GLOBAL TRENDS

APRIL 2021

EMERGING OR EVOLVING DYNAMICS

INTERNATIONAL LEVEL

The Future of the Battlefield

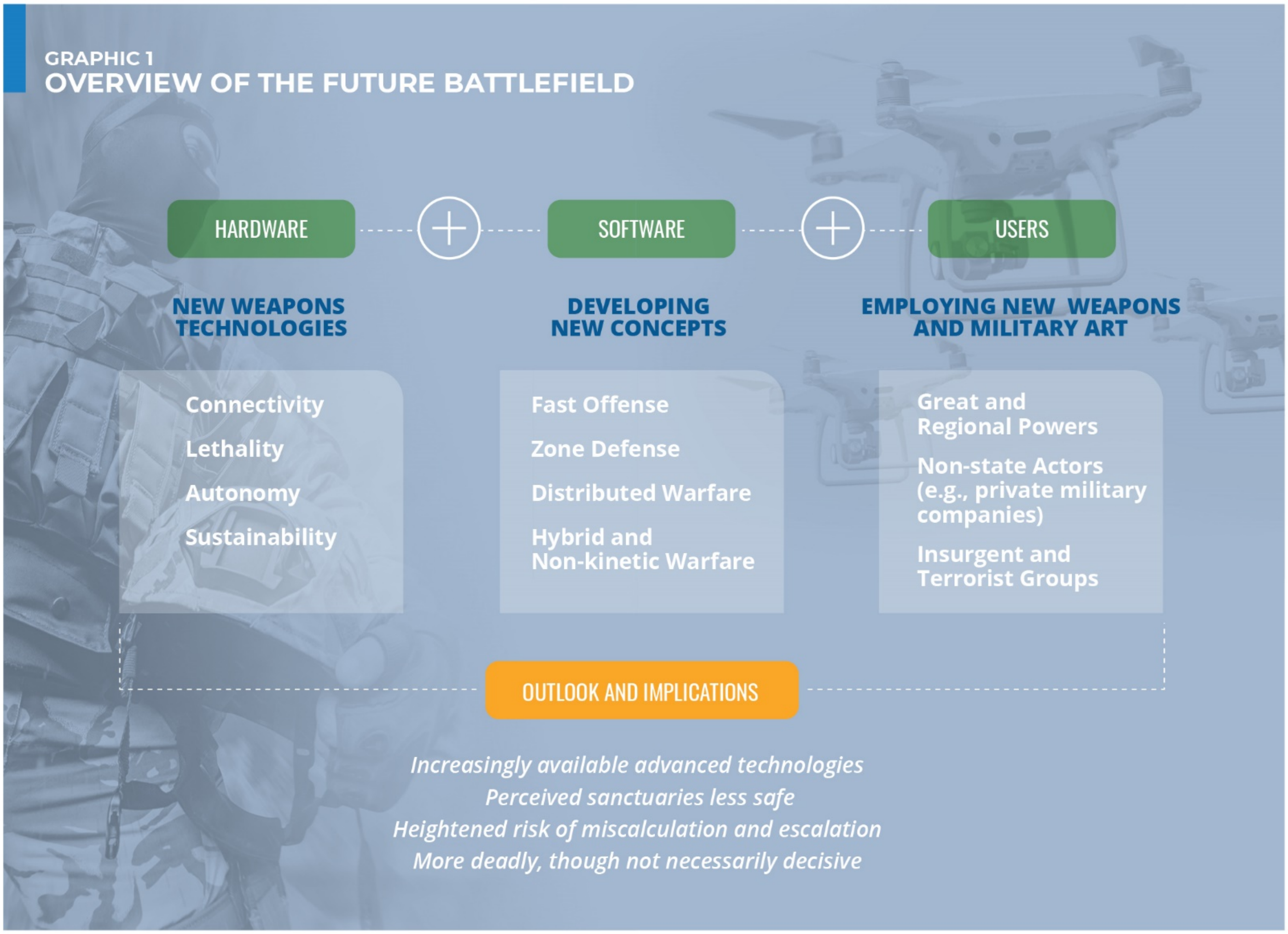
NIC-2021-02493

During the next two decades, military conflict most likely will be driven by the same factors that have historically prompted wars—ranging from resource protection, economic disparities, and ideological differences to the pursuit of power and influence—but the ways in which war is waged will change as new technologies, applications, and doctrines emerge and as additional actors gain access to these capabilities.

