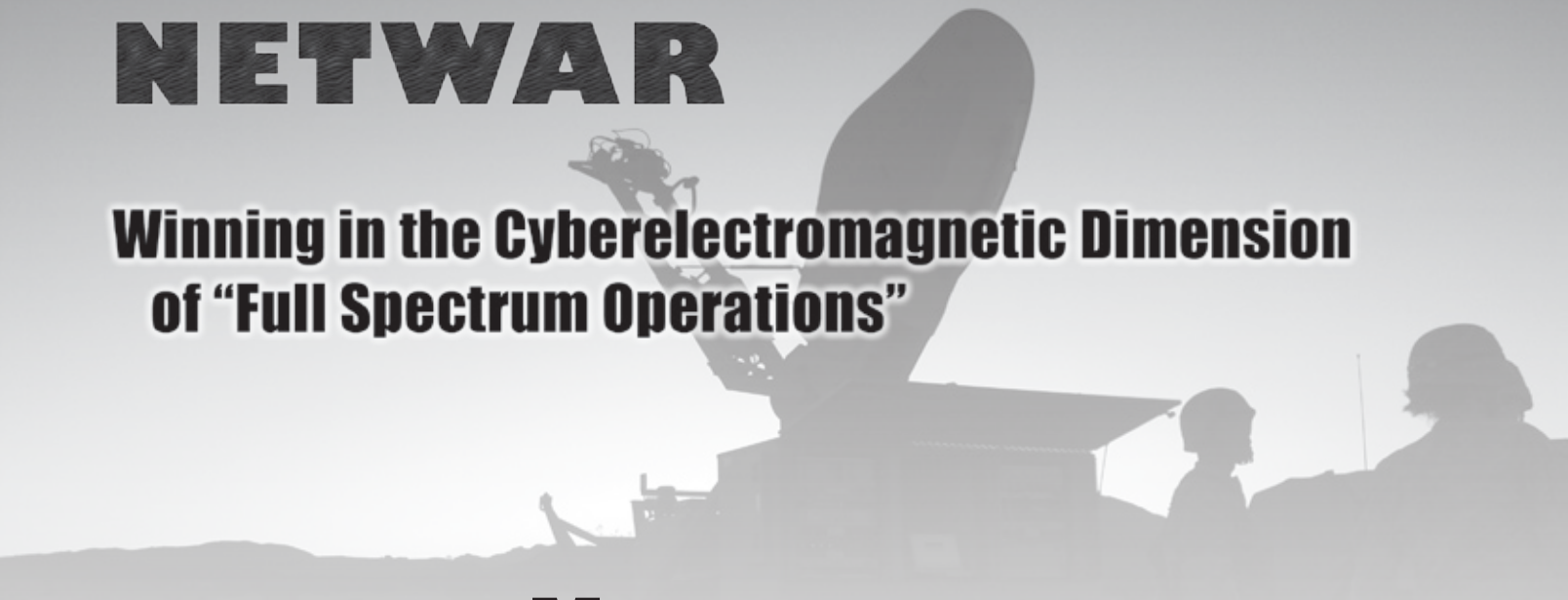
NETWAR

Winning in the Cyberelectromagnetic Dimension of "Full Spectrum Operations"



Brigadier General Huba Wass de Czege, U.S. Army, Retired

MILITARY POWER TODAY has a "moral" or psychological dimension, a public relations dimension, and, significantly, an electrophysical, cyberelectromagnetic dimension.[1] The power of military forces to perform modern missions of all kinds is very much dependent on advantaging its own operations and disadvantaging the various kinds of adversaries it faces in the dimension shaped and bounded by modern communications, information processing, automation, and other rapidly evolving network applications. Just as other complex mission dimensions have their own logic and principles, so has this one.

What makes the cyberelectromagnetic aspect of existence a useful "dimension" is a crosscutting of science and causal logic. Making sense of this dimension for full spectrum operations, and maintaining an advantage in it, requires deeper and more specialized knowledge beyond current expectations. Its significance is changing the way we think about network-enabled military operations, and we must take a broader and more forward-looking view. The art of winning in the cyberelectromagnetic dimension requires deep expertise of a specific and new kind centered on the science of electrophysics, cyberelectronics, complex cyber-network behaviors, *and* how these relate to military tactics, operations, and strategy.[2] Creating this marriage is one key to success, but we must also transform our varied approaches to this dimension into a systemically holistic one.

A Framework of Cyberelectromagnetic Contests

We can organize our thinking about the cyberelectromagnetic dimension into four systemic contests and the science and art prevailing in each:

- The contest between us and our adversaries over what side uses information- and technology-enhanced tools of command more effectively and more reliably (while at the same time applying the counter to it—defeating the other side's effectiveness and reliability).
- The contest of creating and defeating "super efficient" defensive and offensive "integrated strike networks."
- Warring with Internet empowered irregulars.
- The defense of vital local, regional, national, and global information infrastructures.

Brigadier General Huba Wass de Czege, U.S. Army, Retired, was one of the principal developers of the Army's AirLand Battle concept and the founder and first director of the School of Advanced Military Studies, Fort Leavenworth, KS. He holds a B.S. from the United States Military Academy and an M.A. from Harvard University.

