



When the network dies

The Army lacks the battle drills that would help it fight on

BY LT. COL. MICHAEL J. LANHAM

Unprepared soldiers are ineffective soldiers, and the rise of the networked battle space has made this ancient wisdom no less true.

It is curious, then, that when the Army practices operating in contested cyberspace environments, it does so largely in echelons above corps and not throughout the force. What exercises do take place generally understate the likely effects of network outages and overstate our ability to adapt to them.

If we continue to avoid rigorous rehearsal for cyber attack, or fail to implement it at all levels, we are training to meet incompetent adversaries and setting the stage for improvised, ill-coordinated and ineffective responses to competent ones.

Just as the Army has done for every other aspect of combat, it needs to develop a set of battle drills for such environments and work them into the standard training regimen at each echelon of command. These drills must include individual and collective tasks of the sort that would prepare soldiers, commanders and units to face many varieties of cyber events: short- and long-duration, point and pervasive, man-made and natural. To make this practical, we must also give units at all levels the modeling and simulation capabilities they need to hone their defenses, responses and training efforts.

WHAT WE DO

What are our current capabilities and willingness to conduct rigorous rehearsals of operations in contested cyberspace environments?

Before addressing that explicit question, we should acknowledge that there are certainly concerns with authority to conduct rehearsals — unlike tankers skirmishing at the National Training Center, cyber warriors often hone their craft on the actual Internet — but I'll defer such a discussion and presume there are safe, legal, moral and ethical ways of getting better at our jobs.

We should also properly frame what we wish to accomplish. I'm going to borrow an idea from Maj. Gen. Richard Webber, a past commander of the 24th Air Force, his service's component of U.S. Cyber Command. His vision of his command was that he and his airmen will provide "mission assurance," not "information assurance" — that is, that his main goal is not to defend computers per se but rather to assure commanders that they can continue their missions in contested cyber environments. The Army uses different vocabulary, but it's apparent that these two Cyber Command service components share a view.

To that end, the Department of Defense holds rehearsals for cyber attack; these exercises go by names such as Cyber Flag, Bulwark Defender, Turbo Challenge and Cyber Endeavor. But these are largely echelons-above-corps exercises, and the ways we execute them are insufficiently rigorous.

Too often, exercise commanders and planners make fundamental assumptions about retained availability or unrealistically rapid restoration of cyber resources. The exercises tend to be short-duration, not long-duration; to feature degradations or losses of limited scope, not pervasive ones; and to clearly differentiate natural and man-made effects. This allows commanders and staffs to extrapolate impacts and reactions to circumstances they've not encountered. I'm confident readers can recall breezy hand-waving about operating through cyber outages, predictions of restoration of host-nation cyber capabilities despite high-altitude electromagnetic pulse detonations, and otherwise confident assertions that the collective "we" would overcome whatever nature or adversaries threw at us. I'm also confident those same anecdotes are colored by the remembered irritation and pain of actual cyber degradation or losses well below "Cyber Pearl Harbor" thresholds that were not planned, not rehearsed, not well-tolerated and were poorly muddled through by units at every echelon.

At the risk of overgeneralizing, most cyber tabletop exercises and general officer-level leadership games I've been exposed to involved either too few (or too low-ranking) technical-oriented people to splash the cold water of technical realities on the attendees and too few maneuver commanders to splash the cold water of mission priorities beyond cyber on the technical-oriented folks.

An informal and unscientific poll of the Functional Area 53 and INTELST mail lists contributes to the notion that we are also not rehearsing well or often for cyber contingencies at echelons below corps. (By contrast, government officials — at least to judge by their quotes in the media — are quite worried about just these kinds of environments.)

WHAT WE USED TO DO

Our collective failure to perform rigorous cyber-related rehearsals in the form of individual soldier tasks, unit tasks and integral parts of larger-purpose exercises stands in stark contrast to our preparations for threats in the 1980s and '90s. I recall two forms of contingency rehearsals I regularly executed as a platoon leader that could, with analogical reasoning, help us in contested cyberspace environments. The first was rehearsing operations in persistent and nonpersistent chemical environments. The second was the use of radio listening silence, radio silence and signal operating instructions (SOIs) in platoon- through battalion-level operations.

For cyber strikes, what are our standard, rehearsed individual, small-unit or even battalion-level tasks and responses? One response, at an emotional level, could be relief: At last, we can operate without micro-management from afar! But the relief will likely be soon overtaken by confusion and improvisation. How will soldiers navigate when their commercial off-the-shelf mapping hardware and software stop working unless they have practiced using paper maps and lensatic compasses?

