knowing whether it is conventional or nuclear systems that are the intended targets, might fear it is the latter and so prepare for immediate nuclear operations, again risking early weapons use.[125]

Yet another pathway to escalation might arise from a cascading series of cyberstrikes and counterstrikes against vital national infrastructure, rather than on military targets. All major powers, along with Iran and North Korea, have developed and deployed cyberweapons designed to disrupt and destroy major elements of an adversary's key economic systems, such as power grids, financial systems, and transportation networks. Russia, for example, is believed to have infiltrated the U.S. electrical grid, and it is widely assumed that the United States has done the same in Russia.[126]

The danger here is that economic attacks of this sort, if undertaken during a period of tension and crisis, could lead to an escalating series of tit-for-tat attacks against ever more vital elements of an adversary's critical infrastructure, producing widespread harm and eventually leading one side or the other to initiate kinetic attacks on critical military targets, possibly initiating a spiral of escalation ending in nuclear conflict. For example, a Russian cyberattack on the U.S. power grid could trigger U.S. attacks on Russian energy and financial systems, causing widespread disorder in both countries and generating an impulse for even more devastating attacks. At some point, Miller and Fontaine argue, such attacks "could lead to major conflict and possibly nuclear war."[127]

These are by no means the only pathways to escalation resulting from the offensive use of cyberweapons. Others include efforts by third parties, such as proxy states or terrorist organizations, to provoke a global nuclear crisis by causing early-warning

systems to generate false readings ("spoofing") of missile launches. Nevertheless, these examples provide a clear indication of the severity of the threat. As states' reliance on cyberspace grows and cyberweapons become ever more potent, the dangers of unintended or accidental escalation can only grow more severe.

'Defending Forward'

Under these circumstances, one would think the major powers would seek to place restrictions on the use of offensive cyberweapons, especially those aimed at critical NC3 systems. This approach, however, is not being pursued by the United States or the other major powers.

Under the Obama administration, the Department of Defense was empowered to conduct offensive cyberstrikes on foreign states and entities in response to like attacks on the United States, although any such moves required high-level review by the White House (and were rarely approved). This approach was embedded in Presidential Policy Directive 20 (PPD-20) of October 2012, which states that any cyberattack that might result in "significant consequences," such as loss of life or adverse foreign policy impacts, required "specific presidential approval."

Officials in the Trump administration found this requirement unduly restrictive and so persuaded the president to rescind PPD-20 and replace it with a more permissive measure. The resulting document, National Security Presidential Memorandum 13 (NSPM-13), was approved in September 2018, but never made public. From what is known of NSPM-13, senior military commanders, such as Nakasone, were granted preapproval to undertake offensive strikes against foreign entities under certain specified conditions *without* further White House clearance. In accordance with the new policy, military planners were authorized to prepare for offensive cyberattacks by seeking vulnerabilities in adversarial computer networks and by implanting malware in those weak spots for potential utilization when and if a retaliatory strike was initiated. President Biden reportedly has left NSPM-13 in place, but added a requirement that large-scale cyber operations be brought to the National Security Council (NSC) for review and possible adjustment.[128]

As translated into formal military doctrine, this approach is described as "defending forward," or seeking out the originators of cyberattacks aimed at this country and neutralizing them through counterstrikes and the insertion of malware for future activation. As explained by the Cyber Command's vision statement, "Defending forward as close as possible to the origin of adversary activity extends our reach to expose adversaries' weaknesses, learn their intentions and capabilities, and counter attacks close to their origins."[129]

In embracing this strategy, Nakasone and other senior officials insist that their intention is defensive: to protect U.S. cyberspace against attack and deter future assaults on U.S. networks by letting opponents know their own systems will be crippled if they persist in malicious behavior. "For any nation that's taking cyber activity against the United States," said then national security advisor John Bolton when announcing the adoption of NSPM-13, "they should expect we will respond offensively as well as defensively."[130] Any potential adversary following these developments will almost certainly interpret "defending forward" as preparation for offensive strikes in the event of a crisis, which would invite them to step up their own defensive and offensive moves.

Much less is known about the strategic cyberwar policies of other powers, but they likely parallel those of the United States. China, for example, has long been known to employ cyberspace to spy on U.S. military technological capabilities and steal what they can for use in developing their own weapons systems. Russia has been even more aggressive in its use of cyberspace, employing cyberweapons to cripple Ukraine's electrical grid in 2015 and to influence the 2016 and 2020 U.S. elections. That Moscow has also sought to infiltrate the U.S. electrical grid suggests that it, too, intends to "defend forward," by preparing for possible cyberattacks on U.S. command, control, and communications capabilities, including NC3 facilities.

Although largely occurring in secret, what can aptly be called "an arms race in cyberspace" is clearly underway. All of the major nuclear-armed powers are devising ever more powerful offensive and defensive cyberweapons for use both in peacetime and in the event of war. Each is seeking to enhance its defenses against adversary attack; however, just as is the case in ballistic missile offense and defense, it is easier and cheaper to devise offensive cybertools than defensive ones. In the event of a crisis, then, there will be a strong temptation to employ the new technologies early in the encounter, when they might be used to maximum effect—possibly setting in motion an escalatory process resulting in nuclear weapons use.

Arms Control in Cyberspace

Given the various ways in which conflict in cyberspace could result in nuclear weapons use, steps must be taken to minimize the risk of escalation migrating from one domain to the other. It is undeniable, however, that devising agreements to curb malicious and escalatory behavior in cyberspace will prove no easy task. Computer software cannot readily be classified and tallied the way bombers and missiles can, and states do not agree on definitions of offensive and defensive cyberweapons—let alone on measures to control them. Nevertheless, some efforts have

been made to develop rules and protocols to restrain the destabilizing use of cybertechnologies, and these provide a framework for further consideration.

The starting point for all of these initiatives is a recognition that cyberattacks on an adversary's NC3 networks—however appealing as a substitute for or an adjunct to kinetic attacks—pose significant risks of accidental or inadvertent escalation that could prove catastrophic for all parties concerned. As noted by analysts from the U.S. and China assembled by CEIP, these two countries "objectively share common interest" in avoiding a cyber-initiated escalatory cycle. Once acknowledging this fundamental precept, the two sides "could define certain types of cyber operations as mutually off limits and then identify ways to bolster each other's confidence that such limits are being respected."[131]

Of all the measures that would most enhance stability in this respect, experts agree, would be bilateral agreements between the U.S. and Russia and the U.S. and China to abstain from cyberattacks on each other's NC3 systems. Such measures, the CEIP analysts suggested, could include commitments to forgo cyber espionage in each other's core NC3 networks, the planting of disruptive malware in those networks for future use, and offensive cyberstrikes during a crisis. As part of these initiatives, they noted, the parties could agree to separate or "dis-entangle" their conventional and nuclear C3 systems, so as to prevent cyber operations in the one area from spilling over into the other. Together, such steps "could enhance stability and reduce the risk of miscalculation."[132]

While acknowledging that measures of this sort could significantly reduce the risk of inadvertent escalation, most analysts contend that it will prove exceedingly difficult to negotiate such an agreement, given the high level of distrust between the major powers, the high degree of secrecy involved, and the enduring appeal of cyber operations. Verifying such an agreement is assumed to represent another major hurdle, as the nuclear powers are highly reluctant to share information about their NC3 capabilities—let alone their vulnerabilities.[133] Nevertheless, some analysts insist that an agreement of this sort, while not verifiable in the traditional sense, could be made enforceable through a form of mutual deterrence. "Any state that considered launching a cyber operation in violation of the agreement would have to reckon with the possibility that the target (which would presumably be scanning its networks continuously) would detect the intrusion and respond in kind," Acton wrote in the Spring 2020 issue of *Daedalus*.[134]

Assuming that a formal, binding commitment to avoid attacks on each other's NC3 systems is not something the major nuclear powers are likely to agree to in the immediate future, there is still much to gain from dialogues among them on the cyber threats to strategic stability and strategies for mitigating them. Such talks, modeled on the bilateral U.S.-Russian Strategic Stability Dialogue, could include both diplomats and specialists with knowledge of cyber and NC3 systems. A dialogue of this sort "could make it easier to clarify to each other the types of restraint that would be most important for strategic stability," analysts at CEIP suggested in 2021. "It could cover how each side views cyber operations, including what would be seen as escalatory and how each might try to signal willingness to de-escalate or pursue off-ramps." Such a dialogue, they add, "could help prevent inadvertent escalation in crises or conflict."[135]

An added benefit of such conversations is that they could help establish lines of communication between the top cyber officials of rival states, allowing one side or the other to inquire about suspicious activity in its key systems and/or provide reassurance that a disruptive attack is not under way. Participants could also use these sessions to devise confidence-building measures (CBMs) for their governments to undertake. Initiatives of this sort are intended to inculcate a degree of trust among potential adversaries and thereby pave the way for more consequential, binding agreements.

In the cyber realm, CBMs might include, for example, information-sharing on measures being taken by each side to prevent third-party cyberattacks on their NC3 networks, such as attacks by rogue actors seeking to trigger a crisis by spoofing a cyberstrikes by one of the nuclear powers. Other CBMs could include the installation of hotlines connecting each side's top cyber officials, so as to allow for reliable communications even during a crisis.

Many analysts, believing that bilateral measures of this sort will be difficult to achieve in the short term, say that the major nuclear powers should be encouraged to undertake unilateral steps to promote strategic stability. These could include moves to better protect vital computer networks against hostile intrusion and to ensure high-level oversight over all offensive cyber operations. "States can and should act unilaterally to mitigate the risks [of inadvertent escalation]," Acton affirmed in *Daedalus*.[136]

Mindful that offensive cyber operations could be initiated by junior officers lacking a full understanding of the possible escalatory consequences of such moves, Acton and others have called for requirements that all such decisions be subjected to rigorous scrutiny and be made at appropriately high levels of executive oversight. The nuclear powers, Acton wrote, "should put in place rigorous internal processes—if they do not already exist—to ensure that, in deciding whether to proceed with a potentially escalatory cyber operation, the strategic

risks are fully considered and weighed against the potential intelligence and military benefits." Such decisions, moreover, "should rest with the senior officials who would be responsible for managing the real-world consequences of escalation."[137]

Another area where unilateral action would be extremely valuable, analysts agree, would be in securing greater separation between conventional and nuclear C3 systems. As noted earlier, the fact that these systems are often "entangled" means that a cyberattack on conventional networks could spill over into nuclear ones (or appear to be doing so), thereby triggering unintended nuclear escalation. To reduce this risk, the nuclear powers should take action to separate the two systems as much as possible. "Entanglement between conventional and nuclear systems means that attacks on the former could affect or be perceived to be intended to affect the latter," Herbert Lin wrote in 2021.[138]

In addition to advocating these bilateral and unilateral initiatives, various governmental and non-governmental actors have called for the adoption of international norms in cyberspace, to prevent undesirable military outcomes as well as other disruptive actions, such as ransomware attacks and human rights abuses. Normative measures like these would not be binding on nation-states, but might influence their decision-making and discourage malign and destructive activities.

In an effort to facilitate the adoption of such norms, the UN General Assembly (UNGA) established a group of governmental experts in 2011 to assess the dangers in cyberspace and to consider "possible cooperative measures to address them, including norms, rules, or principles of responsible behavior of States."[139] In its first report, released in 2013, the expert group affirmed that "International law, and in particular the Charter of the United Nations, is applicable" in cyberspace, or what it called the information and communications technology (ICT) sphere.[140] A second report, issued in 2015, went further, articulating a set of norms to govern behavior in this sphere. Foremost among these was the precept that states "should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure" of another country.[141] These principles were incorporated into UNGA Resolution 70/237 and approved by member states on December 23, 2015, thus providing an initial framework for responsible state behavior in cyberspace.[142]

Since the adoption of Resolution 70/237, the General Assembly has continued to pursue the development of norms for responsible state behavior in cyberspace. Pursuant to Resolution 73/27 of December 5, 2018, it established an "Open-Ended Working Group," composed of representatives of member states, to consider the adoption of additional norms in the field and to devise confidence-building measures aimed at promoting international cooperation in the implementation of such measures. This group has been meeting regularly and, following the adoption of another UNGA resolution in December 2020, will continue its work for another five-year period, commencing in 2022.

Developing effective restraints on the disruptive use of cybertools is likely to prove a long and arduous process. Analysts worry, moreover, that the speed of technological advance in this realm is exceeding the pace of progress in the political and diplomatic realm. Nevertheless, political leaders have come to grasp the dangers arising from the uncontrolled use of cyberweapons and have begun looking at possible pathways toward sensible control, many of which have been described above. Given the enormous risks of miscalculation in cyberspace, it is essential that leaders accelerate their efforts to assess these dangers and take effective action to minimize them.

Chapter 5:

'Skynet' Revisited: The Dangerous Allure of Nuclear Command Automation

The Pentagon's budget request for fiscal year 2022 included $15.4 billion for modernization of the U.S. nuclear weapons complex, representing a mere down-payment on the estimated $1.7 trillion that will be spent on this massive endeavor over the next 30 years. Most of this largess will be used to replace existing nuclear delivery systems—intercontinental ballistic missiles (ICBMs), missile-firing submarines, and long-range bombers—with new, more capable systems. But a surprisingly large share of the FY 2022 request, nearly $3 billion, was sought for the modernization of the nation's nuclear command, control, and communications (NC3) infrastructure—the electronic systems that inform national leaders of a possible enemy attack and enable the president to order the launch of America's own nuclear weapons.[143]

Just as existing delivery systems are being replaced with a new ICBM (the Sentinel), a new missile submarine (the Columbia-class), and a new strategic bomber (the B-21 Raider), the Department of Defense expects to spend tens of billions of dollars over the coming decades to replace the existing NC3 infrastructure with a far more advanced and capable system, called "NC3 Next." This evolving system of computers and communications links will be designed to speed information-sharing and to protect against increasingly severe cyberattacks.[144] As part of this drive, Pentagon planners also seek to accelerate the *automation* of these systems—a goal that has certain attractions in terms of increased speed and accuracy, but one that raises troubling questions about the role of machines in determining humanity's fate in a future nuclear showdown.

