Center for a New American Security

November 3, 2015

Testimony before the Senate Armed Services Committee Future of Warfare

Paul Scharre, Senior Fellow and Director
20YY Future of Warfare Initiative
Center for a New American Security

Disruptive Change in Warfare

Warfare – the way in which militaries fight – is constantly evolving. Militaries compete in a cycle of innovations, countermeasures, and counter-countermeasures in an attempt to gain an advantage over their enemies. War is a punishing environment, and even a small edge in capability can lead to dramatically different outcomes. A slightly longer-range sensor, missile, or longer spear can mean the difference between life and death. Occasionally, some innovations lead to a major disruption in warfare that changes the rules of the game entirely. Better horse cavalry no longer matter when the enemy has tanks. Better battleships are irrelevant in an age of aircraft carriers. New technologies are often catalysts for these changes, but it is their combination with doctrinal and organizational innovations in war that leads to paradigm shifts on the battlefield. Tanks or aircraft alone might be beneficial, but they require new training, organizations, and concepts for use to create the *blitzkrieg*.

Even while militaries seek ordinary, incremental gains over adversaries, they must constantly be on guard for disruptive changes that revolutionize warfare. This challenge is particularly acute for dominant military powers, such as the United States today, who are heavily invested in existing ways of fighting while underdogs must innovate by necessity.

Are we on the verge of another paradigm shift in warfare? On what timeframe? Is one already underway? And if so, what early conclusions can we draw about these changes? There are two elements driving changes in warfare that will unfold in the coming decades:

The first is the proliferation of existing advanced technologies to a wider range of actors. Even though these technologies already exist, their proliferation to multiple actors across the international system will change the operating environment for U.S. forces. Technologies that the United States has itself used in war, but not yet faced on the battlefield, are finding their way into the hands of potential adversaries. This will force changes in U.S. concepts of operation and capabilities, changes that can be seen in nascent form today but have not yet fully matured.

Bold.
Innovative.
Bipartisan.

Technology does not stand still, however. The information revolution, which has already yielded advances such as GPS, stealth, and precision-guided weapons, continues apace. Advances in autonomy, cyber weapons, data fusion, electronic warfare, synthetic biology, and other areas are likely to drive significant changes in military capabilities. This second driving force – the continued maturation of the information revolution – could lead to even more profound changes in how militaries fight.

The U.S. military must prepare for these changes to come, which will inevitably unfold at uneven rates and in surprising ways. While no one can predict the future, U.S. defense spending represents a *de facto* prediction about what sorts of capabilities planners believe are likely to be useful in future conflicts. Research and development (R&D) and procurement investments often take decades to mature and yield platforms that stay in the force for even longer. The new Air Force long range strike bomber (LRS-B) will not reach initial operational capability for 10 years and will likely remain in the force for decades beyond. The B-52 bomber has been in service for 60 years. This year, the U.S. Navy began laying the keel for a new aircraft carrier, the USS *John F. Kennedy* (CVN-79), which will remain in active service until 2070. These investments represent multi-billion dollar bets that warfare will evolve in such a way that these capabilities will remain useful for decades to come.

Disruptive change is a near certainty over these timescales, however. The twentieth century saw major disruptive changes in warfare in World War I, World War II, the Cold War with the advent of nuclear weapons, and the Gulf War with first-generation information age weapons such as stealth, GPS, and precision strike. Thus, it is imperative that military planners peer as best they can into an uncertain future to try to understand the shape of changes to come.

The Future is Already Here

Science fiction author William Gibson, who coined the term *cyberspace,* has remarked, "The future is already here, it's just not evenly distributed yet." Many of the changes to come in warfare will come not from new technologies, but from the diffusion of existing ones throughout the international system.[1] The resulting difference in scale of a technology's use can often lead to dramatically different effects. A single car can help a person get from point A to point B faster. A world full of cars is one with superhighways, gridlock, smog, suburbia, road rage, and climate change. In war, the battlefield environment can look dramatically different when one technology proliferates to many actors.

There is historical precedent for such changes. At the end of the nineteenth century, the British used an early model machine gun, the Maxim Gun, to aid their conquests of Africa. This technology gave them a decisive advantage over indigenous forces who did not have it. Machine gun technology rapidly proliferated to European competitors, however, resulting in a very different battlefield environment. In World War I, the British faced an enemy who also had machine guns and the result was disaster. At the Battle of the Somme, Britain lost 20,000 men killed in a single day. Their concepts for warfighting had failed to evolve to their new reality.

Today the United States faces a similar challenge. The 1991 Gulf War hinted at the potential of information age warfare. U.S. battle networks comprised of sensors, communication links, and precision-guided weapons allowed U.S. forces to employ great lethality on the battlefield against Iraqi forces.[2] The United States had these advantages because it was a first-mover in the information revolution, capitalizing on these opportunities before others.[3]

Now these same technologies are proliferating to others and the result is a very different operating environment. Thousands of anti-tank guided missiles are in the hands of non-state groups in the Middle East and North Africa. Countries such as China are building long-range missiles to target our bases and ships. Now that others have guided weapons, they can target U.S. forces with great precision, saturating and overwhelming U.S. defenses. Missile interceptors to defend our assets are costly, and the cost-exchange ratios favor the offense.

This vulnerability of major U.S. power projection platforms – our ships, air bases, and aircraft – to precision-guided weapons is particularly unfortunate because it coincides with a long-term trend in decreasing numbers of U.S. major combat systems. For several decades, per unit costs for ships and aircraft have steadily risen, shrinking the number of major combat assets the United States can afford. This trend preceded the current budget crunch and, unless corrected, will continue long after.

