CYBERWAR TAKES SHAPE

Potential trumps problems, but command, control and employment are undefined

DAVID A. FULGHUM/WASHINGTON

Continuing development of cyber-weapons and experimentation with digital warfare are triggering optimism and the occasional operational U-turn.

In a few years, the U.S. Army, Navy and Marine Corps expect to be delivering airborne electronic fires and cyber-attacks for ground troops with a fusion of and Marine Corps expect to be delivering airborne electronic fires and cyber-attacks for ground troops with a fusion of radio battalions, EA-6B Prowlers, EA-18G Growlers and a range of UAVs.

Who actually commands and controls the technology operationally and strategically remains an open question. The uncertainty was illustrated by the formation of Air Force Cyber Command, followed by its months-long pause in bureaucratic limbo and, finally, its re-designation as a numbered air force under U.S. Strategic Command. The institutional tangle was compounded because the services have still not produced a unified plan for electronic warfare and attack. It also contributed to because the services have still not produced a unified plan for electronic warfare and attack. It also contributed to two failures to get the Air Force back into electronic attack with an EB-52 long-range (80-100-naut.-mi.) standoff electronic attack aircraft. The design included the capability to electronically map and attack enemy networks.

"It's not about putting iron on targets anymore; it's about fighting the networks," says a U.S. EW specialist and senior technology officer. "But there is the difficulty that no one has owned cyberwarfare in the past. Now with the massive [cyber] attacks on Estonia and Georgia, it's a real threat and nobody has the charter [to combat it]."

"The organizations and lines of responsibility are still being worked," agrees Lt. Gen. Dave Deptula, the Air Force's deputy chief of staff for intelligence, surveillance and reconnaissance (ISR). "Let me be honest, we're still at the stage of understanding what cyber is. Cyber-operations broach everything from the tactical to the operational to the strategic. How it is used determines what it is.

"My opinion is that we need to normalize operations in cyber just as we've normalized operations in other domains," he says. In an air ops center, "cyberwarfare ought not to be something in a special box that is conducted somewhere else. It needs to be part of the equation in determining a regional contingency plan in equal fashion just like air, space, mari- It needs to be part of the equation in determining a regional contingency plan in equal fashion just like air, space, maritime and ground components."

As cyber- and electronic attack technologies emerge, it is becoming harder to distinguish between cyberwarfare, directed energy and electronic attack, intelligence gathering and information operations. Rationalization of all these elements also is complicated by shrinking manpower and funding.

Meanwhile, there is the new concept of "hybrid warfare," a term coined by U.S. Joint Forces Command. Characteristics of hybrid war are a "very dynamic, uncertain environment [that creates] a lot of change and persistent conflict," says Vice Adm. Robert Harward, the deputy commander of USJFC. The command's operational predictions include increasing dependence on unmanned sensors and aircraft and small fighting units that will employ directed-energy and cyber-weapons.

What the military will look like in 10-15 years "is a little bit of a mystery and may be a little bit of a secret," Defense Secretary Robert Gates told troops in Southwest Asia. But the conflicts in that region are producing templates for future combat—in particular, "the marriage of combat operations and ISR, the ability to dwell over a target, and the ability for relatively small units to have situational awareness of what's going on [around them]," he says. "I think this use of ISR and the integration of intelligence and operations is something we will see continue. This is revolutionizing the way we fight."

Gates bemoans the fact that in some areas first-world nations are already falling behind the insurgents. "How did we end up in a place where the country that invented public relations is being out-communicated by a guy in a cave? Partly, we are still operating too much in a 20th century mind-set."

Air Force officials managing the intersection of ISR, cyberwar, directed energy and information operations echo that concern.

"We need new capabilities to deal with [the enemy's use of advanced technology]," says Deptula. But making the job more difficult is "more demand and fewer resources," he adds. "So we've got to come up with some new approaches. What makes the most sense, given that we're [also] reducing in size?" Part of the answer is high-speed technologies—such as cyberwarfare and high-power microwave (HPM) weapons, he says. But learning to employ them and assign responsibility for their use is still a work in progress.

"As we move from speed-of-sound to speed-of-light weapons, we're beginning to see the changes required to deal with cyber-operations," says Deptula. "HPM is going to be another game-changing capability. We're not there yet, but . . . those capabilities are coming out of ISR, so we have to move rapidly to adapt our organizations to integrate those kinds of weapons. What's critical is to create the command relationships and authority to capitalize on those weapons and not restrict their capabilities.

"Every service ought to have some sort of cyber-component that organizes, trains and equips to how they present force capabilities for combatant commanders," he says. "Then we have a common definition that each of the services can shape to operationally fit their basic core competencies for conduct of military operations in a regional scenario."

As these capabilities are introduced, joint operations are expected to undergo fundamental changes.

"We see a [future] environment that is very much focused on distributed, decentralized, leader-centric and network-enabled [units and] structures [placed] throughout the joint forces," says Harward, who is a Navy Seal and former director of special reconnaissance and direct-action missions in Afghanistan and Iraq. Those special ops-like units will be trained to "have the ability to operate with the commander's intent when systems fail and they can't get information," he says.