The combination of improved sensors, automation, and artificial intelligence (AI) with hypersonics and other advanced technologies will produce more accurate, better connected, faster, longer range, and more destructive weapons, primarily available to the most advanced militaries but some within reach of smaller state and non-state actors.

The proliferation and diffusion of these systems over time will make more assets vulnerable, heighten the risk of escalation, and make combat potentially more deadly, though not necessarily more decisive

This paper was produced by the National Intelligence Council's Strategic Futures Group in consultation with outside experts and Intelligence Community analysts to help inform the integrated Global Trends product, which published in March 2021. However, the analysis does not reflect official US Government policy, the breadth of intelligence sources, or the full range of perspectives within the US Intelligence Community.



GRAPHIC 1

OVERVIEW OF THE FUTURE BATTLEFIELD

HARDWARE + SOFTWARE + USERS

NEW WEAPONS TECHNOLOGIES

Connectivity

Lethality

Autonomy

Sustainability

DEVELOPING NEW CONCEPTS

Fast Offense

Zone Defense

Distributed Warfare

Hybrid and Non-kinetic Warfare

EMPLOYING NEW WEAPONS AND MILITARY ART

Great and Regional Powers

Non-state Actors (e.g., private military companies)

Insurgent and Terrorist Groups

OUTLOOK AND IMPLICATIONS

Increasingly available advanced technologies
Perceived sanctuaries less safe
Heightened risk of miscalculation and escalation
More deadly, though not necessarily decisive

Scope Note: *This assessment focuses primarily on changes in the ways in which wars are likely to be waged and battles are fought during the next two decades, including technologies, doctrines, and actors. It does not address in detail the potential causes or motivations behind future conflicts, nor does it attempt to forecast every potential development in warfare.*

By 2040, a range of potentially revolutionary technologies and novel uses could change the character of how war is waged. We consider these potential changes across three distinct aspects of warfare: **hardware** (the weapons systems and new technologies themselves), **software** (the doctrine, training, and ways these new technologies are used), and **users** (the states or non-state actors employing these weapons and doctrines). For the future of warfare, the applications and combinations of new technologies are as important as the technologies themselves.

- For example, in 1919 it would not have been hard to predict that aircraft, aircraft carriers, tanks, and submarines—all of which were available in World War I—would be used in the next great war. The different ways they would be employed by the various belligerents—each with their own military experiences, perceptions, and traditions—and the technologies which would prevail over others were the real questions, and the ones most difficult to forecast. The same is true today.

HARDWARE: NEW WEAPONS TECHNOLOGIES

During the next two decades, new and emerging technologies could change and potentially revolutionize the battlefield in four broad areas—connectivity, lethality, autonomy, and sustainability.

- **Connectivity:** the ways in which combatants detect and locate their adversaries, communicate with each other, and direct operations;
- **Lethality:** the damage that new weapons and weapon systems can inflict on battlefields;
- **Autonomy:** the ways in which robotics and AI can change who (or what) fights and makes decisions;
- **Sustainability:** the ways that militaries supply and support their deployed forces.

Connectivity

The future of warfare is likely to focus less on firepower and more on the power of information and the way it connects a military's forces through the concepts of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). More than ever, the advantage will lie with whichever side can ***collect*** the most vital information, accurately and quickly ***analyze*** it, and then rapidly and securely ***disseminate*** the information and associated instructions to forces.

The combination of more inexpensive sensors and big data analytics points to a potential revolution in real-time detection and processing of information by 2040. Many of the world's militaries recognize this potential and are already working to capitalize on the power of information to amplify their warfighting strategies and capabilities. They are exploring how emerging technologies, including but not limited to AI, could usher in an era of persistent surveillance and improve their decisionmaking.