Science fiction filmmakers have long envisioned the possibility of machines acquiring the capacity to launch nuclear weapons on their own. The 1964 movie "Dr. Strangelove" presupposes that the Soviet Union has installed a "doomsday machine" primed to detonate automatically should the country come under attack by U.S. nuclear forces. When the U.S. leadership fails to halt such an attack by a rogue Air Force general, the doomsday scenario is set in motion. In the 1983 blockbuster "WarGames," a teenage hacker inadvertently ignites a nuclear crisis when he hacks into the (fictional) War Operation Plan Response (WOPR) supercomputer and prompts the machine to initiate what it believes is a game, resulting in the actual launch of U.S. nuclear weapons. Yet another vision of computers run amok was portrayed a year later in "The Terminator," in which a superintelligent computer known as Skynet again controls U.S. nuclear weapons and elects to eliminate all humans by igniting a catastrophic nuclear war.

To be sure, none of the plans for NC3 automation now being considered by the Department of Defense resemble anything quite like the WOPR or Skynet. However, these plans do involve developing essential building blocks for a highly automated command and control system that will progressively diminish the role of humans in making critical decisions over the use of nuclear weapons. Humans may be accorded the final authority to launch nuclear bombers and missiles as this process unfolds, but assessments of enemy moves and the winnowing down of possible U.S. responses will largely be conducted by machines relying on artificial intelligence.

The total overhaul of America's NC3 infrastructure was first proposed during the Trump administration, in its Nuclear Posture Review (NPR) report of February 2018. The existing NC3 system, the report stated, "is a legacy of the Cold War, last comprehensively updated almost three decades ago." Although many of its individual components—early-warning satellites and radars, communications satellites and ground stations, missile launch facilities, and national command centers—had been modernized over time, much of the interconnecting hardware and software has become obsolete, the report stated. The growing effectiveness

In the 1983 film "WarGames," a computer placed in charge of U.S. nuclear weapons begins a simulation that nearly leads to the launch of U.S. missiles. While no U.S. Defense Department plans resemble anything quite like that scenario, they do seek to develop essential building blocks for a highly automated command and control system that will progressively diminish the role of humans in making critical decisions over the use of nuclear weapons. (Photo: Hulton Archive/Getty Images)

of cyberattacks, moreover, was said to pose an ever-increasing threat to the safety and reliability of critical systems. To ensure that the president enjoyed timely warning of enemy attacks and was able to order appropriate responses—even under conditions of intense nuclear assault and cyberattack—the entire system would have to be rebuilt.[145]

Given these highly demanding requirements, the 2018 NPR report called for overhauling the existing NC3 system and replacing many of its component parts with more modern, capable upgrades. Key objectives, it stated, would include strengthened protection against cyber and space-based threats, enhanced tactical warning and attack assessment, and utilization of sophisticated decision-support technology. These undertakings are ambitious and costly, and so will constitute a major component of the overall nuclear modernization effort going forward. In January 2019, the Congressional Budget Office projected that the cost of modernizing the entire NC3 system over the ensuing decade would total $77 billion.[146]

The 2018 NPR did identify increased automation as a specific objective of this overhaul. That is so, in part, because automation is already built into many of the systems incorporated in the existing NC3 system and will remain integral to their replacements. At the same time, many proposed systems, such as decision-support technology—algorithms designed to assess enemy intentions and devise a menu of possible countermoves from which combat commanders can choose—are still in their infancy. Nevertheless, virtually every aspect of the NC3 upgrade is expected to benefit from advances in AI and machine learning.

The Allure of Automation

The quest to further automate key elements of America's NC3 architecture is being driven largely by an altered perception of the global threat environment. Although the existing framework was always intended to provide decisionmakers with prompt warning of enemy nuclear attack and to operate even under conditions of nuclear war, the operational challenges faced by that system have grown more severe in recent years. Most notably, the decision-making system is threatened by the ever-increasing destructive capacity of conventional weapons and the growing sophistication of cyberattacks—and, as a result of those two, the growing *speed* of combat.

The existing NC3 architecture was designed in the previous century to detect enemy ICBM and bomber launches and provide decision-makers with enough time—as much as 30 minutes in the case of ICBM attacks—to assess the accuracy of launch warnings and still ponder appropriate responses. These systems did not always work as intended—the

history of the Cold War is replete with false warnings of enemy attacks—but the cushion of time prevented a major catastrophe.[147] Moreover, the reasonably clear distinction between conventional and nuclear weapons enabled military analysts to avoid confusing non-nuclear assaults with potentially nuclear ones.

With the introduction of increasingly capable conventional weapons, however, the distinction between nuclear and non-nuclear weapons is being blurred. Many of the new conventionally-armed (but potentially nuclear-capable) ballistic missiles now being developed by the major powers are capable of hypersonic speed (more than five times the speed of sound) and of flying more than 500 kilometers (the limit imposed by the now-defunct Intermediate-Range Nuclear Forces Treaty) and are intended for attacks on high-value enemy targets, such as air defense radars and command-and-control facilities. With flight durations of as little as five minutes, defensive early warning and C3 systems have precious little time to determine whether incoming missiles are armed with nuclear or conventional missiles and to select and then carry out an appropriate response, possibly including the early use of nuclear weapons. (See Chapter 3, "An 'Arms Race in Speed.'")

Cybercombat occurs at an even faster speed, potentially depriving nuclear commanders of critical information and communication links in a time of crisis, thereby precipitating unintended or inadvertent escalation. In the highly contested environment envisioned by the 2018 NPR report, decision-makers may be faced with an overload of inconclusive information and have mere minutes in which to grasp the essential reality—and thence to decide on humanity's fate. (See Chapter 4, "Cyber Battles, Nuclear Outcomes?")

Under these circumstances, some analysts insist, increased NC3 automation will prove essential. Increased reliance on AI, these analysts argue, can help with two of the existing system's most acute challenges: information overload and time compression. With ever more sensors (satellite monitors, ground radars, surveillance aircraft) feeding intelligence into battle management systems, commanders are being inundated with information on enemy actions, preventing prompt and considered decision-making. At the same time, the widespread deployment of hypersonic missiles and advanced cyberweaponry is compressing the time in which such decisions must be made. Artificial intelligence could help overcome these challenges, it is claimed, by sifting through the incoming data at lightning speed and identifying any enemy moves requiring an immediate military response.[148]

"AI will make the process of finding and hitting targets of military value faster and more efficient," the National Security Commission on Artificial Intelligence affirmed in its Final Report, speaking both of nuclear and conventional combat. "Currently, this process generally involves passing data in a serial fashion from a sensor, through a series of humans, to a platform that can shoot at the target. AI will help automate some of the intermediate stages of the decision process." As AI matures, moreover, it will propel "more advanced processes that would operate more akin to a web, fusing multiple sensors and platforms to manage complex data flows and transmitting actionable information to human operators and machines across all [combat] domains."[149]

The decision-making system is threatened by the ever-increasing destructive capacity of conventional weapons and the growing sophistication of cyberattacks—and, as a result of those two, the growing speed of combat.

Automation could be even more useful, advocates argue, by helping commanders—up to and including the president—select nuclear and non-nuclear responses to confirmed indications of an enemy attack. With little time to act, human decision-makers could receive a menu of possible countermoves devised by algorithms. "As the complexity of AI systems matures," the Congressional Research Service noted in 2020, "AI algorithms may also be capable of providing commanders with a menu of viable courses of action based on real-time analysis of the battle-space, potentially improving the quality and speed of wartime decision-making."[150]

Some analysts have gone even further, suggesting that in conditions of extreme time compression, the machines could be empowered to select the optimal response and initiate the attack themselves. "Attack-time compression has placed America's senior leadership in a situation where the existing NC3 system may not act rapidly enough," Adam Lowther and Curtis McGiffin wrote in a 2019 commentary for War on the Rocks, a security-oriented website. "Thus, it may be necessary to develop a system based on [AI], 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."[151]

That commentary provoked widespread alarm about the possible loss of human control over decisions of nuclear use. Even some military officials expressed concern over such proposals. "You will find no stronger proponent of integration of AI capabilities writ large into the Department of Defense," said Lt. Gen. Jack Shanahan, then director of the Joint Artificial Intelligence Center (JAIC), at a September 2019 conference at Georgetown University. "But there is one area where I pause, and it has to do with nuclear command and control." Referring to Lowther and McGiffin's assertion in War on the Rocks that an automated U.S. nuclear launch ability is needed, he said, "I read that. And my immediate answer is, 'No. We do not.'"[152]

Shanahan indicated that his organization was moving to integrate AI technologies into a wide array of non-nuclear capabilities, including command-and-control functions. Indeed, JAIC and other military components are moving swiftly to develop automated C2 systems and to ready them for use by regular combat forces. Initially, these systems will be employed by conventional forces, but the Pentagon fully intends to merge them over time with their nuclear counterparts.

All-Domain Command and Control

The Pentagon's principle mechanism for undertaking this vast enterprise is called the Joint All-Domain Command and Control (JADC2) program. As now envisioned, the JADC2 enterprise will incorporate a multitude of computers working together to collect sensor data from myriad platforms, organize the data into digestible bits, and provide commanders with a menu of possible combat options. As explained by the Department of Defense, "JADC2 provides a coherent approach for shaping future Joint Force C2 capabilities and is intended to produce the warfighting capability to sense, make sense, and act at all levels and phases of war, across all domains, and with partners, to deliver information advantage at the speed of relevance."[153]

The JADC2 program is said to be a core element of the Pentagon's emerging strategy for U.S. victory in the fast-paced wars of the future. Called the Joint Warfighting Concept (JWC) or All-Domain Operations, the new strategy assumes seamless coordination among all elements of the U.S. military. General John E. Hyten, former vice chairman of the Joint Chiefs of Staff, explained that the strategy combines "space, cyber, deterrent [i.e., nuclear forces], transportation, electromagnetic spectrum operations, missile defense—all of these global capabilities together … to compete with a global competitor and at all levels of conflict."[154] The JWC strategy was approved by Chairman of the Joint Chiefs of Staff General Mark A. Milley on March 31, 2021, and Secretary of Defense Lloyd J. Austin III gave it his consent shortly thereafter. In consonance with these moves, Austin also approved the initial strategic plan for the JADC2, ensuring that it would receive high-level attention.[155]

Major responsibility for developing the necessary software for the JADC2 enterprise has been delegated to the Air Force through its Advanced Battlefield Management System (ABMS). As described by the Congressional Research Service, "ABMS proposes using cloud environments and new communications methods to allow Air Force and Space Force systems to share data seamlessly using artificial intelligence to enable faster decision-making."[156] To collect data from the ABMS and integrate it into their respective combat systems, the Army established Project Convergence and the Navy initiated Project Overmatch. Both involve extensive tests of ABMS software and assorted air, sea, and ground weapons.[157]

Spending information on JADC2, ABMS, and Projects Convergence and Overmatch is relatively scant, as these programs do not, for the most part, appear in Department of Defense budget documents and many aspects of them are classified. According to the CRS, the Air Force requested $204 million for its ABMS project in FY 2022 while the Army requested $107 million for Project Convergence; the Navy sought additional funds for its Project Overmatch, but these sums were kept secret.[158] The Pentagon's budget request FY 2023 provided no further information on

Lieutenant General Jack Shanahan, director of the Joint Artificial Intelligence Center, appears at a September 2019 conference at Georgetown University. He spoke of the need for improving artificial intelligence in the U.S. military, but cautioned, "there is one area where I pause, and it has to do with nuclear command and control." (Photo: Georgetown University)

ABMS or JADC2 spending, but indicated that ABMS "contributes to the Joint All-Domain Command and Control (JADC2) concept, which will allow current and future platforms/sensors to instantly share critical operational data across the DoD enterprise in the future contested high-end warfighting environment."[159]

In moving forward on all this, the Pentagon's initial emphasis has been on "data fusion," or the compression of multiple sensor inputs into concise summaries that can be rapidly communicated to and understood by commanders in the field. Over time, however, the JADC2 project is expected to incorporate AI-enabled decision-support systems, or algorithms intended to narrow down possible responses to enemy moves and advise those commanders on the optimal choice. As noted by the Congressional Research Service, "JADC2 intends to enable commanders to make better decisions by collecting data from numerous sensors, processing the data using artificial intelligence algorithms to identify targets, then recommending the optimal weapon—both kinetic and nonkinetic (e.g., cyber or electronic weapons)—to engage the target."[160]

Pentagon officials insist that human commanders will always have the final say in decisions regarding the lethal use of force. Read through the statements of top officials, however, and it appears as if humans will play an ever-diminishing role in the future "kill chain." During a September 2020 test of the ABMS system, for example, AI-powered processors interpreted incoming sensor data on enemy threats, selected optimal responses, and directed a tracked howitzer to fire at a mock enemy cruise missile. "That's an example of us demonstrating something that could not be done the human-to-human way," said Will Roper, the project's chief acquisition officer. "Machine-to-machine, it's easy; human-to-human, impossible."[161]

This all matters because the Defense Department has indicated that the JADC2 system, while intended primarily for use by non-nuclear forces, will eventually be integrated with the nuclear command, control, and communications network now being overhauled. In a 2020 interview, General Hyten was asked if the emerging JADC2 architecture was going to inform development of the remodeled NC3. He responded, "Yes. The answer is yes." Hyten, who had also served as commander of the U.S. Strategic Command, added that some NC3 elements will have to be separated from the JADC2 system "because of the unique nature of the nuclear business." Nevertheless, "NC3 will operate in significant elements of JADC2," and, as a result, "NC3 has to inform JADC2 and JADC2 has to inform NC3."[162]

The intertwined nature of JADC2 and nuclear command-and-control was given added emphasis in March 2022 by Hyten's successor as commander of the U.S. Strategic Command, Admiral Chas Richard. "I am very familiar with what JADC2 is doing in conventional command and control. And in fact, was very pleased that a subset of what JADC2 is doing is for nuclear command and control," he told the Senate Armed Services Committee. "The two systems have to be overlapped to a great extent so that we can have integration."[163]

Stripped of jargon and acronyms, what Hyten and Richard are saying is that the automated systems now being assembled for the conventional C2 enterprise will provide a substructure for the nation's nuclear command-and-control system, or be incorporated into the system, or both. It is possible, then, that in some future crisis, data on conventional operations being overseen by the JADC2 system will automatically be fed into NC3 intelligence-gathering systems—possibly altering their assessment of the nuclear threat and leading to a heightened level of alert—along with a greater risk of inadvertent or precipitous nuclear weapons use.