When plotting the coordinates of a chemical strike broadcast message, soldiers knew to avoid the affected coordinates and its downwind hazard areas. Can units identify and locate specific hazards from a broadcast cyber strike? Do we rely on cyber resources to broadcast alerts about cyber strikes or cyber malfunctions? Are reports from national or combatant-command-level entities sufficiently detailed to allow, say, D Company, 1-327th Infantry, 101st Airborne Division, to know it just received a cyber strike? How does a message from faraway entities even get to D Company? If a report contains an IP address with no other identifying information, are there rehearsed drills to identify the owning unit and the analogous downwind hazards? Can the Army, with high confidence, train soldiers and leaders to recognize adversary-caused cyber effects compared to self-induced problems — i.e., is that unscheduled and unannounced reboot of the commanding general's computer evidence of hostile action or just an ill-advised move by local IT support? Is the temporary loss of NIPR Wi-Fi at an installation a temporary glitch or a man-in-the-middle attack? Are immediate action drills for man-made degradations different from those for confirmed or suspected adversary actions? Are the differences purposeful and meaningful?

Certainly, the "identify and react to a chemical strike" battle drill is no perfect analogy to "cyber strike" battle drill. But it shows the kind of past competency that we must regain in the modern era. Years ago, we willingly put large numbers of people, including high-ranking commanders, through time-consuming and physically uncomfortable battle drills for biological and chemical environments. We developed expectations and rules of thumb for operating tempo slow-downs within planning staffs and standard operating procedures for mechanized and armored forces. At the battalion level, at least, these rehearsals led to confidence that a sufficiently small chemical strike would not inflict too great a casualty rate.

We have yet to consistently inconvenience high-level commanders or develop such expectations for cyber, although DoD leaders appear far more confident of future network attacks than we ever were of chemical strikes by the Soviets.

WHAT WE CAN DO

A second contingency rehearsal we could resurrect would require us to use seemingly long-forgotten skills: operating without our networks and radios for extended periods of time across large battle spaces. Mechanized infantry used to lay communications wire between tracked vehicles when at long halts or in a laager. Soldiers used to use SOI-encoded messages and messengers/couriers for days. Tactical units may still practice these alternate and contingency ways of exercising command and control — but how fast does failover occur, and how comfortable are higher echelons without their data addictions being fed from their subordinates? I am dubious that staffs of division and higher units will find it trivial to work through the old-but-forgotten ways of commanding large outfits without the near-instant gratification of cyberspace capabilities.

Here are a few ways we might practice for such situations. Commanders at various echelons can:

- Self-inflict announced and unannounced reductions of bandwidth in our day-to-day networks: C2, medical, logistics, personnel, finance and contracting — that is, deliberately move to "soda-straw" levels compared to normal levels for days at a time.
- Coordinate with higher commands and request nondestructive defensive fires. A cyber analog could be isolating a network segment or cutting off all online connections except those to a white list of pre-approved, known safe systems.
- Rehearse defensive reconfigurations, deployments of cyber assets that would not be susceptible to the envisioned threat or other "cyber maneuvers."
- Practice failover and load-reduction to alternative transmission modes. If a host nation's communications fail, how does a unit behave when restricted to military or commercial satellite links?

Staffs can practice this, as can commanders. They might, for example, relay past orders from Cyber Command or elsewhere, ask for and implement their services' Cyber Command contingency plans and execute notional cyber defense orders that actually impinge on their perceptions of what's important. Brigade-and-above headquarters can practice reporting timelines that take hours or days instead of seconds or minutes and practice collecting data with clipboards and grease pencils instead of Command Post of the Future and Tactical Integrated Ground Reporting. Crucially, they should practice these drills and tasks not only in garrison, but also during training center rotations. There's no use excluding unit training for deployment — Strategic and Cyber Command have already demonstrated that being "in the fight" is an insufficient rationale for ignoring cyberspace orders and directives.

Finally, nonmaneuver forces must rehearse as well. Medical, logistics, acquisition, strategic intelligence, morale-welfare-recreation and other organizations should also practice cyber operations battle drills. How do they prioritize and continue their missions in the face of long-term or pervasive degradation? Can they send and receive messages up and down the chain of command sufficient for high-priority mission tasks? Can they receive reports from outside their day-to-day operations channels (e.g., Cyber Command or Army Cyber) about a bad computer? Do they have the manpower to find and fix dozens or hundreds of systems amid day-to-day or degraded operations? Can they react in ways short of self-inflicted denial of service to an entire installation, as happened at Fort Campbell in 2004? If the answers to these questions are not reasonably clear and rehearsed, no commander should have confidence in the answers' accuracy.