- In the contest between those looking to hide their activities—whether at the tactical, operational, or strategic-levels of warfare—and those seeking to identify and track them, the balance by 2040 may shift to the "seekers," as increasingly advanced and accessible technologies provide them with continuous global surveillance capabilities.
- In the undersea domain, for example, a combination of more numerous, improved, and relatively inexpensive sensors with advances in commercially available processing power could make submarines—considered the world's first stealth technology—more vulnerable to detection.

This information edge and the technologies that enable it are also likely to become important targets for adversaries in future conflicts. The more connectivity is seen as a decisive advantage for one side, the more the other will seek to disrupt, degrade, and disable the highly connected, information-dependent systems.

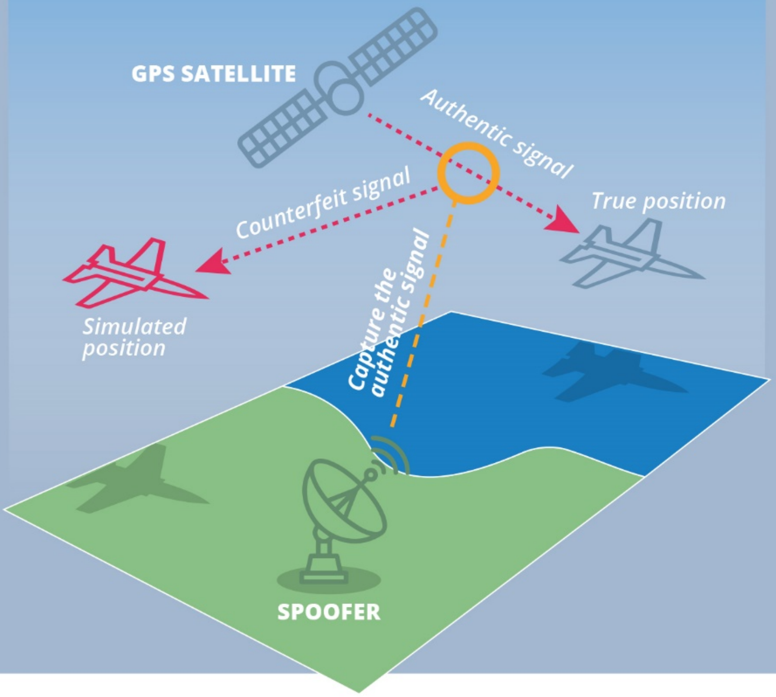
- Such efforts might be focused at the tactical level on using advanced or traditional weapons to eliminate key infrastructure and nodes, or by more subtle—and potentially more disruptive—advanced means, such as cyber or electronic warfare to alter GPS signals to misdirect an opponent's platforms and smart weapons, a technique known as "spoofing." At a more strategic level, cyber attacks and electronic warfare might be used to undermine a military's overall C4ISR infrastructure to confuse or freeze decisionmaking and greatly diminish its ability to fight.
- Modern militaries are particularly vulnerable to any loss of precision navigation, including GPS and its equivalents. For example, in 2010 a software glitch temporarily took as many as 10,000 military GPS receivers offline, affecting systems such as the US Navy's X-47B prototype drone.

GRAPHIC 2

CONNECTIVITY WARFARE: GPS SPOOFING MISDIRECTS PLATFORMS

GPS spoofing involves the broadcast of fake GPS signals to deceive the GPS receivers on aircraft, ships, and other vehicles and equipment, as well as on smart weapons, into misidentifying their actual location.

Such efforts can lure platforms and weapons off course, potentially causing them to stray into neutral or hostile territory or into striking unintended targets.



- C4ISR or other systems, like GPS, that rely on space-based infrastructure probably will be put at further risk by advances in kinetic—and potentially even directed energy—anti-satellite weapons systems, either based on ground or in space themselves.

Lethality

Once an adversary's forces are located by diverse surveillance technologies, increasingly advanced weapons can be used to target them. One of the most significant, ongoing trends in weaponry is the growing combination of high speed, long-range, enhanced destruction potential, and pinpoint accuracy. By 2040, accuracy will be further enhanced by the integration of satellite-provided imagery and positioning, timing, and navigation information in most weapons systems. Such advances will be likely to improve systems capable of striking across continents as well as more tactical weapons, such as guided rockets, artillery shells, and mortar rounds.