Parallel Developments Elsewhere

While the United States is proceeding with plans to modernize and automate its nuclear command-and-control system, other nuclear-armed nations, especially China and Russia, are also moving in this direction. It is conceivable, then, that a time could come when machines on all sides will dictate the dynamics of a future nuclear crisis and possibly determine the onset and prosecution of a nuclear war.

Russia's pursuit of NC3 automation began during the Soviet era, when senior leaders, fearing a "decapitating" attack on the Soviet leadership as part of a preemptive U.S. first strike, ordered the development of a "dead hand" system intended to launch Soviet missiles even in the absence of instructions to do so from Moscow. If the system, known as Perimeter, were to detect a nuclear explosion on Soviet territory and receive no signals from Moscow—implying a nuclear detonation there—it was programmed to inform nuclear launch officers who, in turn, were authorized to initiate retaliatory strikes without further instruction.[164] According to Russian media accounts, the Perimeter system is still in operation and employs some form of AI.[165]

As in the United States, modernization of the country's NC3 system appears to constitute a high priority for Russia's top officials and, like similar efforts in this country, is thought to involve increased reliance on AI and automation. In 2014, Russia's military inaugurated the National Defense Control Center (NDCC) in Moscow, a centralized command post for assessing global threats and initiating whatever military action is deemed necessary, whether

nuclear or non-nuclear. Like the Pentagon's JADC2 system, the NDCC is designed to collect information on enemy moves from multiple sources and provide senior officers with guidance on possible responses.[166]

The Russians are also reported to be constructing an alternative nuclear command post in a secret underground facility. At a November 2020 meeting in Sochi with top government officials, President Putin spoke of the need to maintain safe, reliable, and fast-acting C3 and NC3 systems. "It is absolutely clear that the combat capability of the nuclear triad and the capability of the army and navy on the whole to adequately and quickly respond to potential military challenges directly depend on the stability, effectiveness, and reliability of these systems under any circumstances," Putin told the gathering. Numerous improvements have been and are continuing to be made in the nation's C3 and NC3 systems, he affirmed, with a particular emphasis on "information support, monitoring, and situation analysis." Suggesting a heavy reliance on computers and AI, he noted that "all command posts can receive comprehensive updates in real-time and use them to assess the situation and make substantiated decisions."[167]

China is also investing in AI-enabled data fusion and decision-support systems, although less is known about its efforts in this area. According a 2019 report by Fiona Cunningham of Stanford University, the PLA Rocket Force (PLARF, previously the PLA Second Artillery Force), which operates China's land-based ICBM arsenal, commenced automation of the country's nuclear command system in the late 1990s and has been upgrading its capabilities ever since. By the early 2000s, Cunningham indicated, the Second Artillery was using an automated command-and-control system for its missile units, one that was supposedly capable of "transmitting commands, fusing intelligence, and monitoring launches in real-time." Cunningham noted, however, that China's capabilities in this regard generally lag behind those of the United States and that modernization of its NC3 systems remains a major state priority.[168]

In the 2021 edition of its annual report on *Military and Security Developments Involving the People's Republic of China*, the U.S. Department of Defense reported that the Chinese leadership has adopted a goal of completing the "intelligentization" of the PLA—or the systemic integration of AI and cloud computing into all military operations—by 2027 at the latest. A key goal of this effort, the Pentagon indicated, will be the modernization of the PLA's nuclear and conventional command-and-control systems. According to the report, "PLA strategists have stated new technologies will increase the speed and tempo of future warfare, and that operationalization of AI will be necessary to improve the speed and quality of information processing by reducing battlefield uncertainty and providing decision making advantage over potential adversaries."[169]

Soldiers of the People's Liberation Army march during a parade to celebrate the 70th Anniversary of the founding of the People's Republic of China in 1949, at Tiananmen Square on October 1, 2019 in Beijing, China. (Photo by Andrea Verdelli/Getty Images)

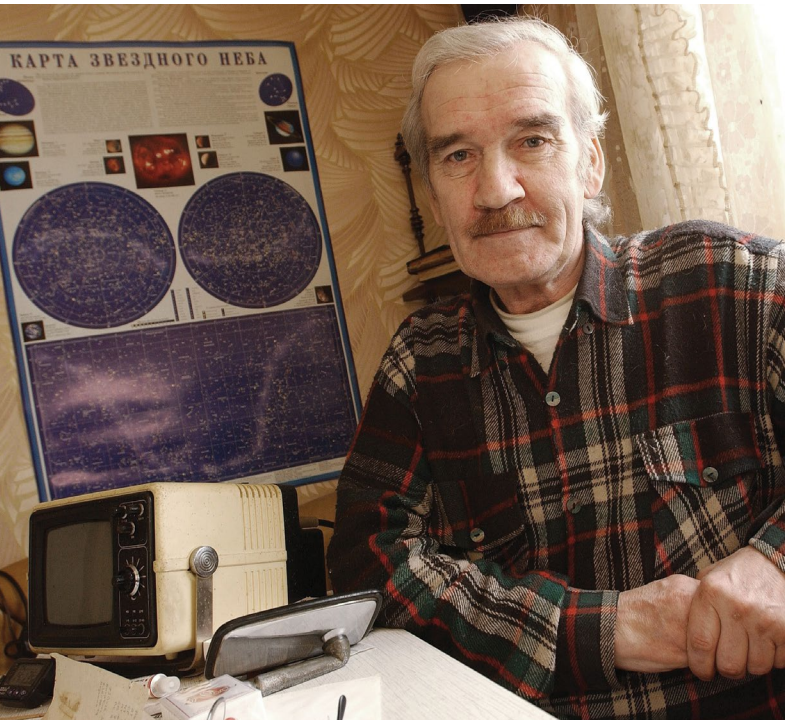
The Perils of Heedless Automation

There are many reasons to be wary of increasing the automation of nuclear command and control, especially when it comes to computer-assisted decision-making. Many of these technologies are still in their infancy and prone to malfunctions that cannot easily be anticipated. Algorithms that have developed through machine learning—a technique whereby computers are fed vast amounts of raw data and are "trained" to detect certain patterns—can become very good at certain tasks, such as facial recognition, but often contain built-in biases conveyed through the training data. These systems also are prone to unexplainable malfunctions and can be fooled, or "spoofed," by skilled professionals. No matter how much is spent on cybersecurity, moreover, NC3 systems will always be vulnerable to hacking by sophisticated adversaries.[170]

AI-enabled systems also lack an ability to assess intent or context. We might ask, for example, whether a sudden enemy troop redeployment indicates an imminent enemy attack or merely the normal rotation of forces? Human analysts can use their sense of the current political moment to help shape their assessment a situation like this, but machines lack that ability, and may assume the worst.

This aspect of human judgment arose in a famous Cold War incident. In September 1983, at a time of heightened tensions between the superpowers, a Soviet nuclear watch officer, Lt. Col. Stanislav Petrov, received an electronic warning of a U.S. missile attack on Soviet territory. Unsure of the accuracy of the warning, he waited before informing his superiors of the strike and eventually told them he believed it was a computer error—as proved to be the case—thus averting a possible nuclear exchange. Machines are not capable of such doubts or hesitations.[171]

Another problem is the lack of real world data for use in training NC3 algorithms. Other than the two atomic bombs dropped on Japan at the end of World War II, there has never been an actual nuclear war and therefore no genuine combat examples for use in devising reality-based attack responses. War games and simulations can be substituted for this purpose, but none of these can accurately predict how leaders will actually behave in a future nuclear showdown. Accordingly, decision-support programs devised by these algorithms can never be fully trusted. "Automated decision-support systems … are only as good as the data they rely on," analysts at the Center for a New American Security (CNAS) wrote in 2019. "Building an automated decision-support tool to provide early warning of a preemptive nuclear attack is an inherently challenging problem because there is zero actual data of what would constitute reliable indicators of an imminent preemptive nuclear attack."[172]



Former Soviet Colonel Stanislav Petrov sits at home in 2004 in Moscow. Petrov helped avert a possible U.S.-Soviet nuclear exchange in 1983, when he doubted the validity of an electronic warning that a U.S. missile attack was underway. (Photo: Scott Peterson/Getty Images)

An equal danger is what analysts call "automation bias," or the tendency for stressed-out decision-makers to trust the information and advice supplied by advanced computers rather than their own considered judgment. For example, an American president, when informed of sensor data indicating an enemy nuclear attack and while under pressure to make an immediate decision, might choose to accept the computer's advice to initiate a retaliatory strike rather than consider possible alternatives, such as with Petrov's courageous decision to pause and investigate further. But with decision-making systems expected to gain ever more analytical capacity over the coming decades, "it is likely that humans making command decisions will treat the AI system's suggestions as on a par with or better than those of human advisers," a 2018 RAND Corporation study noted. "This potentially unjustified trust presents new risks that must be considered."[173]

Compounding all these risks is the likelihood that China, Russia, and the U.S. will all install automated NC3 systems without informing each other of the nature and status of these systems. Under these circumstances, it is possible to imagine a "flash war," roughly akin to a "flash crash" on Wall Street (that is, a stock market crash that is triggered by the interaction of competing corporate investment algorithms). In such a scenario, warns Paul Scharre of CNAS, the data assessment systems of each country could misinterpret signs of adversary moves and conclude that an attack is imminent, leading other computers to order preparatory moves for a retaliatory strike, thereby prompting similar moves on the other side and triggering an escalatory cycle ending in nuclear catastrophe.[174]

Limiting the Dangers

Given these multiple risks, U.S. policymakers and their Chinese and Russian counterparts should be very leery of accelerating NC3 automation. Indeed, General Shanahan acknowledged as much, noting in 2019 that nuclear weapons use "is the ultimate human decision that needs to be made" and warning that "we have to be very careful" when automating NC3, especially given "the immaturity of technology today."[175]

This cautionary outlook also appears to have informed the National Security Commission on Artificial Intelligence when submitting its final report in 2021. "While the Commission believes that properly designed, tested, and utilized AI-enabled and autonomous weapon systems will bring substantial military and even humanitarian benefit,"

it avowed, "the unchecked global use of such systems potentially risks unintended conflict escalation and crisis instability." Acknowledging the immaturity of the technology and its potential for malfunction, the report went on to say, "Unintended escalations may occur for numerous reasons, including when systems fail to perform as intended, because of challenging and untested complexities of interaction between AI-enabled and autonomous weapon systems on the battlefield, and, more generally, as the result of machines or humans misperceiving signals or actions."[176]

To reduce these risks, the Commission recommended several precautionary steps. First, it called on U.S. leaders to "make a clear, public statement that decisions to authorize nuclear weapons employment must only be made by humans, not by an AI-enabled or autonomous system." This would, it claimed, demonstrate a U.S. commitment to the responsible use of AI and enable American leaders to seek similar commitments from the leaders of Russia and China. Recognizing that formal treaties or agreements to limit the deployment of AI-enabled NC3 systems are unlikely to be negotiated in the short-term, it recommended that U.S. and Russian leaders discuss the escalatory dangers of excessive reliance on automated NC3 systems as part of their ongoing Strategic Stability Dialogue, as well as the initiation of a similar dialogue with China.

As these discussions proceed, the Commission noted, participants could agree "to integrate 'automated escalation tripwires' into systems that would prevent the automated escalation of conflict in specific scenarios without human intervention," especially in scenarios that might result in nuclear weapons employment. Lastly, in the hope that such talks will lead, in time, to the negotiation of formal measures to reduce such risks, the report recommended intensive research on tools and strategies for the verification of future agreements.[177]

Aside from the NSCAI's commissioners, the dangers unleashed by excessive reliance on automated nuclear command systems has been addressed by a number of other analysts. Referring to the stock market "flash crash" of May 6, 2010, when the Dow Jones Index lost ten percent of its value in a matter of minutes, Paul Scharre noted that stock markets around the world have since inserted "circuit breakers" into securities trading, automatically halting trading when prices shift rapidly by more than a certain percent. The same, he said, must be done in the case of automated military systems, to ensure that machines do not initiate extreme measures—such as the use of nuclear weapons—without obtaining authenticated human approval.[178]

Given all the uncertainties involved in the automation of nuclear command systems and the catastrophic consequences of miscalculation, it is imperative that the major powers take unilateral steps to ensure that humans exercise ultimate control over nuclear-launch systems and, in dialogues of the sort proposed by the NSCAI, consider common measures to prevent unintended escalation.