Joint Forces Command also embraces the quick introduction of advanced weaponry.

"Everybody recognizes that electronic fires [such as jamming, directed energy and cyberwar] is a capability that ought to be bought, maintained and developed," says Harward. "It's part of the technology advantage that we have

right now, and our ability to expand it will pay dividends. We're looking at it in the experimentation phase and how we might move forward."

Training for the hybrid war also is likely to look different. Planners want high-fidelity, fighter aircraft-like simulators for ground soldiers so that responses to attacks, ambushes and other encounters are well rehearsed before anyone is thrust into combat. Simulators would also allow operational lessons learned to be immediately fed back into the training.

However, researchers are worried that pieces of the digital puzzle are still missing—in particular, projection of new threats that foes may throw at the U.S.

"As you go into a new theater of operations, you see [advanced communications and new uses for networks] pop-up everywhere," he says. "The threat is there, ad hoc, undefined and asymmetric. So you have to stand up your capability quickly to defend and fight your networks. It's changing the way we think about deploying software-defined radios [for example]. We're using common modules that have software functions that are adaptable in real time as the threat changes."

There also are no digital weapons that can be used by nonspecialists, and there is no ability to duplicate networks so attacks and exploitation can be planned and practiced. As a result, the Defense Advanced Research Projects Agency awarded seven six-month contracts totaling about $25 million as startup funding for a National Cyber Range (NCR). The move is being applauded by military officials, who shared their insights into the effort.

It would be the nation's premier cyber-test facility. Candidates would have to provide a complete, integrated system, and Darpa will not act as the integrator.

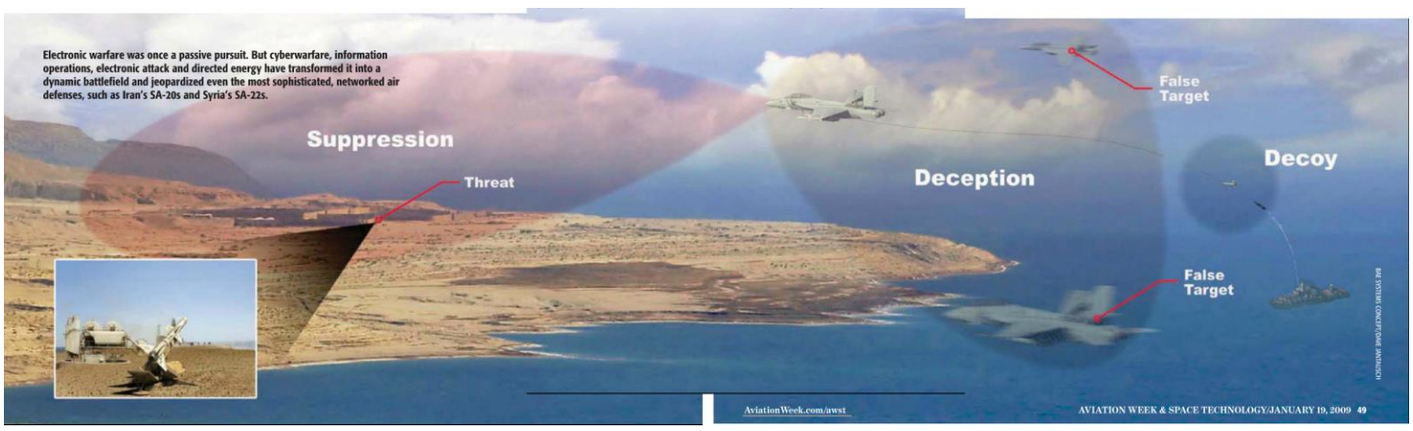
Test analyses are to be unbiased and quantitative assessments of information assurance and survivability tools. The laboratory is to replicate complex, large-scale networks for current and future Defense Dept. weapons and operations.

The capabilities to be tested are host security systems, local-area network security tools and suites, wide-area network systems operating on unusual bandwidths, tactical networks (including the problematic mobile ad hoc networks) and new protocol stacks.

To further hedge their bets, Darpa officials may fund multiple teams to simultaneously build competing prototype NCRs. Testing of the ranges will include demonstration of "packet capture" and automated attacks. Flexibility and adaptation will likely be the key concept to winning the technology wars, just as it is in conventional combat.

"We don't know if knocking down more walls in the intelligence [world], conducting cyber-operations and introducing nonkinetic weapons like HPM are going to be sequential problems, or if they will all arrive together," says Deptula.

"I'd like us to accelerate our ability to meet some of the challenges we have with directed-energy weapons because they certainly will be game-changing," he adds. "Once a capability is fielded and begins to be employed, there's a lot to learn between what was anticipated and what actually takes place. Our organizations must evolve accordingly."



Electronic warfare was once a passive pursuit. But cyberwarfare, information operations, electronic attack and directed energy have transformed it into a dynamic battlefield and jeopardized even the most sophisticated, networked air defenses, such as Iran's SA-20s and Syria's SA-22s.