- The increasing number and accuracy of such systems by 2040, particularly ballistic and cruise missile systems, will pose a significant threat to headquarters, communications facilities, airfields, logistics infrastructure, and other critical targets.

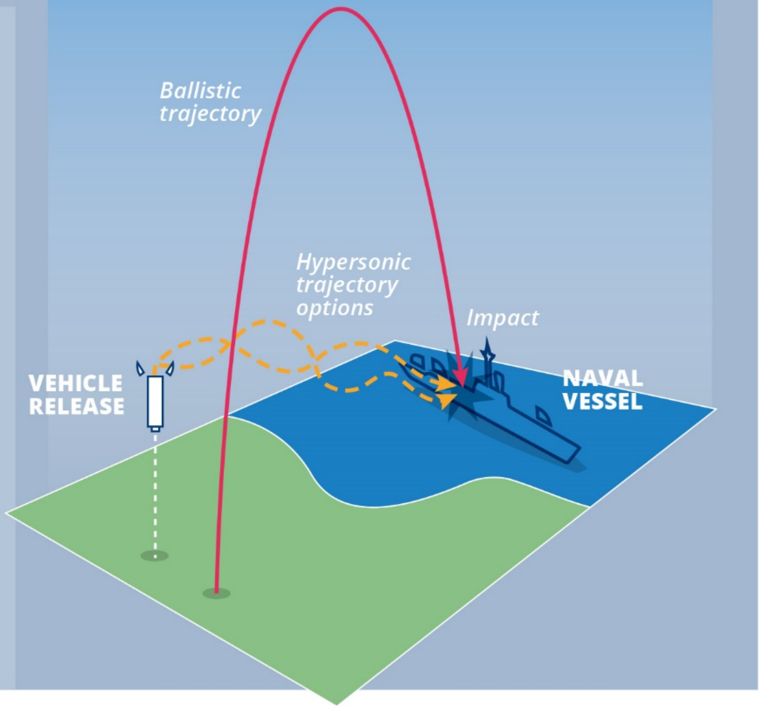
- Long-range precision strike weapons inventories are likely to include increasing numbers of hypersonic systems that can strike targets at great distances with unprecedented maneuverability and speed. These systems will present a daunting challenge for those trying to develop countermeasures that can detect, track, and intercept such fast-moving and maneuvering weapons.

GRAPHIC 3
HYPERSONIC GLIDE VEHICLE TRAJECTORY VS. A BALLISTIC TRAJECTORY

Hypersonic weapons are those that travel in excess of 3,800 miles per hour—five times the speed of sound. Depicted at right is the potential flight profile of one category of hypersonic weapon, a hypersonic glide vehicle (HGV).

Although initially lifted into the atmosphere by a boost vehicle, once released the HGV glides to its target at high speed and is capable of maneuvering throughout its flight. This contrasts to the relatively predicable, parabolic arc of a traditional ballistic missile.

The combination of high maneuverability, precision, and speed will make HGVs a lethal addition to the battlefield. Hypersonic cruise missiles are being developed by various militaries.



Although as yet unproven in combat, directed energy weapons—including lasers and high-power microwaves—may be features of the battlefields of 2040. Whereas long-range precision strike weapons, like hypersonics, hold the potential to revolutionize offense, directed energy weapons could revolutionize defense by, for example, offering an effective means to counter the high-speed and maneuverability of hypersonic weapons. If the challenges of deploying such weapons systems, including energy consumption and replenishment, can be overcome, the cost per shot—delivered at the speed of light—of energy weapons could fall to nearly zero while the rate of fire could theoretically exceed any mechanical system.

- However, even if these weapons are fielded in appreciable numbers during the next 20 years and work as designed, they will still possess inherent limitations. For example, lasers are limited to line-of-sight and may be degraded or defeated by atmospheric obscurants, reflective surfaces, or specialized materials, while high-power microwaves could be defeated by hardening key components of potential targets against their effects.

Autonomy

Autonomous systems and AI are likely to play key roles in the future of warfare because of their widespread applicability to many different functions. Autonomous systems are not new kinds of weapons but are enabling technologies, allowing existing platforms to operate with decreasing levels of human interaction, for extended periods, and in increasingly deadly environments.