Chapter 6:

A Framework Strategy for Reducing the Escalatory Dangers of Emerging Technologies

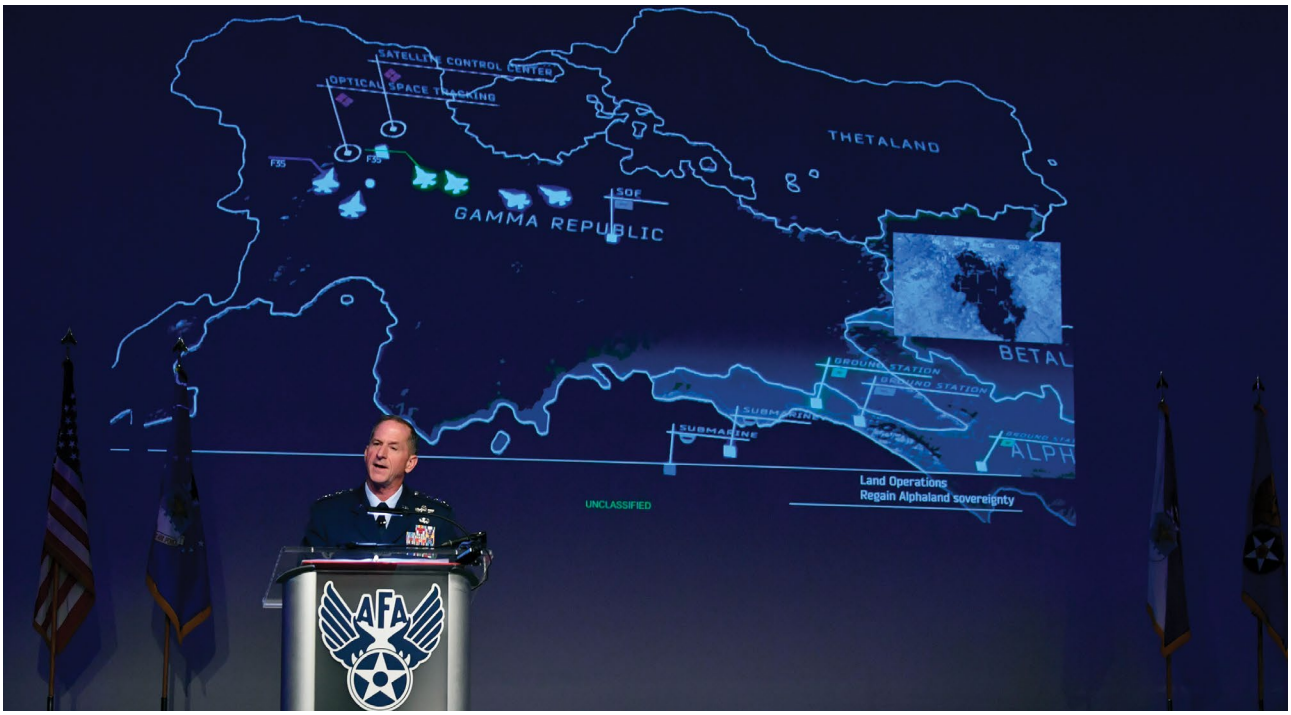
As has been demonstrated in the preceding five chapters, the introduction of new weapons systems employing artificial intelligence and other emerging technologies is dramatically altering the nature of warfare and posing significant risks to strategic stability. The growing utilization of AI-enabled autonomous weapons, we learned, threatens to diminish human control over battlefield dynamics and increase the risk of accidental or inadvertent escalation; the imminent deployment of hypersonic missiles will accelerate the pace of combat, reducing the potential for prudent and well-informed crisis management. Strategic stability is also imperiled, as we have seen, by the development of offensive cyberweapons and a growing reliance on automated battlefield decision-making.

These developments are troubling enough. But the drive to develop and deploy weapons systems employing these technologies is also proceeding at a much faster pace than efforts to assess the dangers they pose and to establish limits on their use. Military leaders of the major military powers, especially those in China, Russia, and the U.S., are keen to exploit the perceived benefits of these technologies as rapidly as possible, so as to obtain a combat advantage in any wars that might erupt between them. In many cases, these efforts have acquired an arms-racing character, as officials in one country point to supposed progress in another to justify their own accelerated utilization of the new technologies.

Although many world leaders have warned of the dangers posed by the weaponization of emerging technologies and called for the adoption of international restraints on such efforts, little progress has been made to accomplish this. "Machines with the power and discretion to take lives without human involvement are politically unacceptable, morally repugnant and should be prohibited by international law," UN Secretary-General António Guterres told a group of governmental experts considering such restraints in March 2019.[179] But the group, assembled under the auspices of the Convention on Certain Conventional Weapons (CCW), was unable to agree on such a prohibition, and the development and deployment of autonomous combat systems have continued apace.

Efforts to control weapons employing other disruptive technologies, such as cyber and hypersonics, have also witnessed little progress. Before the outbreak of fighting in Ukraine, officials from Russia and the U.S. had announced plans to assess the disruptive impact of these technologies as part of the Strategic Stability Dialogue they had undertaken. At the second such meeting, held in Geneva on Sept. 30, 2021, the two sides agreed to establish a "Working Group on Capabilities and Actions With Strategic Effects," which, presumably, would consider the threats to strategic stability posed by emerging and disruptive technologies.[180] However, President Biden suspended these talks after Russia invaded Ukraine on Feb. 24, 2022; both sides have since indicated a willingness to resume the dialogue, but no plans had been made to do so as of February 2023.

The war in Ukraine has further complicated efforts to control the military utilization of emerging technologies by encouraging the belligerents to employ whatever weapons are viewed as providing a battlefield advantage. Both sides, for example, made widespread use of reconnaissance drones to locate enemy positions for attack by planes and artillery, and in some cases have employed armed drones, such as the Turkish Bayraktar TB2 (used by the Ukrainians) and the Iranian Shahed-136 (used by the Russians), to directly engage enemy targets. The Russians also fired Kinzhal hypersonic missiles at logistical facilities in western Ukraine, and are believed to have conducted multiple cyberattacks on Ukrainian government and military networks. All this will no doubt increase



U.S. Air Force Chief of Staff Gen. David Goldfein speaks to the Air Force Association's Air, Space and Cyber Conference in September 2019. As great-power competition in cyberwarfare pushes the technology forward, there are risks that potential escalatory consequences are being ignored. (Photo: Wayne Clark/U.S. Air Force)

the likelihood of other belligerents employing these technologies in future conflicts while complicating the task of adopting international constraints on their use.

Despite these impediments to progress in this field, it is essential to consider possible strategies for regulating the military utilization of emerging and disruptive technologies. At this point, their application to combat has been relatively limited, so the potential battlefield impact of these technologies has not been fully demonstrated. As they become more widely deployed, however, the threats they pose to human control of escalation dynamics and strategic stability will become ever more acute. This is the ideal moment, then, to devise and begin to implement measures designed to curtail this dangerous process.

The Eroding Nuclear "Firebreak"

In constructing such measures, it is essential to remind ourselves of the geopolitical and military contexts in which emerging technologies are being exploited for combat use. After years in which international terrorism was widely viewed as the greatest threat to international peace and stability, the major nuclear powers now perceive themselves to be engaged in a competitive struggle for geopolitical advantage, with every possibility that this struggle could result in war between them. Under these circumstances, all three countries are enhancing their capacity for what the Pentagon calls "high end" warfare, or all-out combat against the modern, well-equipped forces of their adversaries—combat that is expected to employ every advance in military technology.

"We cannot expect success fighting tomorrow's conflicts with yesterday's thinking, weapons, or equipment," former Secretary of Defense Jim Mattis told the Senate Armed Services Committee in April 2018, when describing this new outlook. To prevail in future wars, "[we must invest] in technological innovation to increase lethality, including research into advanced autonomous systems, artificial intelligence, and hypersonics."[181]

A very similar outlook regarding the strategic environment is embedded in Chinese and Russian military doctrine. In language strikingly similar to that of the Pentagon's new strategy, but in mirror image, China's July 2019 white paper on national defense warned of increasing U.S. investment in advanced military capabilities and indicated that if Chinese forces are to prevail in any future U.S.-China conflict, "greater efforts have to be invested in military modernization."[182] Russian doctrine places equal emphasis on the utilization of emerging technologies to ensure success on the battlefield.[183]

The military doctrine of all three countries emphasizes the acquisition of advanced conventional weapons—tanks, missiles, planes, and bombs—designed for fast-paced, firepower-intensive

offensives at the very onset of battle. At the same time, all three are engaged in costly upgrades to their nuclear delivery systems, in most cases involving the replacement of older ICBMs, bombers, and missile-carrying nuclear submarines with newer, more capable versions. More worrisome still, all three are developing "low-yield" warheads for use in so-called "nonstrategic" scenarios, for example, to defeat an overpowering conventional assault by an adversary.

The acquisition of new nuclear munitions for use in such scenarios was an explicit goal of the Nuclear Posture Review adopted by the Trump administration in February 2018, and is believed to figure in Russian military doctrine.[184] Indeed, Russian President Vladimir Putin implicitly threatened to conduct such strikes in the event that Russian-claimed regions in Ukraine came under attack by Western-armed Ukrainian forces.[185] China is less transparent about its nuclear weapons policies, but is known to have developed nuclear warheads for its medium- and intermediate-range ballistic missiles intended for use against U.S. and allied forces in the Asia-Pacific region.[186]

These developments are occurring, moreover, at a time when many of the barriers to the nuclear weapons use erected during the Cold War era have been abandoned, such as the Intermediate-Range Nuclear Forces (INF) Treaty of 1987, or are at risk of being terminated, as is true of the New Strategic Arms Reduction Treaty (New START), which expires in 2026. Those barriers were largely intended to prevent a conventional war from escalating across the "firebreak" separating non-nuclear from nuclear combat; the wider the firebreak, it was assumed, the lesser the risk that a conventional conflict involving the major powers would trigger the use of atomic weapons. As those barriers disappear, the firebreak is shrinking and the risk of escalation is growing.

In today's fiercely competitive strategic environment, moreover, analysts fear that the firebreak is being further eroded by the introduction of increasingly capable non-nuclear weapons, including systems employing emerging technologies of the sort described in earlier chapters.[187] While none of the major powers is likely to initiate a nuclear exchange with one of its principal adversaries—knowing the resulting destruction to its own homeland would be catastrophic—all have adopted military doctrines that emphasize non-nuclear attacks on their adversary's critical military assets (radars, missile batteries, command centers, and so on) at the very onset of a conflict. In most cases, these assets are intended primarily for conventional operations, but some may also house nuclear-related facilities, a situation described by James Acton of CEIP as "entanglement." If these dual-use or co-located facilities came under assault, the target state might conclude that such strikes constituted the prelude to a nuclear attack, and so decide to launch its own nuclear munitions before they could be destroyed by its adversary's incoming weapons.[188]

The military policies and doctrines of the major powers are combining with advances in certain disruptive technologies to erode the nuclear firebreak and undermine strategic stability.

For example, a potential belligerent might choose to deploy its AI-enabled air and naval autonomous weapons in self-directed "swarms" to find and destroy key enemy assets, including its command, control, communications, and intelligence (C3I) facilities. To an adversary, such attacks could be interpreted as the prelude to a nuclear first strike, prompting it to launch its nuclear weapons before they can be destroyed by incoming weapons. The launch of multiple hypersonic missiles early in a conflict to destroy key enemy assets like those described above might also cause the target state to fear that a nuclear strike is imminent, again causing the premature launch of its nuclear weapons. A cyberattack on an enemy's C31 systems, especially those with nuclear command-and-control functions, could produce a similar outcome.

In response to these dangers, the major powers are coming to rely ever more heavily on AI-enabled machines to filter sensor data on enemy movements, decipher their intentions, and select optimal battlefield responses. This increases the danger that humans will cede key combat decision-making tasks to machines that lack a capacity to gauge political and diplomatic contexts in their calculations and are vulnerable to hacking, spoofing, and other failures, possibly leading them to initiate extreme military responses to ambiguous signals and thereby cause inadvertent nuclear escalation.

Enhancing Strategic Stability

Clearly, the military policies and doctrines of the major powers are combining with advances in certain disruptive technologies to erode the nuclear firebreak and undermine strategic stability. Accordingly, efforts

to regulate these technologies should prioritize measures intended to buttress stability and widen the firebreak. Given the variety and complexity of the technologies involved, no single overarching treaty or agreement is likely to achieve this goal. Rather, what is needed is a *framework* strategy, aimed at advancing an array of measures which, however specific their intended outcome, all contribute to the larger goal of enhanced stability.

As noted earlier, the greatest dangers to be overcome are those with the potential to spark an accidental or unintended escalatory spiral. Accordingly, when devising measures to enhance strategic stability, the goal should be to reduce the likelihood of such spirals by eliminating certain types of weapons or enabling systems, or imposing limitations on their numbers and use. Buffers and other escalation-prevention measures can also be adopted, such as the "dis-entanglement" of nuclear and non-nuclear C3I systems. And even when the international environment precludes formal agreements along these lines, states can engage in unilateral actions or join with others in undertaking confidence-building measures aimed at developing a common understanding of the risks posed by the new technologies.