PHOTO: U.S. Soldiers from Company C, 79th Brigade Special Troops Battalion, establish satellite voice and data communications for the brigade command post at Fort Irwin, CA, 6 November 2009. (U.S. Army, MAJ Daniel Markert)

Winning the first two systemic contests requires a theoretical understanding of—

- The organizational impact of automation enhanced networks.
- The relationship between information and combat power.
- The theoretical logic underlying assuring the speed efficiency and integrity of our own networks.
- The theoretical logic of "network-centric" combat organizations.
- The theoretical logic for three different kinds of integrated strike networks.

Winning the last two of these four systemic contests requires a theoretical understanding of the reticular nature of the Internet. Attaining the best military outcomes also requires understanding how the Internet relates to operations at all levels. This discussion addresses applicable foundational theories for formulating a holistic perspective for gaining military advantage in these last two contests.

Winning…requires a theoretical understanding of the reticular nature of the Internet.

The Evolution of the Electron-enhanced Military

Since the beginning of warfare, command decisions have depended on knowledge resident in the commander's brain, immediately acquirable by his own senses, or from those within voice contact. As warfare grew in scale and complexity, key decisions began to depend more on information that needed to make its way to the commander's head from beyond his eyesight and hearing. Orders and instructions had to make their way back to elements of the command. Whatever the medium or method of transmission, information could be manipulated, distorted, interrupted, or otherwise attenuated on the way, thus affecting decisions and execution by operational elements. Enemy agents within eyesight or hearing could read uncoded visual and audible signals. Codes could be and were broken. Messengers and dispatches were captured, and systems of message transmissions were destroyed or disrupted. Genghis Khan's 13th-century "Pony Express" system of couriers was the likely zenith of premodern military communication.

The first telegraph was set up in 1844, and the electron entered the stage as a military communication factor. President Lincoln could communicate almost instantaneously with General Grant in the Civil War. Encoding messages became necessary and routine, as were efforts to intercept messages, break codes, and cut telegraph lines. Electromagnetism was harnessed into the functioning of intelligence, battle command, logistical systems, and fire support. At this last point, the electron began to enhance combat functions and the power to influence operations.

When Marconi's "wireless" radio invention enabled message transmission through the "ether" just before World War I, the possibilities for commanding far-flung and rapidly moving military elements exploded. By World War II, wireless messages made it possible to coordinate operations and logistics of rapidly moving columns and to provide key intelligence instantaneously. Without Marconi's invention, combat power of tanks, trucks, motorized artillery, and aircraft would not have been nearly as dramatic. Signals intelligence and jamming radio signals were also born during this time, as was radar, the use of electromagnetic radio waves to detect moving objects. Radar also spawned "chaff" and other electronic countermeasures. By the mid-20th century, not only could electronic science provide very effective sensors, but also new computing ability replaced the human in the loop between sensing targets and aiming weapons.

The introduction of digital automation opened a third chapter in the story of military communications. At first, electronic computing enhanced the productivity of firepower, but gradually this new technology transformed all military functions and became an important enabler of everything military. By the 1970s computers were extensively deployed in fire control systems of artillery and air defense batteries, as well as in individual tanks and aircraft. By the early 1980s the U.S. armed forces were rapidly entering the "digital age," and now we live in a world of information technology-enhanced networks of great variety and scope where even individual Soldiers use automated information systems.

The Internet has thus become an important channel for military command and staff information

exchange at various levels of classification, providing text, voice, still images, and streaming video. Militaries today are heavily reliant on information technology and information systems to communicate, control forces, coordinate fires, gather and distribute intelligence, conduct surveillance and reconnaissance, and other military activities. Irregular adversaries, warring factions, and criminal cartels have access to many of the same technologies and the funds and entrepreneurial spirit to harness these kinds of capabilities. Being at the leading edge in these technologies is far less important than being most clever in adapting to unique conditions. How these technologies are integrated and employed in specific circumstances will greatly affect modern conflicts.

When the military intelligence branch was established in the late 1960s, the Army chose to establish electronic warfare detachments within military intelligence companies and electronic warfare companies within military intelligence battalions. The Soviets, on the other hand, took a more aggressive stance, establishing separate radio electronic warfare battalions and electronic deception units. They thought of these as weapons system organizations and shadow maneuver units. We thought of these as a hybrid between intelligence gatherers and weapons systems. Even when we formed "combat electronic warfare and intelligence" battalions, we combined intelligence and electronic warfare functions in the same unit. Our equipment tended to be multi-functional, as an economy, and we viewed it as military intelligence assets, even though, by doctrine, electronic warfare was coordinated by the operations officer.

Library of Congress

Marconi wireless school, New York. Operators copying messages transmitted from ships at sea, 1912.

U.S. Army, PFC Melissa Stewart

U.S. Air Force SSGT Jeremy Emond operates the Virtual Secure Internet Protocol Router, Non-secure Internet Protocol Router Access Point, and other internet provider systems at Combat Outpost McClain, Afghanistan, 14 October 2009.

…when we formed "combat electronic warfare and intelligence" battalions, we combined intelligence and electronic warfare functions in the same unit.

The paradigm of the 1980s and early 1990s, called Command and Control Warfare, focused on the tactical attack and defense of military infrastructures. The main emphasis was on command posts, the communications between them, and electronic sensors linked to command posts. This view was not *wrong*, it was just too *limiting*. It didn't conceive of integrating the attack and defense of computer systems already widely deployed throughout military networks.