To date, the U.S. response has been to make its platforms more capable to offset their reduced numbers. This has further driven up costs, exacerbating this trend. In a world where the enemy has unguided weapons, the United States has been willing to accept this trade. The U.S. has fewer ships and aircraft in its inventory than twenty years ago, but they are more capable.

But in a world where the enemy can target U.S. forces with a high-degree of precision, having a small number of exquisite systems creates an enormous vulnerability, because the enemy has fewer targets on which to concentrate firepower.

The Department of Defense broadly refers to these adversary capabilities as "anti-access / area denial" (A2/AD), because any U.S. forces within their range will be vulnerable to attack.[4] The Department of Defense has launched a new offset strategy to regain American military technical superiority. But the solution to this problem cannot be merely a better ship or aircraft. On the current trajectory, those assets would be even more expensive and purchased in fewer numbers, placing even more eggs in a smaller number of vulnerable baskets.

A more fundamental shift in American military thinking is needed. To operate against adversaries with precision-guided weapons, the U.S. needs to disperse its forces, disaggregate its capabilities, confuse enemy sensors through decoys and deception, and swarm enemy defenses with large numbers of expendable assets.

Early thinking along these lines is already underway in many corners of the Department of Defense. The Army's new operating concept includes dispersed operations for anti-access environments.[5] The Marine Corps is experimenting with distributed operations across the littorals. The Naval Postgraduate School is researching aerial swarm combat.[6] And DARPA's System of Systems Integration Technology and Experimentation program aims to disaggregate aircraft capabilities into a swarm of cooperative, low cost expendable air vehicles.[7]

Collectively, these efforts hint at the next paradigm shift in warfare: from fighting as a network of a few, expensive platforms as we do today; to in the future fighting as a swarm of many, low cost assets that can coordinate their actions to achieve a collective whole. The diffusion of advanced military technology is also increasing the number of actors who can effectively contest U.S. forces in certain domains – undersea, the electromagnetic spectrum, space, and cyberspace. Areas where the United

States has largely had freedom of maneuver to date are now becoming increasingly congested, requiring new U.S. responses.

As the U.S. military adjusts to a world of proliferated precision-guided weapons and adapts its concepts of operation to counter-A2/AD capabilities, it must also be cognizant of even more dramatic changes to come.

The Unfolding Information Revolution

The information revolution has already led to significant changes in warfare by enabling the advanced sensors, communications networks, and guided weapons that led to U.S. superiority and now anti-access capabilities as they proliferate. But the information revolution is not stopping. $3.8 trillion is invested annually in information technology, roughly double all military spending—procurement, R&D, personnel, construction—of every country on earth.[8] While the United States was an early first-mover in information technology, the fruits of the massive commercial sector investments in better sensors, processors, and networks will be available to many.

The scale of this investment, along with the continued exponential growth in computing power, virtually guarantees disruptive change.[9] But in what ways will the continuing information revolution change warfare? Specific military applications may not yet be known, but we can look at underlying trends in what information technology enables. Across the many diverse applications of information technology run three core trends: increasing transparency, connectivity, and machine intelligence.

Increasing transparency

One of the core features of the information revolution is the "datafication" of our world—the generation of large amounts of digital data. Combined with the fact that computers make it virtually costless to copy information, this has resulted in a freer flow of information that is making the world increasingly transparent. Satellite images, once the province only of superpowers, are now available free online. Police and security services have found their activities subject to unprecedented scrutiny and are scrambling to adapt, even in the United States.[10] Even secret government data is not as secret as it once was. According to the U.S. government, Edward Snowden stole in excess of an estimated 1.7 million documents, the largest leak in history.[11] A leak of such scale would have been nearly impossible in a pre-digital era. The Vietnam Era Pentagon Papers, by comparison, were a mere 7,000 pages photocopied by hand.[12] The datafication of our world combined with the ease with which digital information can be copied and shared is leading to a world that is more transparent, with secrets harder to keep on all sides. Sifting through this massive amount of data, particularly when it is unstructured and heterogeneous, becomes a major challenge.

Increasing connectivity

Information technology is increasing the degree of connectivity between people and things, both in terms of the number of people and things online as well as the volume and bandwidth of information exchanged. As the Internet continues to colonize the material world, more objects are increasingly networked (e.g., Internet of things), enabling remote access and information-sharing, as well as making them susceptible to hacking. Social media enables many-to-many communication, allowing any individual to share their story or report on abuses of authorities. The result is a fundamental shift in communication power dynamics, upending relationships between individuals and traditional authorities. In addition, connectivity allows crowdsourcing of problems and ideas, accelerating the pace of innovation and the momentum of human communication.

Increasingly intelligent machines

The rapid growth in computing power is resulting in increasingly intelligent machines. When embodied in physical machines, this trend is allowing the growth of increasingly capable and autonomous munitions and robotic systems.[13] Advanced computing also allows for the processing of large amounts of data, including gene sequencing, enabling advances in "big data," artificial intelligence, and synthetic biology. While current computing methods have limitations and face tapering growth rates, possible novel computing methods, such as quantum computing or neural networks, hold potential for continued growth in intelligent machines.[14]

Six Contests That Will Shape the Future of Warfare

As militaries weigh how to spend scarce defense dollars, they must grapple with the challenge of predicting which attributes will be most valuable in the decades to come. Should they focus on speed, stealth, range, sensing, data processing, armor, mobility, or other areas? All of these attributes are valuable, but which will be most crucial to surviving the conflicts of the 21st Century?