Recognizing the difficulty of achieving major breakthroughs in the current international environment—yet determined to achieve progress to the greatest degree possible—we propose the following constituent elements of a framework strategy to restrain and regulate the utilization of emerging technologies for military use. These initiatives are derived from the toolbox developed by arms control advocates over many years of practice and experimentation, as well as the contributions of other experts in the field.[189]

In many cases, the measures described below are already being applied to particular weapons systems, in ways described in the earlier chapters of this primer. Our intent here, however, is to bring them together in a more coordinated fashion, with the overarching goal of reducing the risk to strategic stability. In light of the current political atmosphere, we begin with more achievable initiatives and proceed step-by-step to more sweeping, legally-binding measures requiring political accommodation.

Awareness-Building: Before significant progress can be made in adopting formal measures to regulate the weaponization of emerging technologies, greater effort will be needed to educate policymakers and the general public about the risks posed by the unregulated use of these technologies. While advocates of applying the new technologies for military use have been vociferous in extoling the advantages of doing so, there has been far less effort to address the dangers posed by such weaponization.

A Russian MiG-31 aircraft carries a Kinzhal hypersonic over Moscow's Victory Day parade in 2018. High-speed weapons like this, capable of carrying conventional or nuclear warheads, risk escalating conflicts as decision makers have little time to assess an ambiguous threat. (Photo: Kremlin.ru)

A critical first step, therefore, must be to identify these dangers and make their presence more widely known to government officials and the general public.

In the field of autonomous weapons systems, valuable work of this nature has been performed by the Campaign to Stop Killer Robots ("the Campaign") and its affiliated groups, including Human Rights Watch and the International Committee for Robot Arms Control. The Campaign has focused in particular on the threats to international humanitarian law posed by the deployment of autonomous weapons, employing a combination of public protest and skillful lobbying to raise awareness of these dangers within the diplomatic community. Although it has not been successful in its drive to persuade signatory states of the CCW to adopt a legally binding prohibition on autonomous weapons—largely due to Russian and U.S. opposition—the Campaign has helped forge a coalition of states prepared to consider adoption of a treaty to this effect at the UN General Assembly.[190]

Valuable as these efforts have been, they have addressed only one aspect of the larger problem, the threat to civilians arising from the deployment of autonomous weapons in chaotic situations where such devices—once unleashed from human control—may prove unable to distinguish between combatants and non-combatants. A more comprehensive approach, encompassing the full range of emerging and disruptive weapons, has been adopted by the German Foreign Ministry in organizing a series of conferences on "Capturing Technology, Rethinking Arms Control." Each of these events, held in 2019, 2020, and 2021, assessed the dangers posed by a full range of emerging technologies—including AI, autonomy, cyber, and hypersonics—and considered various approaches to their control.

The German effort, spearheaded by former German Foreign Minister Heiko Maas, has contributed to a growing awareness of these dangers among members of the European Union. At the conclusion of the 2020 conference, the foreign ministers of the Czech Republic, Finland, Germany, the Netherlands, and Sweden issued a joint proclamation expressing their concern over the "mounting risks for international peace and stability created by the potential misuse of new technologies."[191] More such gatherings, involving a wider spectrum of nations, would help increase awareness of these dangers. In the United States, Congress should be encouraged to hold hearings on the destabilizing impacts of certain emerging technologies.

Track 2 and Track 1.5 Diplomacy: At present, government officials from China, Russia, and the United States are barely speaking to one another about strategic nuclear matters, let alone about the dangers posed by the weaponization of emerging technologies. In the absence of such official discourse, it is imperative that scientists, engineers, and arms control experts from these countries meet in neutral settings to assess the additive risks to strategic stability posed by the weaponization of these technologies and to devise practical measures for their regulation and control. Building on the experience of the Pugwash Conferences on Science and World Affairs in assembling experts from many nations, such meetings—often described as "Track 2" diplomacy (as distinct from official discussions, or "Track 1")—could evaluate measures for curtailing or regulating the application of disruptive technologies to military use.

It should be possible, for example, for prominent experts from China, Russia, the U.S., and other interested countries, to meet on an informal basis to discuss possible limits on the deployment of hypersonic missiles or on methods for reducing cyber threats to nuclear command-and-control systems. In fact, Pugwash convened such a session on hypersonic weapons, in Geneva in December 2019. This meeting reportedly brought together several dozen participants from different countries, including scientists, academics, and experts from the NGO and think-tank communities. According to Pugwash, "participants discussed technical aspects, factors driving the development, roles and purposes of hypersonic weapons, as well as risks associated with their deployment and use."[192] The organization has also sponsored several such workshops on "cyber security and warfare," the most recent held in January 2020.[193]

This model can be employed by other organizations to convene similar encounters between experts from the major powers to assess mutual dangers and consider various control options. Ideally, these Track 2, or nongovernmental consultations, can be followed by "Track 1.5" engagements, in which former government officials and others with government ties also participate, helping to ensure that any proposals developed at such gatherings will be given consideration at higher levels.

Unilateral and Joint Initiatives: Given the current state of international affairs, it will prove difficult for the U.S. and Russia or the U.S. and China—or all three meeting together—to agree on formal measures for the control of especially destabilizing technologies. It should, however, be possible for these states to adopt unilateral measures in the hope that they will induce parallel steps by their adversaries and eventually lead to binding bilateral and multilateral agreements.

Noting that the rapid and unregulated utilization of artificial intelligence for military purposes could lead to violations of international humanitarian

law (IHL) and other unintended consequences, the National Security Commission on Artificial Intelligence affirmed in 2021 that countries should take unilateral steps aimed at "reducing risks associated with AI-enabled and autonomous weapons systems and encourage safety and compliance with IHL." Such efforts, it added, "should and must be led by the United States." Among such initiatives, the Commission called for the adoption of ethical guidelines on AI's coupled with strict protocols governing the design, development, testing, and deployment of AI-enabled weapons.[194]

Independently of the NSCAI, the Department of Defense has been developing its own guidelines for regulating the military use of artificial intelligence. This process commenced in February 2020, with the adoption of six "ethical principles" for the use of artificial intelligence by the department. In addition to measures aimed at ensuring the safe and reliable use of AI-enabled systems, the DoD guidelines require that such systems "fulfill their intended functions while possessing the ability to detect and avoid unintended consequences."[195]

Although welcomed by many in the scientific and technical community, the DoD's "ethical principles" did not incorporate procedures for their department-wide implementation, prompting calls for the promulgation of such measures. The Pentagon finally addressed this need in June 2022 with the release of its "Responsible Artificial Intelligence Strategy and Implementation Pathway" report. This document, however, merely reiterated the principles incorporated into the original guidelines and attached a blueprint for further action by DoD agencies.[196] Clearly, then, far more work remains to be done in this area.

Proposals have also been made for the adoption of unilateral measures in the cyberspace realm, aimed at preventing inadvertent attacks on a potential adversary's nuclear C3I systems and protecting one's own systems from such attack. For example, James Acton has called on governments to adopt a "risk-averse" cyber policy, under which they insert barriers against unintended attacks of this sort.[197] Acton has also advocated the unilateral "disentanglement" of nuclear and nonnuclear C3 systems, to reduce the risk that an attack on the latter will be construed as an attack on the former, and so trigger an unintended nuclear exchange.

Similar measures can be devised to reduce the risks posed by other disruptive technologies. For example, states possessing hypersonic missiles could introduce some means to signal to potential adversaries that their weapons—even if capable of carrying nuclear warheads—are loaded solely with conventional ones, thus reducing the risk of "warhead ambiguity" and the premature launch of nuclear weapons.[198]

In addition to unilateral measures of these sorts, various groups of states could agree on joint measures to reduce escalatory risks. These might include, for example, the adoption of common codes of conduct and transparency requirements. Measures of these sorts aimed at autonomous weapons were advocated by 70 nations, including the United States, in a statement delivered to the UN General Assembly on October 21, 2022. Warning of the dangers posed by the unregulated deployment of autonomous weapons systems, the statement called on the international community to "address these risks and challenges by adopting appropriate rules and measures, such as principles, good practices, limitations and constraints."[199]

Strategic Stability Talks: Before governments can undertake the arduous process of negotiating formal arrangements to curb the weaponization of emerging technologies, senior officials must become more familiar with the nature of these technologies and the significant risks they pose; even more essential, officials on all sides must come to understand how their adversaries view these risks. The best way to do this, many experts agree, is to convene a series of "strategic stability talks," composed of government officials, military officers, and technical experts from opposing sides, who can build on the work begun under Tracks 2 and 1.5 diplomacy by identifying the risks posed by destabilizing technologies and devising methods for minimizing them.

Some preliminary efforts of this sort have occurred under the auspices of the Strategic Stability Dialogue (SSD) conducted by U.S. and Russian officials in recent years, albeit without achieving any concrete results.[200] As noted earlier, the two sides agreed in September 2021 to establish a "Working Group on Capabilities and Actions With Strategic Effects," though this group has yet to meet—following the Russian invasion of Ukraine in February 2022, the Biden administration understandably paused the dialogue. However, at the appropriate time, the two sides should resume these talks to hammer out a new arms control agreement to follow the New START Treaty, which expires in 2026, as well as to launch a serious conversation on strategies for minimizing the risks posed by the weaponization of emerging technologies.

It is equally important that experts and officials of the U.S. and China, or the U.S., China, and Russia, commence a similar dialogue. Although both Beijing and Washington have warned of the dangers posed by each other's utilization of advanced technologies for military use, especially cyber, autonomy, and hypersonics, they have never agreed to discussions on mitigating these threats. Highlighting this lack of communication and warning of the risks involved,

the NSCAI recommended in its Final Report that Washington work to establish a "U.S.-China SSD that includes the relevant military, diplomatic, and security officials from both sides."[201]

Once talks of this sort commence, whether between the U.S. and Russia or the U.S. and China, the two parties could undertake confidence-building measures intended to build trust and develop a common understanding of the problems involved. These could range from something as simple as devising a common dictionary of terms to low-level tests of possible verification measures. Such efforts will prove especially important in the area of emerging and disruptive technologies, as these involve complex technical matters that can be difficult for experts, let alone policymakers to grasp. Overcoming these impediments, and constructing a common understanding of the problem, will be essential for any forward progress in this area.[202]

Bilateral and Multilateral Arrangements: Once the leaders of the major powers come to appreciate the escalatory risks posed by the weaponization of emerging technologies, it may be possible for them to reach accord on bilateral and multilateral arrangements intended to minimize these risks. Such accords could begin with nonbinding agreements of various sorts and, as trust grows, be followed by binding treaties and arrangements.

As an example of a useful first step, the leaders of the major nuclear powers could jointly pledge to eschew cyberattacks against each other's nuclear C3I systems. This need not take the form of a binding treaty, but could be incorporated into a joint statement by leaders of the countries involved. While such an agreement "would not be verifiable in the traditional sense," Acton suggests, it would be "enforceable" in that each state would possess the ability to detect and retaliate against such an intrusion.[203]

Similarly, some members the Group of Governmental Experts established under the auspices of the CCW have proposed that states commit to a code of conduct governing the military use of artificial intelligence, incorporating many of the principles contained in the Defense Department's roster of ethical principles for AI use. In particular, such a code would require that humans retain ultimate control over all instruments of war, including autonomous weapons systems and computer-assisted combat decision-support devices. It might also incorporate requirements for the rigorous testing of AI-enabled systems to reduce the risk of accidental or unintended outcomes.[204]

If the major powers are prepared to discuss binding restrictions on the military use of destabilizing technologies, certain priorities take precedence. The first would be an agreement or agreements prohibiting attacks on the nuclear C3I systems of another state by cyberspace means or via missile strikes, especially hypersonic strikes. Another top priority would be measures aimed at preventing swarm attacks by autonomous weapons on another state's missile submarines, mobile ICBMs, and other second-strike retaliatory systems. Strict limitations should be imposed on the use of automated decision-support systems with the capacity to inform or initiate major battlefield decisions, including a requirement that humans exercise ultimate control over such devices.

Without the adoption of measures such as these, cutting-edge technologies will be converted into military systems at an ever-increasing tempo, and the dangers to world security will grow apace. A more thorough understanding of the distinctive threats to strategic stability posed by these technologies and the imposition of restraints on their military use would go a long way toward reducing the risks of Armageddon.

GLOSSARY OF TERMS

Arms control: Arms control is a form of mutual agreement(s) or commitment(s) through which states might reduce nuclear risks. The benefits of arms control include avoiding an action-reaction arms race; reducing incentives to preemptively strike adversary military forces, including nuclear forces; lowering the chances of inadvertent escalation; and saving money.

Artificial intelligence (AI): Artificial intelligence can be understood as "computerized systems that work and react in ways commonly thought to require intelligence, such as solving complex problems in real-world situations," according to the Congressional Research Service. AI is an enabling technology that can be highly tailored to specific applications or tasks.

Asymmetric arms control: Agreement(s) or commitment(s) in which states make non-like-for-like exchanges.

Counterspace capabilities: Outer space is a domain (similar to air, land, and sea) that is now generally considered a warfighting domain, including by the North Atlantic Treaty Organization and the U.S. Department of Defense. Counterspace capabilities can be understood to refer to systems that can disrupt operations or have a destructive effect in outer space. These include: kinetic physical (e.g. direct ascent anti-satellite [ASAT] systems), non-kinetic physical (e.g. lasers), electronic (e.g. jamming or spoofing), and cyber capabilities.

Destination ambiguity: Destination ambiguity occurs when a state could mistakenly believe that an incoming weapon is heading for its territory.

Drones: Drones are known as unmanned underwater vehicles (UUVs), unmanned aircraft systems (UAS), unmanned aerial vehicles (UAVs), remotely piloted aircraft (RPA). A drone is a vehicle that does not have a pilot, crew, or passengers on board, and the vehicle's systems are usually controlled from a ground station or are given a pre-programmed mission. There are two broad categories: drones for surveillance and reconnaissance missions and drones for combat missions (to include providing close air support to troops on the ground and conducting strikes on specific targets). Drones can also be thought of as a visual application of artificial intelligence.