By the mid-1990s, thinkers in militaries everywhere wanted to conceptualize more broadly. Initially, they were looking through the lens of warfare among advanced states, and they saw militaries building networks of automated weapon systems and elaborate command posts filled with computers. Such visionaries saw militaries enabled by advanced communications and spy satellites; they saw modern nation states becoming as dependent on information infrastructures as the most advanced 20th-century states were on industrial and transportation infrastructures. Some even saw the state-controlled broadcast media of an enemy state as a worthy target of disruption and manipulation. Incorporating a new discipline of computer network operations appeared inevitable.

The U.S. military invented the notion of "information operations" (IO). Others used different but similar terms. The focus of IO eventually became dominating an "information domain," achieving "information superiority," and "decision superiority" by combining technical superiority and psychological operations in a mission statement: "influence, disrupt, corrupt, or usurp adversarial human and automated decisionmaking, while protecting our own."

This way of thinking is naively over ambitious and an awkward intellectual construct, one that combines very different psychological and cyberelectromagnetic dimensions. It conflates the causal logic of human and automated decision making. Each is complex in different ways, and by focusing only on decision making, such framing is too limiting.

While "decision superiority" is one way to achieve operational advantage in this dimension, there are other ways to advantage our own operations while disadvantaging adversaries we may face. For instance—

- How do information technologies and the nature of the information they provide enhance combat power?
- What are useful systemic strategies and principles for safeguarding and securing our information-age technological advantages?
- What are useful strategies and principles for creating and defeating other-than-general-purpose command and control networks, such as highly efficient defensive, offensive, and protective "strike" networks?
- What are useful strategies and principles for denying stateless adversaries the unfettered use of the Internet to organize, recruit, propagandize, and attack?
- What are useful strategies and principles for denying state and stateless adversaries the ability to use the Internet to manipulate or destroy national and global civil information infrastructures?

Automation-enhanced Networks and Combat Power

Information technology-enhanced battle command can greatly increase combat power. Used effectively, information technologies empower the command and control structures of the force to deal with uncertainty, react to change, and recognize and exploit opportunities. They reconfigure processes and change the nature of work. The right combinations of information technologies can provide a commonly shared situational awareness, more real-time relevant information, automatic situation updating, and better planning aids. In modern forces, individual platforms can become less important than the "net work" that enables cooperative engagement tactics, facilitating high-tempo operations. The commander's combined arms capabilities can thus be employed much more synergistically.

Information and combat power. That "information is power" has become cliché—the assumption is that more information leads to more power to influence things indirectly. Such conceptions are misleading. Understanding the logic and principles

That "information is power" has become cliché…Such conceptions are misleading.

of *how* modern information capabilities can influence action is what matters. The relevant question is: how does information affect combat power? Combat power cannot be understood in absolute terms or quantities. It has meaning only in a relative sense—relative to that of the enemy—and has meaning only at the time and place where outcomes are determined. Leaders and the forces of their environment, to include the actions of the enemy, transform capability into a balance of relative power that influences outcomes.[3]

Information relevant to the mission and internally consumed by the command contributes to mission success when it enables sound decisions, empowers force, informs maneuver, and provides protection. Likewise the lack of relevant information, or misinformation, can disadvantage the enemy, inhibit his force, disorient his maneuver, and make his forces vulnerable. More specifically, only relevant information informs pending choices and reveals new ones. Only relevant information empowers. In this way, relevant information affects mission outcomes in the physical dimension.

Information projected outward and well-informed public relations can also retain the support of home public sponsors of the mission and the people in the area of operations.[4] Likewise, information projected outward and used by savvy commanders can intimidate, demoralize, mystify, mislead, and surprise adversaries.[5] In both cases, adversaries and other publics do not make choices on the basis of the information willfully beamed at them. Instead, they make their choices through perceptions formed first on the basis of the command's actions, then its reputation, and lastly its explanations or promises. In every such case, such perceptions are influenced from many other directions in many complex ways—by culture, education, and word of mouth from trusted members of society.

This complex milieu not only demonstrates the importance of relevance but also of relevance to specific functions and purposes. The way relevant information has to be fed to specific cells of the organizational body by capillaries of the circulatory system matters. This understanding demonstrates a vital two-sided contest for relative superiority in knowing what is pertinent in a given situation. In this milieu, depriving the enemy of relevant knowledge is as important as gathering such knowledge about the enemy. Being able to gain superiority in relevant knowledge is thus as much dependent on situational factors as it is on satellites, sensors, analytical processors, and staff efforts.

For example, before an ambush is sprung, only the ambusher knows what is truly relevant and thus has relative information superiority. Only seconds before the ambush is activated, those ambushed think they possess relevant knowledge, but in a well-laid ambush the shock of surprise results in complete disorientation. As the ambush evolves, relevant information transfers to well-prepared and well-trained defenders who can, assuming combat power shifts to their advantage, transition properly and defeat the ambush.