As the information revolution continues to mature, six key operational concepts will shape the future of warfare:

1. Hiding vs. Finding
2. Understanding vs. Confusion
3. Network Resilience vs. Network Degradation
4. Hitting vs. Intercepting
5. Speed of Action vs. Speed of Decision-Making
6. Shaping the Perceptions of Key Populations

These contests are a product of both the proliferation of existing guided weapons, sensors, and networks as well as future advancements in information technology. Militaries will seek to both exploit these technologies for their own gain, finding enemies on the battlefield and striking them with great precision, as well as develop countermeasures to conceal their forces, sow confusion among the enemy, degrade enemy networks, and intercept incoming projectiles. As they do so, information-based technologies will not be the only ones that will be useful. Advances in directed energy weapons or electromagnetic rail guns to intercept enemy guided weapons, for example, have great potential value. But the scale of changes in greater transparency, connectivity, and more intelligent machines will make capitalizing on these advantages and countering adversaries' attempts to do so critical for gaining an operational advantage in the battlefields of the twenty-first century. While militaries will seek dominance on both sides of these contests, technological developments may tilt the balance to favor one or the other side over time.

Hiding vs. Finding

One of the prominent features of information-enabled warfare to-date is the development of precision-guided weapons that can strike ships, aircraft, and bases at long distances. Defensively, this has placed a premium on hiding. Non-state groups seek to blend into civilian populations. State actors increasingly rely on mobile systems, such as mobile air defense systems and mobile missile launchers. Because of these innovations in hiding, offensive operations are often limited by intelligence, surveillance, and reconnaissance (ISR) capabilities. For the past two decades, the United States has been on the offensive side of this exchange. However, adversary developments in long-range precision strike are forcing the United States to think more carefully about concealment strategies as well. Because precision-guided weapons can deliver a high volume of lethal firepower directly on a target, whoever gets the first salvo may decide victory. Getting that first shot may also depend increasingly on one's ability to effectively hide, while deploying sufficient sensors to find the enemy first. The maxim "look first, shoot first, kill first" may apply not only in beyond visual range air-to-air combat, but in all domains of warfare.

One important asymmetry in the hiding vs. finding contest is the ability to leverage increasing computer processing power to sift through noise to detect objects, including synthesizing information gained from multiple active or passive sensors. This makes it increasingly difficult for those seeking to hide because they must conceal their signature or actively deceive the enemy in multiple directions at once and potentially against multiple methods of detection. Advanced electronic warfare measures enable precision jamming and deception, but these methods require knowing the location of enemy sensors, which may be passive.[15] Thus, a contest of hiding and finding capital assets may first depend on a preliminary contest of hiding and finding distributed sensors and jammers lurking in the battlespace. These techniques, both for distributed passive sensing and distributed precision electronic warfare, depend upon effectively networked, cooperative forces, which are intimately linked with other contests.[16]

Certain domains of warfare may have inherent characteristics that make hiding more or less difficult, changing where militaries make their investments over time. Warfare undersea is likely to become increasingly important, as the underwater environment offers a relative sanctuary from which militaries can project power well inside adversaries' anti-access zones. Cross-domain capabilities that allow militaries to project power from the undersea into air and land may be increasingly useful. Conversely, as other nations develop counter-space capabilities, U.S. investments in space are increasingly at risk. During the Cold War, the U.S. and U.S.S.R. had a tacit understanding that counter-space capabilities were destabilizing, since they could be seen as a prelude to a nuclear first strike. However, the era of U.S. sanctuary in space is over as U.S. satellites face an increasing array of threats from kinetic and non-kinetic weapons as well as the specter of cascading space debris.[17] Satellites move through predictable orbits in space and maneuvering expends precious fuel, making them inherently vulnerable to attack. This vulnerability places a premium on redundant non-space backups to enhance U.S. resiliency and diminish the incentives for an adversary to strike first in space.

Technology areas that could enhance hiding or finding include:

- Hiding
    - Adaptive and responsive jamming
    - Precision electronic attack
    - Counter-space capabilities (kinetic and non-kinetic)

    - Metamaterials for electromagnetic and auditory cloaking
    - Cyber defenses
    - Low-cost autonomous decoys
    - Undersea capabilities – submarines, autonomous uninhabited undersea vehicles, and undersea payload modules
    - Quantum encryption techniques (which can sense if the communications link is being intercepted)[18]

- Finding
    - Sensor fusion / data fusion
    - Distributed sensing
    - Foliage-penetrating radar
    - Resilient space-based surveillance
    - Low-signature uninhabited vehicles for surveillance
    - Low-cost robotic systems, including leveraging commercial components for clandestine surveillance
    - Long-endurance power solutions (such as radioisotope power) to enable persistent robotic surveillance systems
    - Networked, undersea sensors
    - Cyber espionage
    - Quantum computing (to break encryption)[19]

Understanding vs. Confusion

As the volume and pace of information on the battlefield increases (including misinformation), turning information into *understanding* will be key. A key contest in war will be between adversary cognitive systems, both artificial and human, to process information, understand the battlespace, and decide and execute faster than the enemy. Advances in machine intelligence show great promise for increasing the ability of artificial cognitive systems to understand and react to information in intelligent, goal-oriented ways. However, machine intelligence remains "brittle." While it is possible to design machines that can outperform humans in narrow tasks, such as driving, chess, or answering trivia, human intelligence far outstrips machines in terms of its robustness and adaptability to a wide range of problems. For the foreseeable future, the best cognitive systems are likely to be hybrid architectures combining human and machine cognition, leveraging the advantages of each.[20]

These technologies also offer the potential for new vulnerabilities, as militaries will attempt to thwart their enemies' ability to understand the operating environment by denying accurate information, planting misinformation, and sowing doubt in whatever information an enemy already has. Deception has been a key component of military operations for millennia and will remain so in the future, and these technologies will offer new opportunities for increasing confusion.[21]