Hypersonic missile: A hypersonic missile travels at least five times the speed of sound (Mach 5). Generally, hypersonic missiles fly at lower altitudes than intercontinental ballistic missiles (ICBMs) and at greater altitudes than traditional cruise missiles and are largely intended for regional rather than intercontinental use.

Hypersonic cruise missile (HCM): HCMs are powered by high-speed engines, called scramjets, during flight and are intended to fly at both greater speed and greater altitudes than traditional cruise missiles.

Hypersonic glide vehicle (HGV): HGVs are launched by a rocket before gliding to a target, fly at lower altitudes than ballistic missiles, and feature significant maneuverability

Lethal autonomous weapons (LAWs): LAWs are weapons systems that can, once activated, independently select and engage targets without the need for further manual human intervention. These weapons can be thought of as an application of artificial intelligence, in that LAWs can be enabled to assess the situational context on a battlefield and determine the counterattack according to the processed information.

Offensive cyber operations: Cyberspace is a global domain within the information environment that can encompass the internet, telecommunications networks, computer systems, and embedded processors and controllers. Military offensive operations in cyberspace are intended to project power by the application of force in and through this domain and can create effects that are intended to support operations across the physical domains and cyberspace. Defensive cyber operations, in contrast, are activities meant to defend cyberspace.

Strategic stability: Strategic stability is the convergence of arms race stability and crisis stability.

Arms race stability: Arms race stability is defined as a condition in which two adversaries do not have an incentive to build up their strategic nuclear forces.

Crisis stability: Crisis stability is defined as a condition in which nuclear powers are deterred from launching a nuclear first strike against one another.

Target ambiguity: Target ambiguity occurs when a state could mistakenly believe that its nuclear forces were under attack when its conventional forces were really the target. This situation could occur in particular if a state's nuclear and conventional assets were "entangled" due to dual-use command-and-control systems.

Warhead ambiguity: Warhead ambiguity occurs when a state could mistakenly believe that a conventional

ENDNOTES

1. National Security Commission on Artificial Security (NSCAI), *Final Report*, 2021, p. 22, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.
2. As quoted in Caitlin M. Kenney, "The Next War's 'Butcher's Bill' Will Match WWII's—Unless the US Adapts, Milley Says," Defense One, July 15, 2021, https://www.defenseone.com/threats/2021/07/next-wars-butchers-bill-will-match-wwiisunless-us-adapts-milley-says/183804/.
3. U.S. Department of Defense (DoD), *Defense Budget Overview: DoD Fiscal Year 2023 Budget Request*, April 2022, pp. 2–4, 2–5, 2–10, 4–6, 4–7, https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2023/FY2023_Budget_Request_Overview_Book.pdf.
4. Eric Schmidt, "AI, Great Power Competition & National Security," *Daedalus*, vol. 151, no. 2 (Spring 2022), p. 293.
5. DoD, "Remarks at the Shangri-La Dialogue by Secretary of Defense Lloyd J. Austin III (As Delivered)," June 11, 2022, https://www.defense.gov/News/Speeches/Speech/Article/3059852/remarks-at-the-shangri-la-dialogue-by-secretary-of-defense-lloyd-j-austin-iii-a/.
6. Congressional Research Service (CRS), "Defense Primer: Emerging Technologies," updated December 21, 2021, p. 1, https://crsreports.congress.gov/product/pdf/IF/IF11105.
7. NSCAI, *Final Report*, p. 78.
8. Christopher F. Chyba, "New Technologies & Strategic Stability," Daedalus, vol. 149, no. 2 (Spring 2020), pp. 150–70.
9. Ibid, pp. 150–70. See also Vincent Boulanin, et al, *Artificial Intelligence, Strategic Stability, and Nuclear Risk* (Stockholm: Stockholm International Peace Research Institute, 2020).
10. German Federal Foreign Office, *Capturing Technology, Rethinking Arms Control: Conference Reader*, November 5–6, 2020, p. 4.
11. Schmidt, "AI, Great Power Competition & National Security," p. 294.
12. Public Law 115-232, John S. McCain National Defense Authorization Act for Fiscal Year 2019, Title II, Section 238. For more on AI definitions, see CRS, *Artificial Intelligence and National Security*, Report R45178, updated November 10, 2020, pp. 1–4, https://crsreports.congress.gov/product/pdf/R/R45178/10.
13. CRS, *Artificial Intelligence and National Security*, p. 2.
14. NSCAI, *Final Report*, p. 22.
15. DoD, DoD Fiscal Year 2023 Budget Request, p. 4-7.
16. For background, see CRS, A*rtificial Intelligence and National Security*, pp. 30–34.
17. DoD, Department of Defense Directive no. 3000.09, "Autonomy in Weapon Systems," November 21, 2012, http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf.
18. For extensive background on such systems, see Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (New York: W.W. Norton, 2018).
19. For background, see CRS, *Lethal Autonomous Weapons Systems: Issues for Congress*, Report R44466, April 14, 2016, https://crsreports.congress.gov/product/pdf/R/R44466/4.
20. For a thorough explication of this position, see Human Rights Watch (HRW) and International Human Rights Clinic, *Making the Case: The Dangers of Killer Robots and the Need for a Preemptive Ban*, December 2016, https://www.hrw.org/sites/default/files/report_pdf/arms1216_web.pdf.
21.Definition adopted from Shannon Bugos and Kingston Rief, *Understanding Hypersonic Weapons: Managing the Allure And the Risks, Arms Control Association*, Washington, D.C., 2021, p. 2, https://www.armscontrol.org/sites/default/files/files/Reports/ACA_Report_HypersonicWeapons_2021.pdf
22. See CRS, *Hypersonic Weapons: Background and Issues for Congress*, Report R45811, updated Dec. 13, 2022, pp. 2-4, https://sgp.fas.org/crs/weapons/R45811.pdf
23. See Bugos and Rief, *Understanding Hypersonic Weapons*, pp. 4–7.
24. Ibid, pp. 8–14.
25. Holly Ellyatt, "Russia says it fired hypersonic missiles in Ukraine," CNBC, March 22, 2022, https://www.cnbc.com/2022/03/22/hypersonic-missiles-why-would-russia-use-the-kinzhal-in-ukraine.html
26. *CRS, Hypersonic Weapons*, pp. 16–19.
27. Ibid, pp. 4–14. See also Bugos and Rief, Understanding Hypersonic Weapons, pp. 8–11.
28. UN Office of Disarmament Affairs, *Hypersonic Weapons: A Challenge and Opportunity for Strategic Arms Control*, February 2019, https://www.un.org/disarmament/publications/more/hypersonic-weapons-a-challengeand-opportunity-for-strategic-arms-control/.
29. As cited in Theresa Hitchens, "ARRW to Mayhem to the Future of Hypersonic Operations," Breaking Defense, August 31, 2020, https://breakingdefense.com/2020/08/arrw-to-mayhem-to-the-future-of-hypersonic-operations/.
30. As cited in Kingston Reif and Shannon Bugos, "Pentagon Tests Hypersonic Glide Body," *Arms Control Today*, April 2020, https://www.armscontrol. org/act/2020-04/news/pentagon-tests-hypersonic-glide-body.
31. See David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown, 2018).
32. Ibid, pp. 100–23.
33. See Kate Conger, "Ukraine Says It Thwarted a Sophisticated Russian Cyberattack on Its Power Grid," *The New York Times*, April 12, 2022, https://www.nytimes.com/2022/04/12/us/politics/ukraine-russian-cyberattack.html.
34. For background, see Herbert Lin, *Cyber Threats and Nuclear Weapons* (Stanford: Stanford University Press, 2021), pp. 32–34, 44–79.
35. For discussion, see Andrew Futter, "The Dangers of Using Cyberattacks to Counter Nuclear Threats," *Arms Control Today*, July/August 2016, https://www.armscontrol.org/act/2016-07/features/dangers-using-cyberattacks-counter-nuclear-threats.
36. See James M. Acton, "Cyber Warfare & Inadvertent Escalation," *Daedalus*, vol. 149, no. 2 (Spring 2020), pp. 141–46.
37. NSCAI, *Final Report*, p. 98.
38. Action, "Cyber Warfare & Inadvertent Escalation," pp. 143–44.
39. As cited in Richard Burgess, "Navy's Unmanned Integrated Battle Problem 21 to Culminate in Missile Shoot," Seapower, April 20, 2021, https://seapowermagazine.org/navys-unmanned-integrated-battle-problem-21-to-culminate-in-missile-shoot/.
40. As quoted in Jon Harper, "Esper Calls for 500-Ship Navy to Counter China," National Defense, Oct. 6, 2020, https://www.nationaldefensemagazine.org/articles/2020/10/6/esper-calls-for-500-ship-navy-to-counter-china.
41. U.S. Navy, Chief of Naval Operations, "CNO NAVPLAN, January 2021," p. 6, https://media.defense.gov/2021/Jan/11/2002562551/-1/-1/1/CNO%20NAVPLAN%202021%20-%20FINAL.PDF.
42. As cited in Burgess, "Navy's Unmanned Integrated Battle Problem 21."
43. CRS, *Navy Large Unmanned Surface and Undersea Vehicles: Background and Issues for Congress*, Updated March 25, 2021, Report R45757, https://crsreports.congress.gov/product/pdf/R/R45757/34. See also Justin Katz, "CNO lays out future fleet he wants: 500 ships, 12 carriers, 150 unmanned vessels," Breaking Defense, Feb. 18, 2022, https://breakingdefense.com/2022/02/cno-lays-out-future-fleet-he-wants-500-ships-12-carriers-150-unmanned-vessels/.
44. U.S. Navy, *Department of the Navy Unmanned Campaign Framework*, March 16, 2021, p. 15, https://www.navy.mil/Portals/1/Strategic/20210315%20Unmanned%20Campaign_Final_LowRes.pdf.
45. For background, see Stephen Losey, "How autonomous wingmen