Organizing for action. Once situational factors are understood and taken into account, having the right technical tools makes the difference. Some information factors can contribute to the command's fund of relevant knowledge, and others deduct from the enemy's. Understanding that dynamic is enough to organize for action while expecting the unexpected. Concepts of operation that depend on certainty usually fail. Commanders who assume an informed degree of uncertainty, even when they believe they are well informed, are more likely to absorb and adapt new information and therefore succeed. Assuming "information superiority" should thus never be a prerequisite for action because it leads to acting from a posture of "certainty." There is no way to be certain, ever, because one can never know what the enemy knows or thinks.

In all cases, commanders will need to make relative judgments of how well informed they are and act accordingly. The great advantage of being "well informed" is being able to act "deliberately." The word "deliberate" in Army doctrine means the command understands the situation and the opportunities and difficulties it will encounter well enough to focus the bulk of its resources toward producing an optimized outcome quickly, keeping a relatively small portion of his force uncommitted for contingencies. Deliberate actions can generate the greatest impact, with greatest likelihood, in the least amount of time. An important byproduct of this condition is that the command can prepare for better optimized follow-on actions. The more that actions of a campaign are a chain of deliberate actions, the more swift the positive result.

The complexities of current mission contexts and the nature of our adversaries make becoming "well informed" very difficult. We therefore have to organize to avoid traps, enable rapid learning, and respond effectively to both unexpected difficulties and opportunities. "Hasty attack" and "hasty defense" are doctrinal terms that derive from an era when time in contact with the enemy was the prime cost of information. Modern technology can inform commanders well before they come into physical proximity to an enemy. Thus the term "fighting for information" came about. However, even in modern times, engagement can be a prerequisite for gaining relevant information, especially when fighting irregulars. Well-organized actions in such situations become more informed and deliberate as the engagement progresses.

In other words, how a command organizes its overall operations in its mission environment conditions how much relevant information it needs, and conversely, how much information it has conditions how rapidly and efficiently it can make progress. Army forces must operate competently on any point along the scale between being well enough informed to act deliberately and those more frequent cases when they need to engage without being well informed.

Recent improvements in command systems may not expand the likelihood that organizations will *begin* engagements in deliberate rather than hasty settings, but they should accelerate the *transition* from hasty to deliberate responses when the command is inevitably surprised.

Complications and complexity. The missions of modern military forces combine hidden *complications* and obscure *complexity*. Differentiating between these two kinds of impediments when seeking to become well informed is critical. The differences can condition not only how operations should be organized but also how modern information technologies can best help.

Complicated adversary systems may be well hidden, but they are separable from their environment and can be sensed using technical sensors from a standoff. Deduction and modern analysis can lead to understanding, but modern technical sensor systems linked to automated analytical tools and decision aids more easily accelerate learning about them. Thus deliberate actions against them are more likely today than in former times.

Complex systems, on the other hand, are made up of dynamic, interactive, and adaptive elements that cannot be separated from interaction with their environment. The elements of complex systems we care most about are human communities, tribes, towns, or countries. To make sense of such difficult to understand systems, we mentally impose logical structures, our understanding, over them. These creations of our mind may be in the form of conceptual maps or narratives, and these understandings should never be mistaken for reality. They may be the best basis for acting we have, but they are also hypotheses that require testing. Creating such hypotheses requires induction, abduction, and synthesis that computers are incapable of reaching or mimicking. The best way to test any hypothesis is by the scientific method of falsification. It takes more than stand-off technical intelligence to falsify our theories about complex human systems. It takes actual human interactions to learn about them. Such human systems are therefore difficult to understand well enough to engage deliberately, and modern technical sensor systems have difficulty accelerating the rate of appreciating them. Learning from "out of contact" is impossible, and thus deliberate operations are likely impossible. In such environments, learning while operating will most likely be as much the object of operations as gaining mission ends.

Production and appreciation of relevant information is as much an art as science. Because we can never banish uncertainty in any mission involving systems of human beings, the art of learning involves a skeptical testing of the logic underlying our framing of the mission problem in one part of our brains while we act decisively to solve it with the other. However, this practice and the skillful use of modern command and information systems can manage and mitigate uncertainty, and it can greatly accelerate recovery from surprise. While the operational payoff for being well informed has always been high, it is far higher for organizations equipped with modern information technologies because they can make much better use of the relevant information that exists under such conditions.

The Logic of "Network-centric" Combat Organizations

Exploiting the revolution in surveillance, fire control, precision munitions, automated analysis,

fusion of information, and data manipulation will lead to "network-centric" rather than "platform-centric" combat organizations. In the past, armies have been prudent to take platform-centric organizational design approaches because individual combat platforms tended to become isolated in the chaos of combat. Cooperative engagement tactics are universally valued, but, even so, it has been important to equip platforms so they can survive to fight without outside assistance. Equipping organizations so that each platform can survive in isolation means redundancy, and that translates into bulkier and heavier platforms.

In theory, if platforms can avoid isolation and maintain mutual support during a fight, then they can share some capabilities, and that translates into less overall bulk and weight for the same level of performance. The same principle applies to combat units at any echelon. Having a common operating picture and ultra-reliable communications could greatly enhance cooperative engagement tactics from the basic unit upward. This means that the combat power output of tactical organizations could increase dramatically, but it can also collapse when the network fails.

