In every other generation, it seems, 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 publics pushed diplomats to sign the Geneva Protocol of 1925, prohibiting the use in war of asphyxiating, poisonous, and other lethal gases. World War II witnessed the tragic application of nuclear technology to warfare, and much of postwar diplomacy entailed efforts to prevent the proliferation and use of atomic munitions.

Today, a whole new array of technologies—artificial intelligence (AI), robotics, hypersonics, and cybertechnology, among others—is being applied to military use, with potentially far-ranging consequences. Although the risks and ramifications of these weapons are not yet widely recognized, policymakers will be compelled to address the dangers posed by innovative weapons technologies and to devise international arrangements to regulate or curb their use. Although some early efforts have been undertaken in this direction, most notably, in attempting to prohibit the deployment of...
fully autonomous weapons systems, far more work is needed to gauge the impacts of these technologies and to forge new or revised control mechanisms as deemed appropriate.

Tackling the arms control implications of emerging technologies now is becoming a matter of ever-increasing urgency as the pace of their development is accelerating and their potential applications to warfare are multiplying. Many analysts believe that the utilization of AI and robotics will utterly revolutionize warfare, much as the introduction of tanks, airplanes, and nuclear weapons transformed the battlefields of each world war. “We are in the midst of an ever accelerating and expanding global revolution in [AI] and machine learning, with enormous implications for future economic and military competitiveness,” declared former U.S. Deputy Secretary of Defense Robert Work, a prominent advocate for Pentagon utilization of the new technologies.

The Department of Defense is spending billions of dollars on AI, robotics, and other cutting-edge technologies, contending that the United States must maintain leadership in the development and utilization of those technologies lest its rivals use them to secure a future military advantage. China and Russia are assumed to be spending equivalent sums, indicating the initiation of a vigorous arms race in emerging technologies. “Our adversaries are presenting us today with a renewed challenge of a sophisticated, evolving threat,” Michael Griffin, U.S. undersecretary of defense for research and engineering, told Congress in April. “We are in turn preparing to meet that challenge and to restore the technical overmatch of the United States armed forces that we have traditionally held.”

In accordance with this dynamic, the United States and its rivals are pursuing multiple weapons systems employing various combinations of AI, autonomy, and other emerging technologies. These include, for example, unmanned aerial vehicles (UAVs) and unmanned surface and subsurface naval vessels capable of being assembled in swarms, or “wolfpacks,” to locate enemy assets such as tanks, missile launchers, submarines and, if communications are lost with their human operators, decide to strike them on their own. The Defense Department also has funded the development of two advanced weapons systems employing hypersonic technology: a hypersonic air-launched cruise missile and the Tactical Boost Glide (TBG) system, encompassing a hypersonic rocket for initial momentum and an unpowered payload that glides to its destination. In the cyberspace realm, a variety of offensive and retaliatory cyberweapons are being developed by the U.S. Cyber Command for use against hostile states found to be using cyberspace to endanger U.S. national security.

The introduction of these and other such weapons on future battlefields will transform every aspect of combat and raise a host of challenges for advocates of responsible arms control. The use of fully autonomous weapons in combat, for example, automatically raises questions about the military’s ability to comply with the laws of war and international humanitarian law, which require belligerents to distinguish between enemy combatants and civilian bystanders. It is on this basis that opponents of such systems are seeking to negotiate a binding international ban on their deployment.

Even more worrisome, some of the weapons now in development, such as unmanned anti-submarine
wolfpacks and the TBG system, could theoretically endanger the current equilibrium in nuclear relations among the major powers, which rests on the threat of assured retaliation by invulnerable second-strike forces, by opening or seeming to open various first-strike options. Warfare in cyberspace could also threaten nuclear stability by exposing critical early-warning and communications systems to paralyzing attacks and prompting anxious leaders to authorize the early launch of nuclear weapons.