will help fighter pilots in the next war," DefenseNews, Feb. 15, 2022, https://www.defensenews.com/air/2022/02/13/how-autonomous-wingmen-will-help-fighter-pilots-in-the-next-war/.
46. Theresa Hitchens, "Skyborg AI Flies Second Drone; Demos 'Portability,'" Breaking Defense, June 30, 2021, https://breakingdefense.com/2021/06/skyborg-ai-flies-second-drone-demos-portability/.
47. As cited in Valerie Insinna, "Coming soon: A U.S. competition for sixth-gen drone wingman could begin in FY24," Breaking Defense, Sept. 7, 2022, https://breakingdefense.com/2022/09/coming-soon-a-us-competition-for-sixth-gen-drone-wingman-could-begin-in-fy24/.
48. See U.S. Army, *Robotic and Autonomous Systems Strategy*, March 2017, p. 3, https://mronline.org/wp-content/uploads/2018/02/RAS_Strategy.pdf.
49. Sydney J. Freedberg Jr., "Meet the Army's Future Family of Robot Tanks: RCV," Breaking Defense, Nov. 9, 2020, https://breakingdefense.com/2020/11/meet-the-armys-future-family-of-robot-tanks-rcv/. See also CRS, "The Army's Robotic Combat Vehicle (RCV) Program," In Focus, July 14, 2021, https://www.everycrsreport.com/files/2021-07-14_IF11876_9568af60be380a1f3db5a25cba402e5eb5321bc3.pdf.
50. U.S. Government Accountability Office (GAO), Weapons Systems Annual Assessment, June 2022, pp. 151–152, https://www.gao.gov/assets/gao-22-105230.pdf.
51. See Patrick Tucker, "Russia is Working to Pair Combat Jets and Drones, Too," Defense One, Feb. 17, 2021, https://www.defenseone.com/technology/2021/02/russia-working-pair-combat-jets-and-drones-too/172109/; Roger McDermott, "Russia's Armed Forces Expand UAV Strike Capability," Eurasia Daily Monitor, Feb. 20, 2019, https://jamestown.org/program/russias-armed-forces-expand-uav-strike-capability/; and McDermott, "Moscow Forming First Robotic Military Units," Eurasia Daily Monitor, April 21, 2021, https://jamestown.org/program/moscow-forming-first-robotic-military-units/.
52. Rick Joe, "China's Growing High-End Military Drone Force," *The Diplomat*, Nov. 27, 2019, https://thediplomat.com/2019/11/chinas-growing-high-end-military-drone-force/; H. I. Sutton, "China's Navy Reveals a Large Underwater Robot Which Can Be a Game Changer," *Forbes*, Oct. 1, 2019, https://www.forbes.com/sites/hisutton/2019/10/01/china-reveals-new-robot-underwater-vehicle-hsu-001/?sh=77c626e19910.
53. Joint Statement on Lethal Autonomous Weapons Systems, First Committee, 77th United Nations General Assembly, Oct. 21, 2022, https://estatements.unmeetings.org/estatements/11.0010/20221021/A1jJ8bNfWGlL/KLw9WYcSnnAm_en.pdf.
54. DoD, DoD Directive 3000.09, Autonomy in Weapon Systems.
55. For background on Phalanx and Harpy systems, see Scharre, *Army of None*, pp. 5, 47–48, 111.
56. CRS, *U.S. Ground Forces Robotics and Autonomous Systems (RAS) and Artificial Intelligence (AI): Considerations for Congress*, Report R45392, November 20, 2018, p. 2, https://crsreports.congress.gov/product/pdf/R/R45392.
57. For background, see CRS, *Lethal Autonomous Weapons Systems: Issues for Congress*.
58. DoD, DoD Directive 3000.09, Autonomy in Weapon Systems.
59. See Sam LaGrone, "Navy: Large USV Will Require Small Crews for the Next Several Years," USNI News, Aug. 3, 2021, https://news.usni.org/2021/08/03/navy-large-usv-will-require-small-crews-for-the-next-several-years; David B. Larter, "Here's the DARPA project it says could pull the Navy a decade forward in unmanned technology," C4ISRnet, May 6, 2020, https://www.c4isrnet.com/2020/05/06/heres-the-darpa-project-it-says-could-pull-the-navy-a-decade-forward-in-unmanned-technology/.
60. See CRS, *Lethal Autonomous Weapons Systems*, pp. 14–15.
61. On China's imitation of U.S. UAVs, see Joe, "China's Growing High-End Military Drone Force."
62. For discussion, see Scharre, *Army of None*, pp. 137–179, 137–210.
63. CRS, *U.S. Ground Forces Robotics and Autonomous Systems*, p. 39.
64. See, for example, Cade Matz and Neal E. Boudette, "Inside Tesla as Elon Musk Pushed an Unflinching Vision for Self-Driving Cars," *The New York Times*, Dec. 6, 2021, https://www.nytimes.com/2021/12/06/technology/tesla-autopilot-elon-musk.html.
65. See Scharre, *Army of None*, pp. 189–95.
66. Anish Athalye et al., "Fooling Neural Networks in the Physical World With 3D Adversarial Objects," LabSix, October 31, 2017, https://www.labsix.org/physical-objects-that-fool-neural-nets/. See also CRS, *Artificial Intelligence and National Security*, pp. 29–34.
67. For discussion, see Chyba, "New Technologies & Strategic Stability," pp. 150–70.
68. For background on these principles, see Scharre, *Army of None*, pp. 257–61. See also CRS, *Lethal Autonomous Weapons Systems*, pp. 18–25.
69. HRW, *Making the Case*, p. 5.
70. International Committee of the Red Cross (ICRC), "ICRC Position on Autonomous Weapons Systems," Geneva, May 12, 2021, p. 8, https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems.
71. The Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, usually referred to as the Convention on Certain Conventional Weapons or CCW, is also known as the Inhumane Weapons Convention. UN, Office of Disarmament Affairs, "The Convention on Certain Conventional Weapons," https://www.un.org/disarmament/the-convention-on-certain-conventional-weapons/.
72. See Adam Satariano, Nick Cumming-Bruce, and Rick Gladstone, "Killer Robots Aren't Science Fiction. A Push to Ban Them Is Growing," *The New York Times*, web, Dec. 17, 2021, https://www.nytimes.com/2021/12/17/world/robot-drone-ban.html.
73. Isabelle Jones, "Historic opportunity to regulate killer robots fails as a handful of states block the majority," Stop Killer Robots, Dec. 17, 2021, https://www.stopkillerrobots.org/news/historic-opportunity-to-regulate-killer-robots-fails-as-a-handful-of-states-block-the-majority/.
74. See Group of Governmental Experts Related to Emerging Technologies in the Area of Lethal Autonomous Weapons Systems (LAWS), "Emerging Commonalities, Conclusions and Recommendations," August 2018, https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-_Group_of_Governmental_Experts_(2018)/GGE%2BLAWS%2BAugust_EC%2C%2BC%2Band%2BRs_final.pdf.
75. NSCAI, *Final Report*, pp. 92–95.
76. DoD, "DoD Adopts Ethical Principles for Artificial Intelligence," Feb. 24, 2020, https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/.
77. For background on hypersonic weapons and their potential uses in combat, see Bugos and Rief, *Understanding Hypersonic Weapons*.
78. On the arms control implications of hypersonics, see CRS, Conventional Prompt Global Strike and Long-Range Ballistic Missiles: Background and Issues, CRS Report, R41464, July 16, 2021, https://sgp.fas.org/crs/nuke/R41464.pdf.
79. For background on hypersonic weapons and their characteristics, see ibid. See also Bugos and Reif, *Understanding Hypersonic Weapons*.
80. James Acton, *Silver Bullet? Asking the Right Questions About Conventional Prompt Global Strike*, Carnegie Endowment for International Peace, Washington, D.C., September 3, 2013, p. 75, https:// carnegieendowment.org/2013/09/03/silver-bullet-asking-rightquestions-about-conventional-prompt-global-strike-pub-52778
81. DoD, *DoD Fiscal Year 2023 Budget Request*, p. 4.6.
82. Bugos and Reif, *Understanding Hypersonic Weapons*, pp. 12–14.
83. Theresa Hitchens, "Raytheon, Northrop, Lockheed to Compete for Hypersonic Interceptor," Breaking Defense. Nov. 19, 2021, https://

breakingdefense.com/2021/11/raytheon-northrop-lockheed-to-compete-for-hypersonic-interceptor/.
84. CRS, *Conventional Prompt Global Strike and Long-Range Ballistic Missiles*, p. 6.
85. As quoted in Sydney J. Freedberg Jr., "Army Ramps Up Funding for Laser Shield, Hypersonic Sword," Breaking Defense, Feb. 28, 2020, https://breakingdefense.com/2020/02/army-ramps-up-funding-for-laser-shield-hypersonic-sword/.
86. Rebeccah Heinrichs, "The Hypersonic Missile Debate," Aerospace Corporation, February 9, 2021, https://csps.aerospace.org/events/2021-02-09-hypersonic-missile-debate.
87. Russian Ministry of Foreign Affairs, "Foreign Minister Sergey Lavrov's Interview with Mediaset, Italian Television Network," Moscow, May 1, 2022, https://www.mid.ru/en/foreign_policy/news/1811569/.
88. Vladimir Putin, "Presidential Address to the Federal Assembly," Kremlin, March 1, 2018, http://en.kremlin.ru/events/president/news/56957.
89. Fred Kaplan, "What Should Really Alarm Us About China's New 'Hypersonic' Missile Test," Slate, Oct. 20, 2021, https://slate.com/news-and-politics/2021/10/china-hypersonic-missile-test-alarms.html.
90. Jill Hruby, "Russia's New Nuclear Weapon Delivery Systems: An Open-Source Technical Review," Nuclear Threat Initiative, November 13, 2019, pp. 20, 24, https://www.nti.org/analysis/reports/russias-new-nuclear-weapon-delivery-systems-open-source-technical-review/.
91. Ellyatt, "Russia says it fired hypersonic missiles in Ukraine."
92. As quoted in "'Falling Behind': U.S. Admiral Warns of China Dominance in Hypersonic Missile Race," South China Morning Post, Feb. 16, 2018, https://www.scmp.com/news/asia/east-asia/article/2133583/falling-behind-us-admiral-warns-china-dominance-hypersonic.
93. As quoted in Mike Stone, "U.S. in hypersonic weapon 'arms race' with China -Air Force secretary," Reuters, Nov. 30, 2021, https://www.reuters.com/business/aerospace-defense/us-hypersonic-weapon-arms-race-with-china-air-force-secretary-2021-11-30/.
94. On China's HGV, see Kaplan, "What Should Really Alarm Us About China's New 'Hypersonic' Missile Test." On the U.S. HGV test, see Jen Judson, "U.S.-Developed Hypersonic Missile Hit within 6 Inches of Target, Says Army Secretary," Defense News, October 13, 2020, https://www.defensenews.com/digital-show-dailies/ausa/2020/10/13/us-developed-hypersonic-missile-hit-within-six-inches-of-target-army-secretary-reports.
95. As quoted in Shannon Bugos, "Congress Shouldn't Rubber-Stamp Hypersonic Weapons," Breaking Defense, Sept. 29, 2021, https://breakingdefense.com/2021/09/congress-shouldnt-rubber-stamp-hypersonic-weapons/.
96. As quoted in Aaron Gregg, "Military-Industrial Complex Finds a Growth Market in Hypersonic Weaponry," Washington Post, December 31, 2018, https://www.washingtonpost.com/business/2018/12/21/military-industrial-complex-finds-growth-market-hypersonic-weaponry/.
97. Peter Erbland, "Tactical Boost Glide (TBG)," Defense Advanced Research Projects Agency, n.d., https://www.darpa.mil/program/tactical-boost-glide.
98. Andrew Roth, "Russia will act if NATO countries cross Ukraine 'red lines,' Putin says," Guardian, Nov. 30, 2021, https://www.theguardian.com/world/2021/nov/30/russia-will-act-if-nato-countries-cross-ukraine-red-lines-putin-says.
99. CRS, *Conventional Prompt Global Strike and Long-Range Ballistic Missiles*, pp. 2–3, 23–27.
100. See Acton, "Silver Bullet?" pp. 113–119.
101. Ibid., pp. 126–129.
102. Shannon Bugos, "U.S., Russia Establish Strategic Stability Groups," *Arms Control Today*, November 2021, https://www.armscontrol.org/act/2021-11/news/us-russia-establish-strategic-stability-groups.
103. Mark Gubrud, Rajaram Nagappa, and Tong Zhao, "Test Ban for Hypersonic Missiles?" Bulletin of the Atomic Scientists, August 6, 2015, https://thebulletin.org/roundtable/test-ban-for-hypersonic-missiles/.
104. For discussion of arms control options, see Bugos and Reif, *Understanding Hypersonic Weapons*, pp. 20–23.
105. DoD, *Nuclear Posture Review Report*, April 2010, p. ix, https://dod.defense.gov/Portals/1/features/defenseReviews/NPR/2010_Nuclear_Posture_Review_Report.pdf.
106. DoD, *Nuclear Posture Review*, February 2018, p. 31, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.
107. Ibid, pp. 56–58.
108. For background on U.S. cyberattacks aimed at North Korea, see Sanger, *The Perfect Weapon*, pp. 268–93.
109. As quoted in Aaron Mehta, "Nuclear Posture Review Draft Leaks," Defense News, January 12, 2018, https://www.defensenews.com/space/2018/01/12/nuclear-posture-review-draft-leaks-new-weapons-coming-amid-strategic-shift/.
110. As cited in Brad D. Williams, "Nakasone: Cold War-style deterrence 'does not comport to cyberspace,'" Breaking Defense. Nov. 4, 2021, https://breakingdefense.com/2021/11/nakasone-cold-war-style-deterrence-does-not-comport-to-cyberspace/.
111. For an assessment of these and other cyber-related risks of escalation, see Ariel E. Levite, et al., *China-U.S. Cyber-Nuclear C3 Stability*, Carnegie Endowment for International Peace, April 2021, https://carnegieendowment.org/files/Levite_et_all_C3_Stability.pdf.
112. For a thorough description of the U.S. nuclear weapons enterprise and its constituent NC3 systems, see Lin, Cyber Threats and Nuclear Weapons, pp. 36–89.
113. Levite, et al., *China-U.S. Cyber-Nuclear C3 Stability*, p. 15.
114. For a comprehensive assessment of the cyber threat, see Sanger, *The Perfect Weapon*. On Russian involvement in so-called "ransomware" attacks, see, for example, David E. Sanger and Nicole Perlroth, "Biden Warns Putin to Act Against Ransomware Groups, or U.S. Will Strike Back," *The New York Times*, July 9, 2021, https://www.nytimes.com/2021/07/09/us/politics/biden-putin-ransomware-russia.html.
115. For a thorough assessment of these vulnerabilities, see Lin, *Cyber Threats and Nuclear Weapons*, pp. 38–104. See also Beyza Unal and Patricia Lewis, "Cybersecurity of Nuclear Weapons Systems," Chatham House, January 2018, https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf.
116. Lin, *Cyber Threats and Nuclear Weapons*, p. 91.
117. Kate Conger and David E. Sanger, "U.S. Says It Secretly Removed Malware Worldwide, Pre-empting Russian Cyberattacks," *The New York Times*, April 6, 2022, https://www.nytimes.com/2022/04/06/us/politics/us-russia-malware-cyberattacks.html.
118. Statement of General Paul M. Nakasone before the Senate Armed Services Committee, February 14, 2019, https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf.
119. Julian E. Barnes, "Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections," *The New York Times*, February 26, 2019, https://www.nytimes.com/2019/02/26/us/politics/us-cyber-command-russia.html.
120. For background on these operations, see Sanger, *The Perfect Weapon*, pp. 7–36 and 276–283.
121. David E. Sanger, "Russian Hackers Appear to Shift Focus to U.S. Power Grid," *The New York Times*, July 27, 2018, https://www.nytimes.com/2018/07/27/us/politics/russian-hackers-electric-grid-elections-.html.
122. For a summary of such scenarios, see Page O. Stoutland and