The potential for network-enhanced cooperative engagement tactics is now being introduced into the Army's brigade combat teams, following the lead of Stryker brigades. However, passive armor is unlikely to become obsolete in ground units because it will be difficult to ensure covering fires, suppression, and active protection within the team during worst-case ground combat scenarios. When speed and rapid, decisive results are important, the potential for chaos and loss of mutual support will go up, and the value of passive armor will go up as well. Organizations originally based on platform-centric principles can be transformed into network-centric organizations by upgrading command and control, sensor suites, and munitions. Such upgrades may not reduce the bulk and weight of the organizations or change their appearance, but they will dramatically enhance their combat power (and, incidentally, increase cargo capacity).

Even though the Army's Future Combat System brigades have been cancelled, they presaged ground combat organizations built from the ground up on network-centric principles. Surviving elements of the envisioned brigades, for instance the central networks, will still enter service in brigade combat teams as they become available. Planners envision a robust command and control network to reliably connect the many complementary platform components together. Such a network will greatly enhance teamwork, mutual support, and mutual protection under any conditions. However, the logic of network centricity remains sensitive to mission conditions that affect beyond-the-platform assistance and active defenses. These network-enhanced platforms will be more effective in some environments than others, so applying one kind of unit design to all missions is unlikely. Different designs may be necessary to work effectively in some conditions.

U.S. Air Force, TSGT Efren Lopez

U.S. Soldiers with the 4th Battalion, 23d Infantry Regiment, 5th Brigade Combat Team, 2d Infantry Division, and Afghan National Army soldiers conduct a combined patrol in the village of Shabila Kalan, Zabul, Afghanistan, 30 November 2009.

While modern complex environments may limit the absolute trade-off between traditional passive protection and the automatic active defenses of a network-centric system, beyond-the-platform external assistance will be more reliable than not having such a network at all. The various complementary capabilities distributed throughout the organization can combine to make the unit much more potent and much more survivable in a wide variety of tactical settings. Applying network-centric principles to all unit designs will have universal benefit.

Integrated "strike networks." An integrated strike network is any network specifically designed to engage an enemy with lethal and destructive force. We face a major challenge that we need to understand far better than we do: how to build reliable integrated strike networks while understanding how to incapacitate and defeat those of a hostile adversary. The challenge is not only how to incapacitate and defeat current insurgent wireless networks, but also anticipated future enemies possessing technical savvy and ample resources.

Integrated strike networks have been with us for some time, if we only think of them that way. In the late 1980s the Soviets saw "strike complexes" as the next major military development. They meant the synergistic combination of sensors, connected to processors, connected to decision makers, connected to various lethal, destructive and suppressive weapons, served by robust networks, and *tuned to a specific purpose*.

Soviet theoreticians of the 1980s differentiated between "surveillance strike complexes" and "reconnaissance strike complexes" depending on whether the strike network served a primarily defensive or offensive aim. These are useful distinctions. The former, like integrated air defenses and artillery counter-fire systems, are passive or reactive. They automatically react to the initiative or intrusion of an adversary. The latter, on the other hand, are proactive. An active reconnaissance element of the strike network locates specific high-value targets based on available intelligence: for example, "Scud hunting" operations in the wars with Iraq. They can also be mobile, providing overwatch to advancing forces. Think of "shaping fires" operations in offensive campaigns. This theory is adaptable to irregular force applications as well. Improvised explosive devices and suicide bombers are really elemental building blocks of surveillance and reconnaissance complexes.

Under this rubric, the 1980s-era division artillery with its digitally linked batteries, automated fire control, networked radars, and other sensors was a strike complex that could be configured either as a "reconnaissance strike complex" or as a "surveillance strike complex," depending on whether the mission was defense or offense. Similarly the integrated elaborate air defenses of industrialized armed forces are also "surveillance strike complexes." The improvised explosive devices our Soldiers are encountering are relatively simple strike networks as well. So are the systems the Army has deployed in Iraq and Afghanistan to speedily counter mortar fire.

The power of integrated strike networks derives from the combination of the very short time from initial sensing to striking (making it more likely dynamic targets are engaged) and from the precision and potency of the strike.

A decade from now, the possibilities for various kinds of integrated strike networks will explode. Civilian wireless networks are rapidly expanding around the world, and both wireless technology and computer processors are being integrated in more commonly available devices daily. The very technologies most likely to proliferate soonest will prompt rational opponents fearing attack to defend from "urban web" defenses covered by integrated defensive strike networks. Savvy irregulars, for instance, will use rapidly proliferating technologies to deny access to large cities (or specific urban neighborhoods), jungle and mountain redoubts, and their base areas.

Logical modes of strike networks. Integrated strike networks can be organized to function in three different logical modes:

- Reactive strike defending fixed sites.
- Proactive strike in offensive operations.
- Reactive strike actively protecting mobile assets.

The logic of efficient and rapidly reactive defensive integrated strike networks differ in design and logic from that of a reactive strike network designed for active protection of a mobile platform or mounted formation. A different design logic also applies to a proactive integrated strike network intended to pick apart key elements of a defense. The latter two both support offensive operations.

Understanding these differences in logic is as important to creating and operating platforms as it is to defeating them. In some cases networks are specialized to work only in one of these three logical modes; in other cases integrated strike networks can adopt more than one logical stance, but not at the same time. Shifting from one stance to another consumes time.