These are only some of the challenges to global security and arms control that are likely to be posed by the weaponization of new technologies. Observers of these developments, including many who have studied them closely, warn that the development and weaponization of AI and other emerging technologies is occurring faster than efforts to understand their impacts or devise appropriate safeguards. “Unfortunately,” said former U.S. Secretary of the Navy Richard Danzig, “the uncertainties surrounding the use and interaction of new military technologies are not subject to confident calculation or control.” Given the enormity of the risks involved, this lack of attention and oversight must be overcome.

Mapping out the implications of the new technologies for warfare and arms control and devising effective mechanisms for their control are a mammoth undertaking that requires the efforts of many analysts and policymakers around the world. This piece, an overview of the issues, is the first in a series for Arms Control Today (ACT) that will assess some of the most disruptive emerging technologies and their war-fighting and arms control implications. Future installments will look in greater depth at four especially problematic technologies: AI, autonomous weaponry, hypersonics, and cyberwarfare. These four have been chosen for close examination because, at this time, they appear to be the furthest along in terms of conversion into military systems and pose immediate challenges for international peace and stability.

**Artificial Intelligence**

AI is a generic term used to describe a variety of techniques for investing machines with an ability to monitor their surroundings in the physical world or cyberspace and to take independent action in response to various stimuli. To invest machines with these capacities, engineers have developed complex algorithms, or computer-based sets of rules, to govern their operations. An AI-equipped aerial drone, for example, could be equipped with sensors to distinguish enemy tanks from other vehicles on a crowded battlefield and, when some are spotted, choose on its own to fire at them with its onboard missiles. AI can also be employed in cyberspace, for example to watch for enemy cyberattacks and counter them with a barrage of counterstrikes. In the future, AI-invested machines may be empowered to determine if a nuclear attack is underway and, if so, initiate a retaliatory strike.

In this sense, AI is an “omni-use” technology, with multiple implications for war-fighting and arms control.
Many analysts believe that AI will revolutionize warfare by allowing military commanders to bolster or, in some cases, replace their personnel with a wide variety of “smart” machines. Intelligent systems are prized for the speed with which they can detect a potential threat and their ability to calculate the best course of action to neutralize that peril. As warfare among the major powers grows increasingly rapid and multidimensional, including in the cyberspace and outer space domains, commanders may choose to place ever-greater reliance on intelligent machines for monitoring enemy actions and initiating appropriate countermeasures. This could provide an advantage on the battlefield, where rapid and informed action could prove the key to success, but also raises numerous concerns, especially regarding nuclear “crisis stability.”

Analysts worry that machines will accelerate the pace of fighting beyond human comprehension and possibly take actions that result in the unintended escalation of hostilities, even leading to use of nuclear weapons. Not only are AI-equipped machines vulnerable to error and sabotage, they lack an ability to assess the context of events and may initiate inappropriate or unjustified escalatory steps that occur too rapidly for humans to correct. “Even if everything functioned properly, policymakers could nevertheless effectively lose the ability to control escalation as the speed of action on the battlefield begins to eclipse their speed of decision-making,” writes Paul Scharre, who is director of the technology and national security program at the Center for a New American Security.

As AI-equipped machines assume an ever-growing number and range of military functions, policymakers will have to determine what safeguards are needed to prevent unintended, possibly catastrophic consequences of the sort suggested by Scharre and many others. Conceivably, AI could bolster nuclear stability by providing enhanced intelligence about enemy intentions and reducing the risk of misperception and miscalculation; such options also deserve attention. In the near term, however, control efforts will largely be focused on one particular application of AI: fully autonomous weapons systems.

**Autonomous Weapons Systems**

Autonomous weapons systems, sometimes called lethal autonomous weapons systems, or “killer robots,” combine AI and drone technology in machines equipped 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.”

Some such systems have already been put to military use. The Navy’s Aegis air defense system, for example, is empowered to track enemy planes and missiles within a certain radius of a ship at sea and, if it identifies an imminent threat, to fire missiles against it. Similarly, Israel’s Harpy UAV can search for enemy radar systems over a designated area and, when it locates one, strike it on its own. Many other such munitions are now in development, including undersea drones intended for anti-submarine warfare and entire fleets of UAVs designed for use in “swarms,” or flocks of armed drones that twist and turn above the battlefield in coordinated maneuvers that are difficult to follow.