Technology areas that could affect understanding or confusion include:

- Understanding
    - Artificial cognitive systems
        - Advanced microprocessor design[22]
        - Data processing and "big data" analytics

    - Artificial intelligence, neural networks, and “deep learning”
  - Human cognitive performance enhancement
    - Pharmaceutical enhancements, such as Adderall or Modafinil
    - Training methods, such as transcranial direct current stimulation
    - Synthetic biology
  - Human-machine synthesis
    - Human factors engineering and human-machine interfaces
    - Brain-computer interfaces[23]
    - Synthetic telepathy

- Confusion
  - Cyber espionage and sabotage
  - Misinformation, deception, and spoofing attacks
  - Human performance degradation
  - Tailored biological weapons

An important asymmetry between the United States and potential adversaries is the uneasiness with which human enhancement technologies are viewed in the United States. While there are no legal or ethical objections *per se* to human enhancement, they raise many legal and ethical issues that must be addressed. Experiments with cognitively enhancing drugs and training techniques can and have been performed in military labs, meeting stringent legal and ethical requirements.[24] However, there remains a cultural prejudice in some military communities against human enhancement, even for treatments that have been shown to be both safe and effective. The Department of Defense currently lacks overarching policy guidance to the military services to articulate a path forward on human performance enhancing technologies.[25]

Network Resilience vs. Network Degradation

Networking allows military forces to fight as a coherent whole, rather than as individual, non-cohesive units. For the past two decades, the U.S. military has been able to leverage the advantages of a networked force and has largely fought with freedom of maneuver in space and the electromagnetic spectrum. However, military networks will be increasingly contested by jamming, cyber attacks, and physical attacks on communications nodes. Resilient networks that are flexible and adaptable in the face of attacks, as well as doctrine that can adapt to degraded network operations, will be key to maintaining a force that can fight through network attacks. This includes “thin line” redundant backups that may offer limited communications among distributed forces, as well as off-network solutions. While many solutions for network resilience encompass doctrine and training to fight under degraded network conditions, technological solutions are also important to maintain networks under stress. This includes not only communications, but also position, navigation, and timing data, which are critical for synchronized and precise global military operations.

Technology areas affecting network resilience and degradation include:

- Network resilience
  - Protected communications, such as low probability of intercept and detection communications

    - High-altitude long-endurance aircraft or airships to function as pseudo-satellites ("pseudo-lites")
    - Software-defined radios (to allow adaptable communications)
    - Open-architecture communications systems, to allow rapid adaptability of hardware and software to respond to enemy jamming
    - Cyber defenses
    - Autonomous undersea vehicles (to protect undersea communications infrastructure)
    - Lower-cost space launch options
    - Faster-responsive space launch options to replenish degraded space architectures
    - GPS-independent position, navigation, and timing

- Network degradation
    - Improved jamming techniques
    - Offensive cyber weapons
    - Anti-satellite weapons (kinetic and non-kinetic)
    - High-powered microwave weapons to disrupt or destroy electronic systems

Hitting vs. Intercepting

Finding the enemy, understanding the data, and passing it to the right warfighting elements is only a prerequisite to achieving effects on target, frequently from missiles or torpedoes. If "knowing is half the battle," the other half is violence. Because guided weapons can put lethal effects directly on a target, intercepting inbound threats or diverting them with decoys is generally a more effective response than attempting to mitigate direct hits via improved armor. However, missile defense is a challenging task. Missiles are difficult to strike mid-flight, requiring multiple interceptors, resulting in cost-exchange ratios that currently favor the offense.

A number of possible technology breakthroughs could tilt this balance in either direction:

- Hitting
    - Networked, cooperative munitions, including cooperative decoys and jammers
    - Hypersonic weapons
    - Advanced stealth, both for missiles and aircraft
    - Large numbers of low-cost swarming missiles or uninhabited systems to saturate enemy defenses
    - Airborne, undersea, or sea surface arsenal ships or "missile trucks" to more cost-effectively transport missiles to the fight
    - High-fidelity decoys to increase the costs to defenders
    - Long-endurance uninhabited aircraft to enable long-range persistence and strike

- Intercepting
    - Low cost-per-shot electric weapons, such as high-energy lasers and electromagnetic rail guns
    - High quality radars for tracking incoming rounds and guiding interceptors
    - Long-endurance uninhabited aircraft for forward ballistic missile defense, both for launch detection and boost phase intercept

- Persistent clandestine surveillance, from space assets, stealthy uninhabited aircraft, or unattended ground sensors for early detection of ballistic missile launch and pre-launch preparation

The U.S. military has long sought low cost-per-shot weapons such as high-energy lasers and electromagnetic rail guns to upend the missile defense cost-exchange ratio. High-energy lasers have already been demonstrated against slow-moving, unhardened targets such as low-cost drones or mortars. Current operationally-ready lasers are in the tens of kilowatts, however, and scaling up to sufficient power to intercept ballistic missiles would require on the order of a megawatt, more than an order of magnitude improvement.[26] While such improvements are frequently seen in computer-based technologies, laser technology and perhaps more importantly key enablers such as cooling and energy storage are not improving at such a rapid pace. Electromagnetic rail guns, on the other hand, currently show the most promise for defense against ballistic missiles. They require significant amounts of power, however, on the order of tens of megajoules, necessitating more advanced power management systems, similar to those on the DDG-1000 destroyer.[27]

Speed of Action vs. Speed of Decision-Making

Speed has always been a critical aspect of warfare. Understanding the battlefield and reacting faster than the enemy can help in achieving a decisive edge over one's adversary, forcing the enemy to confront a shifting, confusing chaotic landscape. In recent times, this has been instantiated in the American military concept of an "observe, orient, decide, act" (OODA) loop, where adversaries compete to complete this cycle faster than the enemy, thus changing the battle's conditions before the enemy can understand the situation and effectively respond. But the concept is ancient. Sun Tzu wrote, "Speed is the essence of war."[28]

Many emerging technologies have the potential to accelerate the pace of battle even further, including hypersonics, directed energy weapons, cyber weapons, and autonomous systems. Militaries will seek to leverage these technologies and other innovations, such as improved training, doctrine, or organizations, to understand and react faster than the enemy. Nascent developments in these areas highlight a different contest, however – the challenge commanders have in keeping control over their own forces on the battlefield.