Reactive strike defensive. Though highly effective, the logic of a "surveillance" or defensive strike network is relatively simple, consistent, and *predictable*. Any penetration of the area of surveillance of

a defensive strike network is immediately identified "friend or foe," an engagement decision is made, the best available response is selected, targeting data is sent to the responding weapon system, the target is engaged, damage is assessed, and the cycle may repeat again if required. This entire "kill chain" can be automated, or it could contain human nodes as sensors or decision makers. Some elements could be very "low tech."

The Army's long-established and well-functioning counter-battery system integrates long-range radars, automated fire control, and firing batteries in "quick fire" loops. Well-planned defenses for most of the last century included such rudimentary defensive strike networks. Their sensors were forward observers or manned radars linked by radio or telephone to fire direction centers. These were further linked to aircraft or to cannons on the ground or afloat. The replacement of analog with digital technology greatly speeds the "kill chain," and renders it far more efficient.

However, the more important point is that this concept has great potential at every level in and across the services. Theoretically, we could establish systems at every level to respond instantly to every *recognizable* hostile phenomenon. The science of automatic target recognition is advancing rapidly. This application of technology has the potential for strengthening defenses to a remarkable degree, especially in circumstances in which target discrimination is not a great concern.

Proactive strike offense. We should also expect our opponents to exploit this concept. All future offensive actions could be supported by offensive networks with reconnaissance elements initiating the kill chain. Such networks can be reliably keyed to finding and destroying specific key components of the enemy's system of defense. Such proactive systems can also carry out deliberate ambush-like engagements with devastating effects on the enemy. The greatly expanded ability to acquire, track, and process more targets at greater ranges will make it possible for proactive offensive systems to strike many discrete targets that comprise the essential elements of an opposing military formation or functional grouping, *all at once*.

Equally important will be a planning mind-set that sees target sets in terms of their systemic significance. This mind-set merely requires the adaptation of the principles of "target value analysis" developed by the Army artillery school in the early 1980s. This approach to "deep battle" targeting was used to identify the highest payoff targets in a large force array based on our knowledge of enemy doctrine, the context of the engagement, and the mission of the friendly force.

There are great advantages to employing precision weapons in large numbers and within compressed timeframes. The concept of "time-on-target" artillery strikes is not new. The advantage of precision fires is greatest against unwarned enemy formations or fixed sites. Their effectiveness against mobile forces begins to degrade rapidly once the enemy is warned and begins to evade. Such evasion greatly increases the difficulty of subsequent targeting.

Suppression. Modern forms of suppression will also be important to integrate within offensive strike networks. In military parlance, "suppression" proactively degrades human actions and organizational functions of the enemy sufficiently to provide temporary advantages to the attacker. We will need to suppress the enemy's capabilities when we can't assure lethal effects or destruction, or when lethal and destructive means don't serve our purposes. The success of close combat offensive actions in urban and fortified areas especially depends upon effective suppression. During the assault phase of such operations, Marine and Army infantrymen need it to survive while they close on enemy positions.

Today, ground combat forces depend mostly on the blast and flying steel byproduct of lethal munitions for close combat suppression. Precision lethal munitions are too expensive for suppressive fires. In the short run, high explosive "dumb" munitions (that are less expensive but are heavy) provide what is called "area coverage," which indiscriminately causes great amounts of collateral damage in urban combat. If more scientific resources and funding were devoted to this important niche requirement, we could have suppressive munitions that greatly reduce collateral damage and the potential for casualties on both sides. By being more efficient, they could also consume less cargo capacity.

The shock of deliberate ambush-like (very compressed time frame) precision engagements described above also magnifies suppressive effects.

…we could have suppressive munitions that greatly reduce collateral damage and the potential for casualties on both sides.

This would be even more so if suppressive munitions can be interspersed with precise ones. Thus the enemy could be presented with an overwhelming problem that would cause even more rapid and complete organizational collapse, allowing ground assault by smaller forces with fewer casualties.

Reactive strike mobile protection. Offensive operations also will depend on *reactive* protection systems. These are in essence a mobile variant of defensive strike networks. An ever-increasing danger for advancing air or ground maneuver is entering the effect zone of an enemy's defensive integrated strike network. Any potential opponent could cover prepared defense at every echelon with difficult-to-spot sensors and hidden observers that are networked to indirect surface and air defense weapons.

A two-pronged approach is required to avoid unacceptable casualties when these kinds of defenses cannot be outflanked and there is insufficient opportunity to reduce these with standoff means only. Over-watching offensive integrated strike networks could find and dismantle the most vulnerable elements of the enemy system ahead of the advance. However, this will usually be insufficient and will need to be accompanied by a layering of reactive protection systems that are rapid counter-fire systems set to react immediately to defeat any source of missile, artillery, mortar, or rocket fire. Relatively close-in reactive protection from long-range, high-caliber, direct-fire systems is also possible. These can certainly be organized today to support attacking network-centric air and naval formations. These principles also apply to tactical combat formations on land.

One of the great dangers to mobile ground tactical units will be encounters with hidden dismounted infantry armed with simple anti-tank weapons, or direct-fire systems hidden in "keyhole" positions. In these cases both active and passive protection alone could be insufficient. Classical over-watch techniques using vehicular optics and direct-fire weapons also could be insufficient. However, combining these with a system of over-watch that is capable of sensing the first enemy shot, locating the source, and immediately engaging it with a combination of lethal precision and suppressive effects could be sufficient to limit casualties and permit more rapid advances. If the enemy came to understand that any shot fired at the friendly unit could result in an immediate and deadly response, he would be greatly deterred.