WEAPONS OF MASS DESTRUCTION

The threat posed by weapons of mass destruction will remain and may increase as technological advances and the proliferation of knowledge and skills continue. Additionally, Syria's repeated use of chemical weapons and the use of toxic agents by North Korea and Russia for assassinations raise the prospect of "normalizing" the use of such weapons. Meanwhile, nuclear states almost certainly will continue modernizing their nuclear forces, viewing them as a deterrent and a hedge against potential peer adversaries

- **Russia,** for example, is currently partway through a modernization of its strategic nuclear forces, including a new road-mobile intercontinental ballistic missile, a new ballistic missile submarine, an upgraded heavy bomber, and a new bomber intended to carry hypersonic weapons.
- **China** is likely to continue its multiyear effort to modernize its nuclear missile forces, including deploying sea-based weapons, improving its road-mobile and silo-based weapons, and development of hypersonic glide vehicles. These new capabilities are intended to ensure the viability of China's strategic deterrent by providing a second-strike capability and a way to overcome missile defenses.

- **Unmanned Vehicles.** UAVs are already accepted—even assumed—warfighting tools on battlefields worldwide. The next two decades are likely to see greater development and deployment of a host of other unmanned vehicles, ranging from ground vehicles to sea-based surface and subsurface platforms. Such vehicles are ideal for performing mundane, repetitive activities—such as resupply missions for manned platforms—as well as for performing hazardous missions like reconnoitering enemy bunkers and strongpoints, laying or clearing land- and sea-based mines, or searching for submarines.
- **Lethal Autonomous Weapons.** As autonomous technology progresses, some countries may not be concerned about having humans in the loop of firing decisions. As a result, it is possible that by 2040—and despite the associated ethical and legal challenges to their use—truly autonomous, lethal weapons could roam the battlefield and make their own targeting and engagement decisions.
- **Swarming.** Unmanned systems of all types are rapidly becoming more numerous, more capable, and cheaper. Attacks by small swarms of UAVs have already been observed—for example, as US Special Forces troops fought to retake the Iraqi city of Mosul from ISIS in the fall of 2016, they were attacked by at least a dozen armed UAVs dropping grenades and improvised explosives. However, the power of swarming is more than just numbers—swarms of unmanned vehicles could communicate with each other and adjust their tactics and targets as circumstances change.

A Talon 3B robot approaching an anti-personnel mine during a training exercise in Iraq.

ROBOT USE: EVOLVING AND EXPANDING

Robots are now commonly used to assist in mine-clearing and explosive ordinance disposal. Larger, more advanced unmanned ground vehicles are being developed by various militaries to perform a variety of combat and support roles. The US Army, for example, plans to soon begin fielding the S-MET, a robotic "mule" about the size of a small automobile that is intended to haul supplies, weapons, and other gear for infantry units. Such a vehicle would fill a support role performed by actual beasts of burden for millennia.

The development and evolving capabilities of these autonomous systems are closely linked to advances in AI. AI is already used to enhance the performance of a variety of existing weapon systems, such as target recognition in precision warheads, and can be used in support of humans in human-machine teaming, including decisionmaking tools, or as a decisionmaking engine itself. By 2040, military decisionmaking derived from AI is likely to incorporate available space-based data in real-time support to operations.