The deployment of fully autonomous weapons systems poses numerous challenges to international security and arms control, beginning with a potentially insuperable threat to the laws of war and international humanitarian law. Under these norms, armed belligerents are obligated to distinguish between enemy combatants and civilians on the battlefield and to avoid unnecessary harm to the latter. In addition, any civilian casualties that do occur in battle should not be disproportionate to the military necessity of attacking that position. Opponents of lethal autonomous weapons systems argue that only humans possess the necessary judgment to make such fine distinctions in the heat of battle and that machines will never be made intelligent enough to do so and thus should be banned from deployment.

At this point, some 25 countries have endorsed steps to enact such a ban in the form of a protocol to the Convention on Certain Conventional Weapons (CCW). Several other nations, including the United States and Russia, oppose a ban on lethal autonomous weapons systems, saying they can be made compliant with international humanitarian law.

Looking further into the future, autonomous weapons systems could pose a potential threat to nuclear stability by investing their owners with a capacity to detect, track, and destroy enemy submarines and mobile missile launchers. Today’s stability, which can be seen as an uneasy nuclear balance of terror, rests on the belief that each major power possesses at least some devastating second-strike, or retaliatory, capability, whether mobile launchers for intercontinental ballistic missiles (ICBMs), submarine-launched ballistic missiles (SLBMs), or both, that are immune to real-time detection and safe from a first strike. Yet, a nuclear-armed belligerent might someday undermine the deterrence equation by employing undersea drones to pursue and destroy enemy...
ballistic missile submarines along with swarms of UAVs to hunt and attack enemy mobile ICBM launchers.

Even the mere existence of such weapons could jeopardize stability by encouraging an opponent in a crisis to launch a nuclear first strike rather than risk losing its deterrent capability to an enemy attack. Such an environment would erode the underlying logic of today’s strategic nuclear arms control measures, that is, the preservation of deterrence and stability with ever-diminishing numbers of warheads and launchers, and would require new or revised approaches to war prevention and disarmament.\(^{11}\)

**Hypersonic Weapons**

Proposed hypersonic weapons, which can travel at a speed of more than five times the speed of sound, or more than 5,000 kilometers per hour, generally fall into two categories: hypersonic glide vehicles and hypersonic cruise missiles, either of which could be armed with nuclear or conventional warheads. With hypersonic glide vehicle systems, a rocket carries the unpowered glide vehicle into space, where it detaches and flies to its target by gliding along the upper atmosphere. Hypersonic cruise missiles are self-powered missiles, utilizing advanced rocket technology to achieve extraordinary speed and maneuverability.

No such munitions currently exist, but China, Russia, and the United States are developing hypersonic weapons of various types. The U.S. Defense Department, for example, is testing the components of a hypersonic glide vehicle system under its Tactical Boost Glide project and recently awarded a $928 million contract to Lockheed Martin Corp. for the full-scale development of a hypersonic air-launched cruise missile, tentatively called the Hypersonic Conventional Strike Weapon.\(^{12}\) Russia, for its part, is developing a hypersonic glide vehicle it calls the Avangard, which it claims will be ready for deployment by the end of 2019, and China in August announced a successful test of the Starry Sky-2 hypersonic glide vehicle described as capable of carrying a nuclear weapon.\(^{13}\)

Whether armed with conventional or nuclear warheads, hypersonic weapons pose a variety of challenges to international stability and arms control. At the heart of such concerns is these weapons’ exceptional speed and agility. Anti-missile systems that may work against existing threats might not be able to track and engage hypersonic vehicles, potentially allowing an aggressor to contemplate first-strike disarming attacks on nuclear or conventional forces while impelling vulnerable defenders to adopt a launch-on-warning policy.\(^{14}\) Some analysts warn that the mere acquisition of such weapons could “increase the expectation of a disarming attack.” Such expectations “encourage the threatened nations to take such actions as devolution of command-and-control of strategic forces, wider dispersion of such forces, a launch-on-warning posture, or a policy of preemption during a crisis.” In short, “hypersonic threats encourage hair-trigger tactics that would increase crisis instability.”\(^{15}\)