In short, we should periodically apply the enemy's most dangerous cyber course of action and work through how we adapt to it. We should resist the temptation to assume cyber capabilities will return to normal or near normal after only brief periods of interruption with no substantial or long-term degradation of operations. We should test our self-confidence with rigor, not blithely trust in our use of "superior" technology and information.

WHAT WE NEED TO DO THIS

Of course, there are challenges to all this. Full-participation exercises are expensive for units and the services to plan and execute. There are almost always more staff-recommended training objectives than commanders can reasonably fit into a schedule and budget.

With too few resources and too many demands, what are other options? Commands could pick the cyber-analogs of map exercises, tactical exercises without troops, or command-post exercises.

Here's another option, one that promises better preparation without much increase in cost: Use rapid, decentralized and customizable modeling and simulation tools. This suggestion raises a number of questions. For example, can such tools:

- Reflect the variety of knowledge, beliefs, practices, behaviors and capabilities possessed by soldiers, units, other services, other coalition partners and host nations?
- Adequately depict cyber capabilities, including specific systems and their dependencies, classified networks and communications mediums?
- Reduce our cyber rehearsal gap?

The answer to the first two questions is "yes, with caveats," but to the last, it is a definitive yes. We know this because such tools already exist. Leading research universities such as Carnegie Mellon University, George Mason University, Vanderbilt University and others have taken them from laboratory experiments to commercial applications.

One example of such a set of tools and workflow exists at Carnegie Mellon's Center for Computational Analysis of Social and Organizational Systems. Its AutoMap tool uses machine learning to quickly create models of organizations, which can then be used to analyze data flows, look at social networks and perform what-if experiments using agent-based simulations.

A staff might feed AutoMap a collection of documents that describe the organization: joint and service doctrine; descriptions of tactics, techniques and standard operating procedures; emails; reports; briefings; etc. The software can sort the documents' words and concepts into categories — agents, organizations, roles, beliefs, knowledge, tasks, resources, events, locations and actions — and create a complex representation of the organization.

The commander and staff can then take this socio-technical, multi-mode model and inflict simulated cyber attacks on their organizations. The tools for the assessment of the attacks' effects are already in wide use by the intelligence, counter-IED and service academy communities. Such tools include ORA, UCINet, Palantir, Pajek and Analyst Notebook. (Helpfully, the Joint IED Defeat Organization has produced side-by-side comparisons of these tools.)

The results of these simulated attacks may inspire confidence in one's cyber preparations. When the Air Force Research Lab used Air Force doctrine documents to model the service's Air Operations Centers, the resulting model indicated that the AOCs were significantly more resilient to cyber attack than a cursory review suggested. But these kinds of models can also reveal vulnerabilities in organizational structure, IT setup, manning and processes. As commanders and staffs create adaptations, and possibly even solutions to the vulnerabilities, they can tweak their model and re-run the simulated attacks until they achieve a satisfactory response. Such simulations are certainly not proof or prediction of real-world success, but they allow us to move beyond gut feelings, personal opinions and hyperbole toward rigorous and repeatable experimentation.

All this can be done without disrupting a command's operational networks and with relatively little impact on the rest of the unit. The next step is staging soldier-in-the-loop exercises to calibrate the model to reality, and ultimately, developing battle drills to hone the unit's ability to carry out its missions under cyber attack.

CONCLUSIONS

From short-duration denial-of-service attacks to sophisticated advanced persistent threats, from seafloor landslides to high-altitude electromagnetic pulses, a vast range of potential network problems threaten our wired way of war. Yet rehearsing operations in contested cyber environments remains a capability gap at all Army echelons. If we fail to adequately plan and rehearse for adversaries that exploit that gap, we almost assure ourselves a difficult initial future fight and a hard slog out of an initial future mess.

Tools like AutoMap have drastically reduced the time, money and expertise needed to construct useful organizational models to just hours or days instead of the weeks to months needed by the Battle Labs. Best of all, the Army does not need to wait for gold-plated, grade-A M&S capabilities from a defense contractor that require a staff of statistical analysts and professional model builders. We can use capabilities coming out of our research universities, give them to soldiers and their commanders, and begin reducing the gap today.

[Subscribe](#) | [Renew](#) | [Customer Service](#) | [Advertising](#) | [Contact Us](#)
For inquiries about reproduction or distribution of any materials contained herein, please [click here](#).

GANNETT

Users of this site agree to the [Terms of Service](#), [Privacy Notice/Your California Privacy Rights](#), and [Ad Choices](#)

All content © 2013, Armed Forces Journal