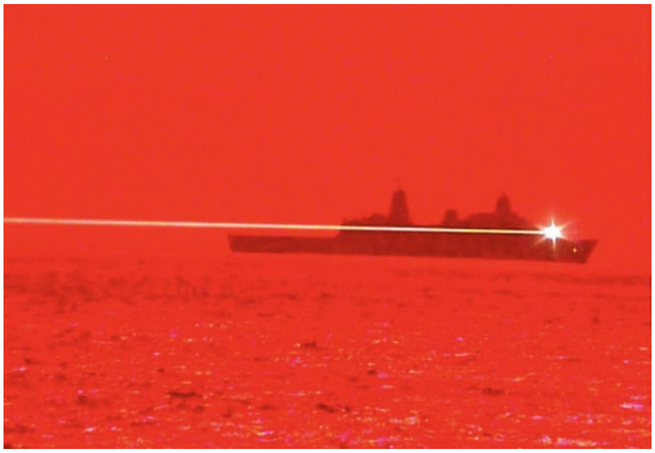
- China, for example, is actively pursuing the use of AI for a wide range of applications, including for information and data analysis; for war-gaming, simulations, and training; and for command decisionmaking. Russian President Vladimir Putin said in 2017 that the nation that leads in development of AI would "become ruler of the world."
- Nevertheless, AI faces technological hurdles and shortcomings that it must overcome to meet its full potential on the battlefield. AI and the machine learning algorithms that underpin it excel at well-bounded tasks but get things wrong if faced with confusing or unexpected input. For example, it is possible to imagine a scenario in which lethal autonomous weapons driven by AI become overwhelmed by inputs in the dynamic and often chaotic environment of combat and either shut down, wander off, or even begin targeting friendly forces.

Sustainability

Finally, other new technologies, specifically robotics, additive manufacturing, biotechnology, and energy technologies are likely to greatly improve military logistics and sustainment.

- **Unmanned Vehicles** could be used for logistical support, making relatively mundane but often dangerous supply runs between rear area bases and forces deployed in the field.
- **Additive manufacturing capabilities**—such as 3-D printing with new materials including advanced metals or ceramics—have the potential to revolutionize military logistics by producing supplies, parts, and perhaps equipment cheaply, quickly, and where they are needed.

- **Biotechnologies** could improve the ability of individual soldiers to fight and survive on the battlefield. Soldiers might use medical devices on or inside their bodies to monitor their fitness status and, as the field progresses, use devices to diagnose health issues or injuries and inject medications—even while in combat.
- **New energy technologies**—such as small nuclear reactors, or high-density electrical power storage—could have an equally transformative effect on logistics and weapon systems by reducing the amount of fuel necessary to operate forward deployed facilities and equipment, or by serving as the power source for future directed energy weapons.



The May 2020 test of a laser weapon system installed aboard the USS Portland (LPD 27). The system successfully disabled a UAV used as a target, according to the US Navy.

DIRECTED ENERGY WEAPONS: POTENT, BUT POWER-DEPENDENT

Lasers and other directed energy weapons (DEWs), as well as rail-guns, under development rely on electrical energy to function. As a result, one potential downside of DEWs is that if they are denied a power source—by, for example, battle damage—they would be rendered inoperable.

SOFTWARE: DEVELOPING NEW CONCEPTS

The ways in which new weapons and technologies are employed on the battlefield will be just as important as the technologies themselves, particularly in determining whether military breakthroughs are truly revolutionary or merely advanced versions of today's military art. Just as new and untried doctrinal concepts were debated before the First and Second World Wars, militaries worldwide are working to develop the doctrine (the "software") for how these new tools of war will be employed—some in novel ways but others reflecting more of an evolution from today's tactics and strategies. There are at least four discrete but not mutually exclusive visions for how actors might employ new weapons and techniques in coming years:

Fast Offense

As a devastating opening salvo, hypersonic weapons, perhaps in combination with more numerous, advanced conventional missiles, could strike an opponent's military and civilian infrastructure near simultaneously before the defenders could mount any kind of response. Because of the range and accuracy of such weapons, the attacker most likely would not have to extensively position forces beforehand, limiting indicators and warning for the opponent.

Zone Defense

While some new technologies appear to favor offense or expeditionary warfare, certain other new technologies appear to provide more help for defense, particularly for small states focused on securing their homeland. For example, unmanned systems today generally require large and expensive airframes to accommodate the engines and fuel tanks necessary to operate far from their home base or loiter for extended periods over foreign or hostile territory. However, if the goal is to maintain situational awareness and defend the airspace, maritime claims, or home territory of a nation, then large numbers of small and cheap unmanned systems may be just as effective.

Distributed Warfare

The proliferation of high-speed and highly accurate, lethal weapons will call into question the survivability of expensive, high-value, and difficult to quickly replace platforms and weapons systems. One potential mitigation strategy could be the further development and implementation of distributed forces and operations.