While some portions of these capabilities have been demonstrated in recent combat situations, we have also seen failures. Failures tend to be at the beginning and end of the "kill chain" (target identification and damage assessment) when human eyes are replaced with technical sensors and when firing decisions are based on inadequate discrimination. Reactive protection systems will also have problems finding the source of missiles without predictable trajectories—like cruise missiles. These are issues that will eventually be resolved, but so far we have been generous in funding "shooters" and far too miserly in funding the networking and sensing capabilities to make these systems reliable. The full potential of modern organizations can only be achieved when vital networks are functioning.

Network speed, efficiency, and integrity. This empowerment of modern military forces bears a price. Some are concerned that tactical wireless networks and global positioning systems can be jammed, communication services can be denied, precision munitions' aim can be disrupted, and entire networks can fail when system-level databases are attacked or network control structures suffer hostile exploitation. New benefits incur new risks and vulnerabilities, but these are well worth bearing when the cost of mitigation is far less than the value of benefits.

Automation-enhanced networks cannot provide advantage if risks and vulnerabilities are not mitigated. There are many ways the enemy could impede the speed, efficiency, and integrity of our networks and information processing capabilities, and we could do the same to theirs. In fact, the force that doesn't tend to both sides of this equation is at a disadvantage.

Assuring the speed, efficiency, and integrity of our automation-enhanced networks requires a holistic approach. It also requires a broadly assigned but

Assuring the speed, efficiency, and integrity of our automation-enhanced networks requires a holistic approach.

specific set of responsibilities with increased leader awareness and education. It thus will require a new and rigorous way of thinking. New and more functional rules are needed for a time when the power of a byte of information has a very short half-life. When information is pushed far forward, within a small window of time, and to a specific tactical element not normally privy to the product of highly classified sources, clarity and rigor are paramount. Networks and information processing capabilities are an obvious Achilles' heel, and the challenges of safeguarding our communications and network processes, and thus our secrets, are rapidly increasing.

Operations security and information assurance are old problems made more difficult by operating amongst indigenous populations, in widely scattered deployments, and across great distances. Rapid appearance of newer technologies compounds associated difficulties. The Army has managed a challenging analog-to-digital transformation only within the last decade and while at war. Another major wave of change is already underway to replace the new generations of systems with leap-ahead technologies derived from the Future Combat System program's advanced networks. These will replace voice radio and telephone services with "voice-over-Internet protocol" and add many useful web-based automated processes and services. Such advances depend on the reliability of billions of lines of software code.

Command attention, unit "SOPs" (standard operational procedures), "training to standards," and strict adherence to discipline are the first lines of defense. The important disciplines of "operations security" and "information assurance" must become rigorously foundational habits and a matter of command interest at all levels. At the institutional level, the computer network defense side of computer network operations, and the science and art of signals security as it applies to the new communications technologies, will become higher priorities.

As new priorities enter into the design of command systems, they too must be robust and not prone to catastrophic failure. When systems fail they should fail "gracefully," and according to a logical design that assures the reliability of core functions first. Thus, the systemic capabilities that enable self-defense in a crisis must be the most robust and least prone to fail. Next in importance are the systemic capabilities and attributes that enable mutual support within an integrated defense. Next would be assuring the ability to conduct limited offensive operations. Last in priority would be assuring the more ambitious capabilities that enable independent and "distributed" offensive operations.

In this schema, units at the lowest level are responsible for the least-sophisticated threats, and, as the levels of sophistication and difficulty increase, the responsibilities are echeloned upward. As reliant as the Army has become on its rapidly evolving and complicated information "system of systems," and as tempting as their disruption is to adversaries, much institutional intellectual energy has been invested toward meeting this challenge. Issues of maintaining system reliability are as important in education and training as is the art of gaining the most benefit from them. A balance has to be struck between providing functionality and applying safeguards, and a healthy tension is needed between creative approaches and common-sense considerations.

Become Master Cyber-Soldiers

This transformational bargain is analogous in some ways to the transformation from foot- and animal-powered transport to modern mechanized forms of mobility. While the new modes of transport greatly empowered armies, they also introduced great new vulnerabilities. The price of that transformation was also significant: much greater and more elaborate logistical efforts requiring new kinds of knowledge, skills, discipline, and habits as well as new areas for command attention.

Addressing the quandaries of mechanization required understanding the logistical dimension systemically. While many observers of the First and Second Gulf Wars marveled at the display of modern information-technology enhanced operations, they should have been awed by the mastery

U.S. Army, SGT Jeffrey Alexander

U.S. Army CPT Aaron Pearsall, commander of Delta Company, 1st Battalion, 501st Infantry Regiment, 4th Brigade, 25th Infantry Division, coordinates with his platoon leader, during a joint patrol, led by Afghan National Army soldiers in Sabari, Afghanistan, 17 January 2010.

of modern mobility and logistics. General H. Norman Schwartzkopf's "Hail Mary" maneuver, and General Tommie Franks' two-prong dash for Baghdad could not have occurred before every commander in the chain understood what he had to do "systemically." All the component actions and relationships had to be understood holistically—not only the integrated flow of parts and supplies but also the protection of the convoys in the flow and the supply discipline and preventative maintenance practiced by the maneuvering force. Commanders had to become "master logisticians."