The tension between the speed of action on the battlefield and the speed of decision-making by commanders will be an important aspect of future warfare. Disaggregated and dispersed swarming tactics may be valuable for operating within A2/AD areas and decentralized control will push decision-making closer to the battlefield's edge, but this comes at a cost of less direct control for higher commanders. Coordinating action across a widely dispersed battlefield will improve operational effectiveness, but depends upon resilient networks and effective command and control architectures. Different militaries will balance these tensions in different ways, with some retaining centralized control and others delegating decision-making to battlefield commanders.

While this tension between centralized vs. decentralized command and control is not new, an important new dimension to this dilemma is the role of automation. Autonomous systems – robotics, data processing algorithms, and cyberspace tools – all have the potential to execute tasks far faster than humans. Automated stock trading, for example, happens at speeds measured in milliseconds.[29] Autonomous systems will pose advantages in reacting quickly to changing battlefield conditions. They also pose risks, however. Autonomous systems are "brittle" – if used outside of their intended operating conditions, they may fail unexpectedly and dramatically. Automated stock trading, for example, has played a role in "flash crashes," including the May 2010 flash crash where the U.S. stock market lost nearly 10 percent of its value in a matter of minutes.[30] Autonomous systems also may be more vulnerable to some forms of spoofing or behavioral hacking, which also allegedly played a role during the 2010 flash crash.[31] Militaries will therefore want to think hard about the balance of human and machine decision-making in their systems. "Human circuit breakers" may be valuable safeguards against hacking and failures in autonomous systems, even if they induce some delays.[32]

One example area where militaries already face this challenge is in defending against rocket, missile, and mortar attack. At least 30 countries have automated defensive systems to defend land bases, ships, and vehicles from saturation attacks that could overwhelm human operators.[33] These systems are vital for protecting military assets against salvos of guided munitions, but they are not without their drawbacks. In 2003, the U.S. Patriot air defense system shot down two friendly aircraft and its automation played a role in the incidents.[34]

Balancing the tension between the speed of action on the battlefield and the speed of decision-making by commanders is less about specific technologies than how those technologies are used and the training, rules of engagement, doctrine, and organizations that militaries employ. Realistic training under conditions of imperfect information and degraded networks can help prepare commanders for real-world situations that demand decisive, decentralized action. Improved human-machine interfaces and design can also help in retaining effective human control over high-speed autonomous systems.[35] Cognitive human enhancement may also play a role. Ultimately, militaries will have to balance the risks associated with delegating too much authority – whether to people or autonomous systems – and running the risk of undesired action on the battlefield vs. withholding authority and risking moving too slowly to respond to enemy action. There is no easy answer to this problem, but technology that quickens the pace of battle is likely to force it to be an even more significant dilemma in the future.

Shaping the Perceptions of Key Populations

Technologies can aid in the conduct of war, but war is fought by people. Maintaining the support of key populations has always been critical in war. In guerrilla wars and insurgencies, influencing the civilian population is a direct aim of both sides, but even in nation-state conflicts domestic support is crucial to sustaining the campaign. Militaries have often sought, as both sides did in World War II, to sap the will of the enemy population, either through propaganda or even direct attacks.

The radical democratization of communications brought about by social media, the internet, blogs, and ubiquitous smartphones has increased the diversity of voices and the volume and pace of information being exchanged, altering the way in which actors compete to influence populations. In a pre-internet era, mass communications were the province of only a few organizations – governments and major media organizations. Even in democratic countries, there were only a handful of major newspaper and television outlets. Information technology and the advent of many-to-many communications has shifted the media landscape, however. Any person can now gain a nationwide or international following on YouTube, Twitter, or any number of other social media venues. Governments and non-state groups are already leveraging these tools to their benefit. Jihadist videos showing attacks – both for propaganda and instructional purposes – are available on YouTube. Russia has deployed an army of

Twitter bots to spread its propaganda.[36] The Islamic State similarly employs a sophisticated network of human Twitter users to spread its messages.[37]

Various conflict actors, state and non-state alike, will seek to leverage new media tools as well as old media to help spread their messages. While states generally have more resources at their disposal, the net effect of the widespread availability of social media is to increase the relative power of non-state groups, whose messaging tools are now far more capable than twenty years ago. This means that even in conflicts between nation-states, messaging directly to various publics – the enemy's, one's own, and third parties – may be critical to influencing perceptions of legitimacy, victory, and resolve.

Strategic Agility: A Strategy for Managing Disruptive Change

How should the U.S. military prepare for these potential disruptive changes in warfare? While investments in key technology areas are important, the U.S. defense budget is insufficient, even in the best of times, to invest in every possible game-changing opportunity. Moreover, technology alone will rarely lead to paradigm shifts in warfare without the right concepts for use. To sustain American military dominance, the Department of Defense should pursue a strategy of *strategic agility*, with a focus on increasing the DoD's ability to rapidly respond to disruptive changes in warfare.[38] Rapid reaction capabilities, modular design, and experimentation are critical components of achieving strategic agility.