- The combination of precise geolocation, high-fidelity battlefield awareness, instant communications, and standoff weapons means that militaries by 2040 may no longer need to mass forces in time and space to the extent historically or traditionally deemed necessary to achieve their objectives.

- However, there is a risk that if any of the critical enablers—particularly communications—required to facilitate distributed warfare are damaged, disrupted, or destroyed by hostile action, then a military's overall warfighting system could devolve from an interlinked, cohesive network into a disconnected and broken mosaic incapable of conducting effective combat operations.

CYBER: BOTH WEAPON AND DOMAIN

Cyber attacks that degrade or deny the use of military hardware can render modern military forces at least temporarily unable to perform their mission, even while inflicting minimal casualties or physical damage. During the next two decades, such attacks—perhaps in concert with limited, real-world military operations—may increasingly be seen by some actors as a relatively cheap and effective means to disrupt an adversary.

- Cyber attacks are likely to be increasingly integrated into a combined arms approach to achieve information superiority in future conflicts. Some countries, such as China and Russia, already view military cyber operations during a conflict as part of an integrated information warfare campaign to disrupt opponents' weapons systems and operations by hacking surveillance and weapons guidance systems, command and control networks, and logistics nodes.

- In the lead-up to and during a conflict, countries' civilian infrastructure may also face cyber attacks intended to disrupt daily life and undermine public support by exploiting social divisions and sowing doubt and chaos. Targets for such attacks could include energy and communications sectors, as well as media services.

- Many countries likely would be hard-pressed to mount an effective defense against such attacks because of poor communication and coordination between their militaries and their civilian cyber sectors.

Hybrid and Non-Kinetic Warfare

States are likely to increasingly compete in the “gray zone” using among other things non-official or plausibly deniable proxies, including private military companies (PMCs). Although the use of proxies is not an entirely new phenomenon—much of the Cold War-era competition between the United States and the Soviet Union involved proxy conflicts, deniable forces, and disinformation campaigns—the increasingly hyper-connected environment is changing some of the tools and techniques.

- In addition to actual combat operations undertaken by proxy or otherwise deniable forces, this type of conflict will include a spectrum of non-kinetic actions that could be undertaken either independently or in support of a conventional military component, such as attacks on undersea fiber optic cables, cyber operations, GPS jamming and spoofing, and information operations.

THE USERS: EMPLOYING NEW WEAPONS AND MILITARY ART

Ultimately, the choice of new technologies and the development of warfighting concepts are likely to depend on the unique threat perceptions, strengths, and vulnerabilities of individual actors. Potential actors range from great and regional powers to non-state actors, such as PMCs and insurgent and terrorist groups. National and organizational cultures as well as internal dynamics probably will play a role in how different actors adopt and employ new technologies. The extent to which these actors encourage initiative and innovation or are otherwise open to change is likely to determine their success mastering the full potential of new technologies and doctrines.

Some advanced or emerging technologies—such as hypersonics—may remain within the purview of great powers and wealthier state actors, but relatively low cost and more widely available automated systems and cyber tools could be exploited by lesser powers and non-state actors to achieve high impact and even strategic-level effects. Lesser or rising powers may be more innovative because they have less to lose by taking chances, are less burdened by legacy systems, and can sometimes leapfrog ahead by skipping generations of development or investing in new and untested military or commercial technologies.

- Iran in 2019 demonstrated the ability to creatively weave together different technologies and techniques when it conducted a coordinated, long-range strike on oil production facilities in Saudi Arabia using a combination of armed UAVs and cruise missiles—an attack that briefly shut down more than 5 percent of global oil production and produced a spike in oil prices.

- PMCs, particularly those operating at the behest of one of the great powers and with potential access to the best technologies, also are likely to incorporate advanced weapons and surveillance equipment into their operations. Unfettered by the bureaucracies, doctrines, and traditions of state militaries, it is possible that PMCs might lead the way in identifying new and innovative ways to apply increasingly advanced technologies on the battlefield.

- Insurgent and terrorist groups may try to make further use of advanced technologies as they become increasingly cheap and easy to acquire. Already, it is easy for would-be terrorists to construct or purchase UAVs and adapt them to carry a few pounds of explosives.