As difficult as the transformation to machine power was, the benefits were worth the price of making the system of transport robust and effective and learning how to operate, supply, and maintain it properly. The challenge of doing the same for this new form of 21st-century empowerment is no more daunting than it was for earlier habits of thought. It took time for understanding to sink in then, and it likely will now again.

However, analogies can be more instructive by exploring the differences. Whereas the advantages of mechanized mobility were obvious, and primarily affected one major element of combat power (tactical and operational maneuver), the advantages of automation-enhanced networks are subtle and pervasive. This makes understanding how to gain advantage and mitigate risks all the more difficult. Commanders *must* become systemically savvy masters of the craft in far less time.

Actual and potential adversaries are becoming practiced and ever-more clever in this field. Even though we now have the technical and tactical lead, we could fail to transform the knowledge we have at these levels into strategic advantages in future conflicts. We know how to design, install, operate, and maintain the most advanced automation-enhanced networks in the world, and we know how to defeat any extant integrated air defense system and military or governmental command and control system.

We also have world-class technical and tactical experts in designing, installing, operating, and maintaining automation-enhanced networks in electronic warfare, computer network operations, electronic and cyber-military deception, information assurance, and operations security. But we still think in terms of separate wireless or cyber-system attack and defend tactics. We separate the fields of experts who create and operate our advanced networks from the experts who destroy and manipulate the enemy's. Realities of these emergent technologies demand that we elevate thinking now from narrow technical and tactical compartments to the operational art of thinking in terms of a systemic whole for full spectrum operations. Getting to that level requires thinking critically, creatively, and systemically about this contest.

Critical thinking in this dimension depends on paying close attention to the hard facts and new realities unfolding rapidly before our eyes. It also depends on identifying the currently relevant, definitive ways to achieve operational advantage in this dimension and constructing sound theories that sufficiently describe and explain the logic of cause-and-effect so as to predict and control outcomes to our advantage.

Constructing sound *new* theories for gaining advantage is also a matter of creativity. By understanding how we arrived at current ways of thinking—and challenging the categories, paradigms,

conventions, and definitions that currently pattern and trammel our thought—we can facilitate creativity. The real world of this dimension is changing very rapidly, and thus we should not be limited by outmoded ways of thinking, ones that may have been useful even ten years ago. The only purpose of such artificial mental constructs is to make sense of the real world. When old constructs are no longer helpful, we should abandon them and create more useful ones.

"Cyberwar" is a catchy term, but it lacks theoretical validity. It unnecessarily limits our reasoning to hidebound notions of tradition, suggesting old naval and airpower analogies of controlling or dominating a military "domain." Conceptually separating what happens daily on the Internet from what happens in the kinds of networks I have addressed ignores their connection and would therefore be unrealistic and dangerous. Denying terrorists and extremists unfettered ability on the Internet is a high priority. The speed, ubiquity, and potential anonymity of Internet media make them ideal communication channels for militant groups and terrorist organizations.

Denying adversaries of whatever kind the ability to attack our Internet accessible national financial, transportation, power generation, and other information infrastructures in times of war is another national priority. Some thinkers in foreign lands advance the notion of "active defense" and even preemptive attacks attributable to others in case of threat. Others see such capabilities in their possession as powerful deterrents. There is no doubt that Army forces should play a part in defense of our strategic infrastructures and in counteroffensives against adversaries who attack them. ***MR***

"Cyberwar" is a catchy term, but it lacks theoretical validity. It unnecessarily limits our reasoning…

NOTES

1. It is useful to think of "dimensions" of operations when a specific set of ways to advantage operations share significant amounts of common causal logic and rest on a common scientific foundation. But unlike a "domain" such as air, land, sea, or space in which separate operations, or even campaigns, are conceivable, operations in a dimension are inseparable from the operation-as-a-whole.

2. Just as it is necessary to understand human psychology and human social behavior to succeed in the art of unifying physical and psychological impact, and that of keeping friends and winning allies, knowledge in these fields is crucial to this art. The first term, electro-physics, is the root science that defines this field. Cyber-electromgnetics is a term I prefer over "Cyber space" to cover the science that bounds and defines modern communications, including the Internet. Cyber space is a term that suggests a boundless dimension, like outer space. The modern system of communications called the Internet may seem boundless to the uninitiated, but it is not. And it can be mapped and understood. Moreover, the character of modern operations is so shaped by these sciences, and the enabling capabilities that stem from them that to not consider these a "dimension" would be limiting.

3. This conception of military mission relevant power, the ability to influence, is based on a model developed by the author in 1976 in a paper entitled "Understanding and Developing Combat Power." This thought model was adopted by the U.S. Army in the 1982 version of Field Manual 100-5, *Operations*. This useful theoretical construct was inexplicably dropped from U.S. doctrine about ten years later.

4. See "Keeping Friends and Gaining Allies" in the May-June 2009 *Military Review* for more detail on the theories for informing publics to maintain the support of those at home and gaining the support of those relevant to success in the area of operations.

5. See "Unifying the Physical and Psychological Dimensions of Operations" in the March-April 2009 *Military Review*. It articulates sound and useful theories for influencing the human decision making of actual or potential adversaries in the modern context.