Rapid reaction capabilities

U.S. military forces have evolved considerably since the Cold War, but the nation remains saddled with a Cold War-era bureaucracy that is too sluggish to respond to the pace of change of modern warfare. The DoD's capability development process proved wholly inadequate to respond to emergent needs in Iraq and Afghanistan, necessitating the creation of ad hoc standalone processes and task forces, such as the MRAP Task Force, ISR Task Force, JIEDDO, Rapid Equipping Force, Joint Rapid Acquisition Cell, and other entities.[39] While the specific capabilities that these groups fielded may not be needed in future wars, the need for rapid reaction capabilities is universal. In fact, rapidly responding to enemy innovations is likely to be even more critical in major nation-state wars than in counterinsurgencies, which often play out over longer time horizons and at lower violence levels. DoD should move to institutionalize many of the ad hoc processes developing during the most recent wars and ensure the Department is better prepared for rapid adaptability in future conflicts.

Modular design

Even as DoD pursues more rapid reaction capabilities, major platforms such as submarines, aircraft carriers, aircraft, and tanks will still have lifespans measured in decades. In order to ensure their continuing utility, modularity should be front and center in their design, with the platform conceived of as a "truck" to carry various weapon systems that can be more easily upgraded over time. In practice, this modular design principle is already in use in many weapon systems throughout the U.S. military, from the F-16 to the B-52 to the M-1 tank, all of which have had many upgrades over the course of their lifespan. Some platforms are inherently modular, such as aircraft carriers, which carry aircraft that then project combat power.[40] This principle of modularity, which emphasizes "payloads over platforms" should be expanded to include "software over payloads" as well, allowing rapid technology refresh to keep pace with the information revolution.

Furthermore, modular design can evolve entirely beyond the platform, as the DARPA SOSITE program does, emphasizing the weapon *system* as a collection of plug-and-play platforms that can be upgraded over time. This concept places a greater burden on protected communications between distributed system elements. When successful, however, this concept allows even more rapid technology refresh as individual platform elements can be replaced individually without redesigning the entire weapon system, upgrading combat capability incrementally and at lower cost.

Experimentation

In 1943, Lieutenant General Lesley McNair, then Commander of Army Ground Forces, sent a memorandum to the Chief of Staff of the Army arguing for reducing armor-centric units in favor of making tanks subordinate to infantry. LTG McNair explained that the success of the German blitzkrieg was, in his mind, an aberration and that the proper role of tanks was "to exploit the success of our infantry."[41] The fact that there remained significant debates within the U.S. Army as late as 1943, *after* Germany had decisively demonstrated the effectiveness of armored forces in Europe, shows the importance of doctrine in exploiting paradigm shifts in warfare. New technologies alone rarely accrue significant battlefield advantage if they are not used in combination with new concepts of operation, training, doctrine, and organization.

From a training perspective, the U.S. military currently retains many advantages over potential adversaries; however, that also means others have more room for improvement. When it comes to embracing new doctrinal or organizational shifts, however, U.S. military dominance may actually be a weakness. U.S. organizations heavily invested in current ways of warfighting may be slow to adapt to disruptive changes.[42] A rigorous and deliberate program of experimentation is critical to uncovering new ways of warfighting and breaking out of pre-conceive doctrinal paradigms.

Experiments differ from training or unit qualification as the purpose of experiments is to try new ideas, fail, adapt, and try again in order to learn how new technologies change warfare. The U.S. military currently lacks sufficient depth in experimentation, which is critical to sustaining U.S. military advantage in the face of disruptive change. The ability to rapidly adjust not only the hardware and digital software comprising military power, but also the human software—the training, doctrine, concepts of operation, and organizations—is likely to be the most critical factor in ensuring long-term advantage.

Conclusion

The twentieth century saw a number of major disruptive changes in warfare, with the introduction of machine guns, tanks, aircraft, submarines, nuclear weapons, GPS, stealth, guided munitions, and communications networks all changing how militaries fought in war. The penalty for nations that failed to adapt to these changes was high. While the United States weathered these changes and in many cases led them, future success is not guaranteed. The proliferation of existing advanced technologies around the globe and the continued unfolding of the information revolution will drive further changes in how militaries fight. To be best prepared for the changes to come, the U.S. military should pursue strategic agility, supported by rapid reaction capabilities, modular design, and experimentation to rapidly respond to disruptive change. While the specific shape of the future is uncertain, the need to adapt to the challenges to come is universal.

End Notes

[1] Michael Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics* (New Jersey: Princeton

[2] Max Boot, *War Made New: Weapons, Warriors, and the Making of the Modern World* (Gotham, 2006).

[3] Barry Watts, *The Evolution of Precision Strike* (Washington DC: Center for Strategic and Budgetary Assessments, 2013).

[4] U.S. Department of Defense, *Air-Sea Battle: Service Collaboration to Address Anti-Access & Area Denial Challenges* (Washington DC, 2013).

[5] U.S. Army, *The U.S. Army Operating Concept: Win in a Complex World, 2020-2040,* October 31, 2014, http://www.tradoc.army.mil/tpubs/pams/tp525-3-1.pdf.

[6] Rollin Bishop, "Record-Breaking Drone Swarm Sees 50 UAVs Controlled by a Single Person," *Popular Mechanics,* September 16, 2015, http://www.popularmechanics.com/flight/drones/news/a17371/record-breaking-drone-swarm/.

[7] Defense Advanced Research Projects Agency, "System of Systems Integration Technology and Experimentation (SoSITE)," http://www.darpa.mil/program/system-of-systems-integration-technology-and-experimentation.