The development of hypersonic weaponry poses a significant threat to the core principle of assured retaliation, on which today’s nuclear strategies and arms control measures largely rest. Overcoming that danger will require commitments on the part of the major powers jointly to consider the risks posed by such weapons and what steps might be necessary to curb their destabilizing effects.

The development of hypersonic munitions also introduces added problems of proliferation. Although the bulk of research on such weapons is now being conducted by China, Russia, and the United States, other nations are exploring the technologies involved and eventually could produce such munitions on their own eventually. In a world of widely disseminated hypersonic weapons, vulnerable states would fear being attacked with little or no warning time, possibly impelling them to conduct pre-emptive strikes on enemy capabilities or to commence hostilities at the earliest indication of an incoming missile. Accordingly, the adoption of fresh nonproliferation measures also belongs on the agenda of major world leaders.\(^{16}\)

**Cyberattack**

Secure operations in cyberspace, the global web of information streams tied to the internet, has
become essential for the continued functioning of the international economy and much else besides. 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. It is increasingly evident, however, that governmental bodies, often working in conjunction with some of those individuals, are employing cyberweapons to weaken their enemies by sowing distrust or sabotaging key institutions or to bolster their own defenses by stealing militarily relevant technological know-how.

Moreover, in the event of a crisis or approaching hostilities, cyberattacks could be launched on an adversary’s early-warning, communications, and command and control systems, significantly impairing its response capabilities. For all these reasons, cybersecurity, or the protection of cyberspace from malicious attack, has become a major national security priority.

Cybersecurity, as perceived by U.S. leaders, can take two forms: defensive action aimed at protecting one’s own information infrastructure against attack; and offensive action intended to punish, or retaliate against, an attacker by severely disrupting its systems, or to deter such attack by holding out the prospect of such punishment. The U.S. Cyber Command, elevated by President Donald Trump in August 2017 to a full-fledged Unified Combatant Command, is empowered to conduct both types of operations.

In many respects then, the cyber domain is coming to resemble the strategic nuclear realm, with notions of defense, deterrence, and assured retaliation initially devised for nuclear scenarios now being applied to conflict in cyberspace. Although battles in this domain are said to fall below the threshold of armed combat (so long, of course, as no one is killed as a result), it is not difficult to conceive of skirmishes in cyberspace that erupt into violent conflict, for example if cyberattacks result in the collapse of critical infrastructure, such as the electric grid or the banking system.

Considered solely as a domain of its own, cyberspace is a fertile area for the introduction of regulatory measures that might be said to resemble arms control, although referring to cyberweapons rather than nuclear or conventional munitions. This is not a new challenge but one that has grown more pressing as the technology advances. At what point, for example, might it be worthwhile to impose formal impediments to the cyber equivalent of a disarming first strike, a digital attack that would paralyze a rival’s key information systems? A group of governmental experts was convened by the UN General Assembly to investigate the adoption of norms and rules for international behavior in cyberspace, but failed to reach agreement on measures that would satisfy all major powers.

More importantly, it is essential to consider how combat in cyberspace might spill over into the physical world, triggering armed combat and possibly hastening the pace of escalation. This danger was brought into bold relief in February 2018, when the Defense Department released its latest Nuclear Posture Review report, spelling out the Trump administration’s approach to nuclear weapons and their use. Stating that an enemy cyberattack on U.S. strategic command and control systems could pose a critical threat to U.S. national security, the new policy holds out the prospect of a nuclear response to such attacks. The United States, it affirmed, would only consider using nuclear weapons in “extreme circumstances,” which could include attacks “on U.S. or allied nuclear forces, their command and control, or warning and attack assessment capabilities.”