Samantha Pitts-Kiefer, "Nuclear Weapons in the New Cyber Age: Report of the Cyber-Nuclear Weapons Study Group," Nuclear Threat Initiative, September 2018, p. 12, https://media.nti.org/documents/Cyber_report_finalsmall.pdf.
123. James N. Miller Jr. and Richard Fontaine, "A New Era in U.S.-Russian Strategic Stability," Harvard Kennedy School Belfer Center for Science and International Affairs and the Center for a New American Security, September 2017, p. 18, https://www.cnas.org/publications/reports/a-new-era-in-u-s-russian-strategic-stability.
124. Stoutland and Pitts-Kiefer, "Nuclear Weapons in the New Cyber Age," p. 12.
125. See James M. Acton, "Escalation Through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risk of Inadvertent Nuclear War," *International Security*, vol. 43, no. 1 (Summer 2018), pp. 56–99.
126. See Ivan Nechepurenko, "Kremlin Warns of Cyberwar After Report of U.S. Hacking Into Russian Power Grid," *The New York Times*, June 17, 2019, https://www.nytimes.com/2019/06/17/world/europe/russia-us-cyberwar-grid.html.
127. Miller Jr. and Fontaine, "New Era in U.S.-Russian Strategic Stability," p. 19.
128. See Zachary Fryer-Biggs, "The Pentagon Has Prepared a Cyberattack Against Russia," Daily Beast, November 2, 2018, https://www.thedailybeast.com/the-pentagon-has-prepared-a-cyber-attack-against-russia. On the Biden administration's retention of NSPM-13, see David Sanger, Julian E. Barnes, and Nicole Perlroth, "Preparing for Retaliation Against Russia, U.S. Confronts Hacking by China," *The New York Times*, March 7, 2018, https://www.nytimes.com/2021/03/07/us/politics/microsoft-solarwinds-hack-russia-china.html.
129. U.S. Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command," p. 4, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.
130. As quoted in Fryer-Biggs, "Pentagon Has Prepared a Cyberattack Against Russia."
131. Levite, et al., *China-U.S. Cyber-Nuclear C3 Stability*, p. 14.
132. Ibid, pp. 32–33. Inadvertest
133. See Lin, *Cyber Threats and Nuclear Weapons*, p. 130.
134. Acton, "Cyber Warfare & Inadvertent Escalation," p. 145.
135. Levite, et al., *China-U.S. Cyber-Nuclear C3 Stability*, p. 40.
136. Acton, "Cyber Warfare and Inadvertent Escalation," p. 143.
137. Ibid, pp. 143–44. See also Lin, *Cyber Threats and Nuclear Weapons*, pp. 123–31, 143–46.
138. Lin, *Cyber Threats and Nuclear Weapons*, p. 128.
139. UN General Assembly (UNGA), Resolution 66/24, Developments in the field of information and telecommunications in the context of international security, December 2, 2011, https://undocs.org/A/RES/66/24.
140. UNGA, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General," A/68/98, June 24, 2013, https://undocs.org/A/68/98.
141. UNGA, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General," A/70/174, July 22, 2015, https://undocs.org/en/A/70/174.
142. UNGA, General Assembly Resolution A/70/237, December 23, 2015, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/457/57/PDF/N1545757.pdf.
143. DoD, *Defense Budget Overview, DoD Fiscal Year 2022 Budget Request*, chap. 2, pp. 12–14, https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2022/FY2022_Budget_Request_Overview_Book.pdf.
144. CRS, "In Focus: Nuclear Command, Control, and Communications (NC3) Modernization," Dec. 8, 2020, https://sgp.fas.org/crs/nuke/IF11697.pdf.
145. *DoD, Nuclear Posture Review 2018*, pp. 56–58.
146. U.S. Congressional Budget Office, *Projected Costs of U.S. Nuclear Forces, 2019 to 2028*, January 2019, p. 2, https://www.cbo.gov/system/files/2019-01/54914-NuclearForces.pdf.
147. For an account of nuclear control accidents during the Cold War, see Scott D. Sagan, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons* (Princeton: Princeton University Press, 1993).
148. CRS, *Artificial Intelligence and National Security*, pp. 9–13.
149. NSCAI, *Final Report*, p. 80
150. CRS, *Artificial Intelligence and National Security*, p. 13.
151. 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/.
152. As quoted in Sydney J. Freedberg Jr., "No AI for Nuclear Command and Control: JAIC's Shanahan," Breaking Defense, September 25, 2019, https://breakingdefense.com/2019/09/no-ai-for-nuclear-command-control-jaics-shanahan/.
153. DoD, "Summary of the Joint All-Domain Command & Control (JADC2) Strategy," March 2022, https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF.
154. As quoted in Colin Clark, "Gen. Hyten On The New American Way of War: All-Domain Operations," Breaking Defense, Feb. 18, 2020, https://breakingdefense.com/2020/02/gen-hyten-on-the-new-american-way-of-war-all-domain-operations/.
155. Theresa Hitchens, "SecDef OKs Joint Warfighting Concept; Joint Requirements Due Soon," Breaking Defense, June 16, 2021, https://breakingdefense.com/2021/06/secdef-oks-joint-warfighting-construct-joint-requirements-due-soon/. See also DoD, "Summary of the Joint All-Domain Command & Control (JADC2) Strategy."
156. CRS, "In Focus: Advanced Battlefield Management System," Sept. 27, 2021, https://sgp.fas.org/crs/weapons/IF11866.pdf.
157. On Project Convergence, see CRS, "In Focus: The Army's Project Convergence," Sept. 27, 2021, https://sgp.fas.org/crs/weapons/IF11654.pdf. On Overmatch, see Yasmin Tadjdeh, "Navy Dedicates More Resources To Secretive Project Overmatch," National Defense, Aug. 10, 2021, https://www.nationaldefensemagazine.org/articles/2021/8/10/navy-dedicates-more-resources-to-secretive-project-overmatch.
158. CRS, "In Focus: Joint All-Domain Command and Control (JADC2)," Updated Jan. 21, 2022, https://sgp.fas.org/crs/natsec/IF11493.pdf.
159. DoD, *Fiscal Year 2022 Budget Request*, p. 3–16.
160. Ibid.
161. As quoted in Theresa Hitchens, "Picking 1st ABMS Capabilities a Top Issue at Air Force Corona," Breaking Defense, Sept. 23, 2020, https://breakingdefense.com/2020/09/picking-1st-abms-capabilities-a-top-issue-at-air-force-corona/.
162. As quoted in Colin Clark, "Nuclear C3 Goes All Domain: Gen. Hyten," Breaking Defense, February 20, 2020, https://breakingdefense.com/2020/02/nuclear-c3-goes-all-domain-gen-hyten/.
163. As quoted in Aaron Mehta, "Why nuclear command and control can't be separated from JADC2," Breaking Defense, March 8, 2022, https://breakingdefense.com/2022/03/why-nuclear-command-and-control-cant-be-separated-from-jadc2/.
164. Michael C. Horowitz, Paul Scharre, and Alexander Velez-Green, "A Stable Nuclear Future? The Impact of Autonomous Systems and Artificial Intelligence," December 2019, pp. 12–13, https://arxiv.org/ftp/arxiv/papers/1912/1912.05291.pdf.
165. As noted in Edward Geist and Andrew J. Lohn, "How Might

Artificial Intelligence Affect the Risk of Nuclear War?" RAND Corp., 2018, p. 10, https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE296/RAND_PE296.pdf.
166. See Tyler Rogoway, "Look Inside Putin's Massive New Military Command and Control Center," Jalopnik, November 19, 2015, https://foxtrotalpha.jalopnik.com/look-inside-putins-massive-new-military-command-and-con-1743399678.
167. As quoted in Joseph Trevithick, "Putin Reveals Existence Of New Nuclear Command Bunker," The Warzone, Nov. 11, 2020, https://www.thedrive.com/the-war-zone/37569/putin-reveals-existence-of-new-nuclear-command-bunker-and-says-its-almost-complete.
168. Fiona Cunningham, "Nuclear Command, Control, and Communications Systems of the People's Republic of China," Nautilus Institute, July 18, 2019, https://nautilus.org/napsnet/napsnet-special-reports/nuclear-command-control-and-communications-systems-of-the-peoples-republic-of-china/.
169. DoD, *Military and Security Developments Involving the People's Republic of China 2021, Annual Report to Congress*, p. 89, https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF.
170. See CRS, *Artificial Intelligence and National Security*, pp. 29–34.
171. On the Petrov incident, see Scharre, *Army of None*, pp. 1–2.
172. Horowitz, Scharre, and Velez-Green, "Stable Nuclear Future?" p. 17.
173. Geist and Lohn, "How Might Artificial Intelligence Affect the Risk of Nuclear War?" p. 18.
174. Scharre, *Army of None*, pp. 199–230.
175. Freedberg Jr., "No AI for Nuclear Command and Control: JAIC's Shanahan."
176. NSCAI, *Final Report*, p. 97.
177. Ibid, pp. 97–103.
178. Scharre, *Army of None*, pp. 199–210.
179. "Autonomous weapons that kill must be banned, insists UN chief," UN News, March 25, 2019, https://news.un.org/en/story/2019/03/1035381.
180. Shannon Bugos, "U.S., Russia Establish Strategic Stability Groups."
181. Written Statement of Secretary of Defense Jim Mattis, Senate Armed Services Committee, April 26, 2018, https://www.armed-services.senate.gov/imo/media/doc/Mattis_04-26-18.pdf.
182. State Council Information Office of the People's Republic of China, "China's National Defense in the New Era," July 2019, http://english.www.gov.cn/atts/stream/files/5d3943eec6d0a15c923d2036.
183. See Roger McDermott, "Russia's Military Scientists and Future Warfare," Eurasia Daily Monitor, June 5, 2019, https://jamestown.org/program/russias-military-scientists-and-future-warfare/.
184. DoD, *Nuclear Posture Review 2018*. On Russian nuclear doctrine, see Anya Loukianova Fink and Olga Oliker, "Russia's Nuclear Weapons in a Multipolar World," *Daedalus*, vol. 149, no. 2 (Spring 2020), pp, 37–55.
185. See David E. Sanger and William J. Broad, "Russia's Small Nuclear Arms: A Risky Option for Putin and Ukraine Alike," *The New York Times*, Oct. 3, 2022, https://www.nytimes.com/2022/10/03/us/politics/russia-tactical-nuclear-weapons.html.
186. See Hans M. Kristensen and Matt Korda, "Chinese Nuclear Forces, 2020," *Bulletin of the Atomic Scientists*, vol. 76, no. 6 (2020), pp. 443–57.
187. See Steven E. Miller, "A Nuclear World Transformed: The Rise of Multilateral Disorder," *Daedalus*, vol. 149, no. 2 (Spring 2020), pp. 17–36.
188. See Acton, "Escalation Through Entanglement."
189. For a review of the arms control "toolbox" and other proposals for controlling destabilizing technologies, see Jon Brook Wolfsthal, "Why Arms Control?" *Daedalus*, vol. 149, no. 2 (Spring 2020), pp. 101–15. See also Giacomo Persi Paoli, Kerstin Vignard, David Danks, and Paul Meyer, Modernizing Arms Control: Exploring Responses to the Use of AI in Military Decision-Making (Geneva, Switzerland: UN Institute for Disarmament Research, 2020).
190. Jones, "Historic opportunity to regulate killer robots fails."
191. "Minister's Declaration at the Occasion of the Conference 'Capturing Technology, Rethinking Arms Control,'" November 6, 2020, https://www.auswaertiges-amt.de/en/newsroom/news/maas-rethinking-arms-control/2413346.
192. Pugwash, "Geneva Workshop on Hypersonic Weapons," Geneva, Dec. 15, 2019, https://pugwash.org/2019/12/15/geneva-workshop-on-hypersonic-weapons/.
193. Pugwash, "Geneva workshop on Cyber Security and Warfare," March 2, 2020, https://pugwash.org/2020/03/02/geneva-workshop-on-cyber-security-and-warfare-2/.
194. NSCAI, *Final Report*, pp. 97–100.
195. DoD, "DoD Adopts Ethical Principles for Artificial Intelligence."
196. DoD, *Responsible Artificial Intelligence Strategy and Implementation Pathway*, June 2022, https://www.ai.mil/docs/RAI_Strategy_and_Implementation_Pathway_6-21-22.pdf.
197. Acton, "Cyber Warfare & Inadvertent Escalation," pp. 143–44.
198. See Acton, *Silver Bullet?*, pp. 116–17.
199. Joint Statement on Lethal Autonomous Weapons Systems, First Committee, Oct. 21, 2022.
200. Kingston Reif and Shannon Bugos, "No Progress Toward Extending New START," *Arms Control Today*, July/August 2020, pp. 31–32.
201. NSCAI, *Final Report*, p. 99.
202. See, for example, Acton, *Silver Bullet?*, pp. 134–38. See also Michael C. Horowitz, Lauren Kahn, and Casey Mahoney, "The Future of Military Applications of Artificial Intelligence: A Role for Confidence-Building Measures? *Orbis*, Fall 2020, pp. 527–43.
203. Acton, "Cyber Warfare & Inadvertent Escalation," p. 145.
204. See, for example, Vincent Boulanin, Kolja Brockmann, and Luke Richards, *Responsible Artificial Intelligence Research and Innovation for International Peace and Security* (Stockholm: Stockholm International Peace Research Institute, 2020).

Arms Control Association

The Arms Control Association (ACA), founded in 1971, is a national nonpartisan membership organization dedicated to promoting public understanding of and support for effective arms control policies. Through its public education and media programs and its magazine, *Arms Control Today (ACT)*, ACA provides policymakers, the press and the interested public with authoritative information, analysis and commentary on arms control proposals, negotiations and agreements, and related national security issues. In addition to the regular press briefings ACA holds on major arms control developments, the Association's staff provides commentary and analysis on a broad spectrum of issues for journalists and scholars both in the United States and abroad.

Increasingly in recent years, advanced military powers have begun to incorporate and rely on new kinds or new applications of advanced technologies in their arsenals, such as artificial intelligence, robotics, cyber, and hypersonics, among others.

The weaponization of these technologies may potentially carry far-ranging, dangerous consequences that expand into the nuclear realm by running up the escalation ladder or by blurring the distinction between a conventional and nuclear attack. Arms control, therefore, emerges as a tool to slow the pace of weaponizing these technologies and to adopt meaningful restraints on their use.

This report examines four particular new kinds or new applications of technologies—autonomous weapons systems, hypersonic weapons, cyberattacks, and automated battlefield decision-making—and proposes a framework strategy aimed at advancing an array of measures that all contribute to the larger goal of preventing unintended escalation and enhancing strategic stability.

Arms Control Association

1200 18th Street NW, Suite 1175
Washington, D.C. 20036
www.armscontrol.org