[8] "Gartner Says Worldwide IT Spending to Grow 2.4 percent in 2015," *Gartner.com,* January 12, 2015, http://www.gartner.com/newsroom/id/2959717.

[9] Computing power continues advancing at an exponential rate, but the pace of change has begun to decline. See "Performance Development," *Top500.org,* http://www.top500.org/statistics/perfdevel/; and Michael Feldman, "Life Beyond Moore's Law," *Top500.org*, http://www.top500.org/blog/life-beyond-moores-law/.

[10] Scott Calvert, "In Baltimore, Arrests Down and Crime Up," *Wall Street Journal,* May 20, 2015, http://www.wsj.com/articles/in-baltimore-arrests-down-and-crime-up-1432162121. Michael S. Schmidt and Matt Apuzzo, "F.B.I. Chief Links Scrutiny of Police With Rise in Violent Crime," *New York Times,* October 23, 2015, http://www.nytimes.com/2015/10/24/us/politics/fbi-chief-links-scrutiny-of-police-with-rise-in-violent-crime.html?_r=0.

[11] Chris Strohm and Del Quentin Wilber, "Pentagon says Snowden took most U.S. secrets ever: Rogers," *Bloomberg,com,* January 9, 2014, http://www.bloomberg.com/news/articles/2014-01-09/pentagon-finds-snowden-took-1-7-million-files-rogers-says.

[12] Douglas O. Linder, "The Pentagon Papers (Daniel Ellsberg) Trial: An Account," 2011, http://law2.umkc.edu/faculty/projects/ftrials/ellsberg/ellsbergaccount.html.

[13] Robert Work and Shawn Brimley, *20YY: Preparing for War in the Robotic Age* (Washington DC: Center for a New American Security, 2014). Paul Scharre, *Robotics on the Battlefield Part 1: Range, Persistence and Daring* (Washington DC: CNAS, 2014), and *Robotics on the Battlefield Part 2: The Coming Swarm* (Washington DC: CNAS 2015. From a certain perspective, a guided weapon is a simple robot.

[14] Top500.org.

[15] Mark J. Mears, "Cooperative Electronic Attack Using Unmanned Air Vehicles," Air Force Research Lab, Wright-Patterson Air Force Base, http:// www.dtic.mil/dtic/tr/fulltext/u2/a444985.pdf.

[16] Paul Scharre, "Robotics on the Battlefield Part II: The Coming Swarm," 32.

[17] Brian Weeden, "The End of Sanctuary in Space," *War is Boring,* https://medium.com/war-is-boring/the-end-of-sanctuary-in-space-2d58fba741a#.u6i8y2rpd. On the prospect of a runaway cascade of space debris, see Donald J. Kessler and Burton G. Cour-Palais (1978). "Collision Frequency of Artificial Satellites: The Creation of a Debris Belt".*Journal of Geophysical Research* **83**: 2637–2646, http://onlinelibrary.wiley.com/doi/10.1029/JA083iA06p02637/abstract.

[18] This technique is called quantum key distribution. For an overview, see Valerio Scarani et al., "The Security of Practical Quantum Key Distribution," Reviews of Modern Physics **81**, 1301, September 30, 2009, http://arxiv.org/pdf/0802.4155.pdf.

[19] Steven Rich and Barton Gellman, "NSA seeks to build quantum computer that could crack most types of encryption," *Washington Post,* January 2, 2014.

[20] Paul Scharre, "Centaur Warfighting: The False Choice of Humans vs. Automation" (forthcoming). Tyler Cowen, "What are Humans Still Good for? The Turning Point in Freestyle Chess may be Approaching," Marginal Revolution, November 5, 2013.

[21] For example, Sun Tzu wrote: "All warfare is based on deception." Sun Tzu, *The Art of War*, Chapter 1.

[22] Top500.org.

[23] For example, see Nick Stockton, "Woman Controls a Fighter Jet Sim Using Only Her Mind," *Wired,* March 5, 2015, http://www.wired.com/2015/03/woman-controls-fighter-jet-sim-using-mind/.

[24] For example, see Caldwell et al., "Modafinil's Effects on Simulator Performance and Mood on Pilots During 37 H Without Sleep," *Aviation, Space, and Environmental Medicine* (September 2004), 777-784, http://www.ncbi.nlm.nih.gov/pubmed/15460629; McKinley et al., "Acceleration of Image Analyst Training with Transcranial Direct Current Stimulation," *Behavioral Neuroscience* (February 2015), http://www.ncbi.nlm.nih.gov/pubmed/24341718.

[25] For an overview, see Patrick Lin et al., "Enhanced Warfighters: Risk, Ethics, and Policy," January 1, 2013, http://ethics.calpoly.edu/greenwall_report.pdf.

[26] Jason Ellis, "Directed Energy Weapons: Promise and Prospects," *Center for a New American Security* (Washington, DC), April 2015, http://www.cnas.org/sites/default/files/publications-pdf/CNAS_Directed_Energy_Weapons_April-2015.pdf.

[27] Office of Naval Research, "Electromagnetic Railgun," http://www.onr.navy.mil/Science-Technology/Departments/Code-35/All-Programs/air-warfare-352/Electromagnetic-Railgun.aspx; U.S. Navy, "DDG-1000 fact sheet," http://www.navsea.navy.mil/teamships/PEOS_DDG1000/DDG1000_factsheet.aspx.

[28] Sun Tzu, *The Art of War*, Chapter 11. This statement is sometimes translated as "swiftness" or "rapidity" in place of "speed."