The policy of other states in this regard is not so clearly stated, but similar protocols undoubtedly exist. Accordingly, management of this spillover effect from cyber- to conventional or even nuclear conflict will become a major concern of international policymakers in the years to come.

The Evolving Arms Control Agenda

To be sure, policymakers and arms control advocates will have their hands full in the coming months and years just preserving existing accords and patching them up where needed. At present, several key agreements, including the 1987 Intermediate-Range Nuclear Forces Treaty and the 2015 Iran nuclear accord are at significant risk, and there are serious doubts as to whether the United States and Russia will extend the 2010 New Strategic Arms Reduction Treaty before it expires in February.
2021. Addressing these and other critical concerns will occupy much of the energy of key figures in the field for some time to come.

As time goes on, however, policymakers will be compelled to devote ever-increasing attention to the military and arms control implications of the technologies identified above and others that may emerge in the years ahead. Diplomatically, these issues logically could be addressed bilaterally, such as through the currently stalled U.S.-Russian nuclear stability talks, and when appropriate in various multilateral forums.

Developing all the needed responses to the new technologies will take time and considerable effort, involving the contributions of many individuals and organizations. Some of this is already underway, in part due to a special grant program on new threats to nuclear security initiated by the Carnegie Corporation of New York. Further more attention to these challenges will be needed in the years ahead. More detailed discussions of possible approaches for regulating the military use of these four technologies will be explored subsequently in ACT, but here are some preliminary thoughts on what will be needed.

To begin, it will be essential to consider how the new technologies affect existing arms control and nonproliferation measures and ask what modifications, if any, are needed to ensure their continued validity in the face of unforeseen challenges. The introduction of hypersonic delivery systems, for example, could alter the mutual force calculations underlying existing strategic nuclear arms limitation agreements and require additional protocols to any future iteration of those accords. At the same time, research should be conducted on the possible contribution of AI technologies to the strengthening of existing measures, such as the nuclear Nonproliferation Treaty, which rely on the constant monitoring of participating states’ military and military-related activities.

As the weaponization of the pivotal technologies proceeds, it will also be useful to consider how existing agreements might be used as the basis for added measures intended to control entirely novel types of munitions. As indicated earlier, the CCW can be used as a framework on which to adopt additional measures in the form of protocols controlling or banning the use of armaments, such as autonomous weapons systems, not imagined at the time of the treaty’s initial signing in 1980. Some analysts have suggested that the Missile Technology Control Regime could be used as a model for a mechanism intended to prevent the proliferation of hypersonic weapons technology.

Finally, as the above discussion suggests, it will be necessary to devise entirely new approaches to arms control that are designed to overcome dangers of an unprecedented sort. Addressing the weaponization of AI, for example, will prove exceedingly difficult because regulating something as inherently insubstantial as algorithms will defy the precise labeling and stockpile oversight features of most existing control measures. Many of the other systems described above, including autonomous and hypersonic weapons, span the divide between conventional and nuclear munitions and raise a whole other set of regulatory problems.

Addressing these challenges will not be easy, but just as previous generations of policymakers found ways of controlling new and dangerous technologies, so too will current and future generations contrive novel solutions to new perils.

ENDNOTES


3. Richard Danzig, Technology Roulette: Managing Loss of Control as Militaries Pursue Technological


8. For background on these systems, see Scharre, Army of None.


11. For discussion of this risk, see Geist and Lohn, How Might Artificial Intelligence Affect the Risk of Nuclear War?


16. For a discussion of possible measures of this sort, see ibid., pp. 35–46.


---

Michael T. Klare is a professor emeritus of peace and world security studies at Hampshire College and senior visiting fellow at the Arms Control Association. This is the first in a series he is writing for Arms Control Today on the most disruptive emerging technologies and their implications for war-fighting and arms control.

Source URL: https://www.armscontrol.org/act/2018-12/features/challenges-emerging-technologies