OUTLOOK AND IMPLICATIONS

Novel war-fighting technologies have emerged throughout history, often to great acclaim, but only to have limited impact on the battlefield, while others—such as gunpowder—have gone on to have profound effects. Identifying precisely which and to what extent new technologies and techniques will have the most impact on the future character of warfare is notoriously difficult. Nevertheless, the advanced capabilities that are already making appearances on the battlefield, or are on the horizon, point to several trends and potential implications for war, and peace, in 2040.

Increasingly available advanced technologies

Many of the advanced systems that are likely to be developed and deployed during the next 20 years represent proliferation threats. At the ongoing pace of technological change and diffusion, many militarily relevant technologies are likely to become more available and widespread for both states and non-state actors.

- Space technology and services, for example, are inherently dual-use, meaning that advanced, space-based services—such as high-resolution imagery—will be available for military applications as well as civil government and commercial use.
- The proliferation and relatively low cost of technology has already created a particularly low barrier to conflict in cyberspace, enabling small countries or groups to achieve strategic effect without expensive weapons systems and personnel. The application of low-cost cyberspace capabilities also could provide an advantage against technology-dependent nation or organization.
- Given the spread of technology and central role that commercial industry plays in the development of new applications and systems, it is possible to imagine a convergence of dynamics in which a new kind of PMC emerges that provides cutting edge military capabilities—such as robotic weapons and platforms operated by mercenaries—for a fee. This could enable lesser military powers to avoid the cost of developing a modern military and training skilled personnel.

Perceived sanctuaries less safe

Long-range precision strike capabilities mean that areas once thought to be relatively safe from conventional attack because of distance will be increasingly vulnerable, including airfields, assembly areas, and command and control centers. Countries may also face concerted cyber attacks, unbound by geography, against critical infrastructure to disrupt troop movements, cause chaos among the civilian population, and weaken public resolve for military action.

Heightened risk of miscalculation and escalation

The increasing availability of advanced weapons systems and growing employment of hybrid and non-kinetic warfare are likely to further challenge long-held understandings of inter-state deterrence, possibly risking unintended escalation into direct inter-state conflict.

- If hypersonic and other advanced, precision-strike weapons prove to be as effective and hard to defend against as conventional wisdom suggests, these systems could be ideal first-strike weapons. If tensions are high, leaders might feel pressured to strike first out of fear of losing their advanced arsenals of hypersonics and other weapons to an opponent's first strike.
- Increased gray zone activities, even if intended to avoid full-scale military confrontations, introduce another risk variable, particularly as capabilities grow over time. In a confrontation, neither side is likely to be completely sure how the other will react when, for example, state-backed private military contractors are killed in battles or cyber attacks disable critical infrastructure or disrupt an election. In essence, the employment of such methods assumes that the other side will not seek to escalate.

More deadly, though not necessarily decisive

Future conflicts involving great or medium powers could be extraordinarily violent from the outset, yet also protracted and inconclusive. For centuries, adversaries have started wars thinking they had some edge that would enable them to win quickly and decisively. Sometimes they have been correct, but on other occasions leaders who thought they had war-winning technologies or military strategies turned out to be wrong. With the wide variety of new-but-untried warfighting technologies and concepts, it is possible such dynamics will continue to repeat themselves during the next 20 years.

- For historical comparison, Japan's attack on Pearl Harbor in 1941 crippled the US Navy's Pacific Ocean battleship fleet and killed more than 2,400 Americans. In the future, advanced and increasingly lethal weapons could achieve similarly impactful effects and inflict comparable casualties on a nation's armed forces in the opening minutes of a conflict.
- The swiftness and scale of such destruction could lead any country that suffers similar losses in a future conflict to concede or otherwise withdraw from combat because of loss of military capability and confidence, shock over casualties, or a combination that undermine its will to fight. However, it is possible that such apparently decisive losses galvanize a nation to carry on the fight, regardless of cost in blood and treasure, as happened with the United States after Pearl Harbor. Such a scenario might also compel a nation to employ new weapons technologies or novel approaches to warfare that it might not otherwise have considered to try to defeat its opponent.