[29] Irene Aldridge, *High-Frequency Trading: A Practical Guide to Algorithmic Strategies and Trading Systems, 2nd Edition* (Wiley Trading, 2013), http://www.amazon.com/gp/product/B00B0H9S5K/ref=dp-kindle-redirect?ie=UTF8&btkr=1.

[30] U.S. Commodity Futures Trading Commission and U.S. Securities and Exchange Commission, *Findings Regarding the Market Events of May 6, 2010* (September 30, 2010), 2, http://www.sec.gov/news/studies/2010/marketevents-report.pdf. See also, Torben G. Andersen and Oleg Bondarenko, "VPIN and the Flash Crash," *Journal of Financial Markets* 17 (May 8, 2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1881731; David Easley, Marcos Lopez de Prado, and Maureen O'Hara, "The Microstructure of the 'Flash Crash': Flow Toxicity, Liquidity Crashes, and the Probability of Informed Trading," *The Journal of Portfolio Management*, 37, no. 2 (Winter 2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1695041; and Wes Bethel, David Leinweber, Oliver Ruebel, and Kesheng Wu, "Federal Market Information Technology in the Post Flash Crash Era: Roles for Supercomputing," *Proceedings of the Fourth Workshop on High Performance Computational Finance* (September 25, 2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1939522.

[31] Douwe Miedema and Sarah N. Lynch, "UK Speed Trader Arrested over Role in 2010 'Flash Crash'," *Reuters*, April 21, 2015, http://www.reuters.com/article/2015/04/21/us-usa-security-fraud-idUSKBN0NC21220150421.

[32] Paul Scharre and Michael C. Horowitz, "Keeping Killer Robots on a Tight Leash," *Defense One,* April 14, 2015, http://www.defenseone.com/ideas/2015/04/keeping-killer-robots-tight-leash/110164/.

[33] Paul Scharre and Michael C. Horowitz, "An Introduction to Autonomy in Weapon Systems," *Center for a New American Security*, February 2015, http://www.cnas.org/sites/default/files/publications-pdf/Ethical%20Autonomy%20Working%20Paper_021015_v02.pdf.

[34] John K. Hawley, "Looking Back at 20 Years of MANPRINT on Patriot: Observations and Lessons," *Army Research Laboratory*, September 2007, http://www.arl.army.mil/arlreports/2007/ARL-SR-0158.pdf. Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics, *Report of the Defense Science Board Task Force on Patriot System Performance Report Summary*, 20301-3140 (January 2005), http://www.acq.osd.mil/dsb/reports/ADA435837.pdf.

[35] John K. Hawley, "Not by Widgets Alone: The Human Challenge of Technology-intensive Military Systems," *Armed Forces Journal*, February 1, 2011, http://www.armedforcesjournal.com/not-by-widgets-alone/.

[36] Lawrence Alexander, "Social Network Analysis Reveals Full Scale of Kremlin's Twitter Bot Campaign," *GlobalVoices.org*, April 2, 2015, https://globalvoices.org/2015/04/02/analyzing-kremlin-twitter-bots/ and Lawrence Alexander, "The Curious Chronology of Russian Twitter Bots," *GlobalVoices.org*, April 27, 2015, https://globalvoices.org/2015/04/27/the-curious-chronology-of-russian-twitter-bots/. For an interesting survey of Twitter bot activity and analysis of a specific application, see Stefanie Haustein et al., "Tweets as impact indicators: Examining the implications of automated 'bot' accounts on Twitter," http://arxiv.org/pdf/1410.4139.pdf.

[37] Jared Cohen, "Digital Counterinsurgency: How to Marginalize the Islamic State Online," *Foreign Affairs* (November/December 2015), https://www.foreignaffairs.com/articles/middle-east/digital-counterinsurgency.

[38] Richard Danzig, *Driving in the Dark Ten Propositions About Prediction and National Security (Washington DC: Center for a New American Security, 2011).*

[39] Mine Resistant Ambush Protected Vehicle (MRAP) Task Force; Intelligence Surveillance and Reconnaissance (ISR) Task Force; Joint Improvised Explosive Device Defeat Organization (JIEDDO). For more on these and other rapid capability processes, see Department of Defense, "Report of the Defense Science Board Task Force on Fulfillment of Urgent Operational Needs," July 2009, http://www.acq.osd.mil/dsb/reports/ADA503382.pdf; Christopher J. Lamb, Matthew J. Schmidt, and Berit G. Fitzsimmons, "MRAPs, Irregular Warfare, and Pentagon Reform," *Institute for National Strategic Studies*, Occasional Paper 6, June 2009, http://usacac.army.mil/cac2/cgsc/sams/media/MRAPs.pdf; and Ashton B. Carter, "Running the Pentagon Right," *Foreign Affairs,* January/February 2014, https://www.foreignaffairs.com/articles/united-states/2013-12-06/running-pentagon-right.

[40] Jerry Hendrix, *Retreat from Range: The Rise and Fall of Carrier Aviation* (Washington DC: Center for a New American Security, 2015).

[41] Kent Roberts Greenfield, Robert R. Palmer and Bell I. Wiley, *United States Army in World War II, The Army Ground Forces, The Organization of Ground Combat Troops* (Washington, D.C.: U.S. Government Printing Office, 1947), 319-335, http://www.history.army.mil/html/books/002/2-1/CMH_Pub_2-1.pdf. See also Kenneth Steadman, "The Evolution of the Tank in the U.S. Army," Combat Studies Institute: U.S. Army Command and General Staff College, April 21, 1982.

[42] Paul Scharre, "How to Lose the Robotics Revolution," *War on the Rocks,* July 29, 2014, http://warontherocks.com/2014/07/how-to-lose-the-robotics-revolution/.