Cyber defense planning

Operating on Unconventional Terrain

LTC Michael Lanham

The question "How can the Army better plan and execute effective cyber defense?" is too broad. We can craft more effective solutions if we narrow the question. And we can develop approaches that more closely align with traditional military vocabulary and symbology than does our current tendencies to 'go geek.'

The approach, is to use the military decision making process, augmented with doctrinal Joint and Army graphics, and treat cyber terrain approximately the same as we treat the land and air domains.

Using the mnemonic of mission, enemy, time, terrain, civilians, we'll ask some clarifying questions, starting with "Better than what?"

How will we know when we are 'better' (mission) and if the improvement is enough? What resources (troops, terrain, time, equipment) are available to become 'better'? What are the constraints and restraints (mission, civilians, enemy, time, ROE)? Is there a prioritized threats list or defended asset list such as Air Defense Artillery creates/uses? Is the commander willing to conduct economy of force operations in defending one or more cyber positions, routes, or line of communication?

Is defense of the secure internet protocol network, given its cryptographic separation from other networks, one of those economies of force operations? Can our economy of force operation be all or some of the non-secure internet protocol network positions—even though our sustainment (personnel, finance, maintenance, and strategic and tactical logistics) warfighting function does most of its work there? How concerned is the commander with threats to morale-oriented use of DoD cyber infrastructure compared to threats exploit such use as an avenue of approach to NIPRNet and shared infrastructure?

Cyber defense planners need to know current threats (enemy, civilians, troops) as well as current friendly situations two-levels-up and one-level-down (troops, commander's intent). With that knowledge, its extremely likely that COA recommendations for the physical and cyber AORs will contain multiple decision and branch points. Examples of decision points include: whether to isolate (clear cyber fires) units in contact against immediate/high impact cyber threats to other units; whether and how to clear cyber fires for units not in contact against slow-spreading malware; whether to temporarily exempt some mission areas and units (e.g. aero-medevac for combat theaters) from anti-malware directives; whether and how to react to a fast-moving threat, even with some units in direct fire contact; to whom can the Commander permanently or temporarily delegate such decisions.

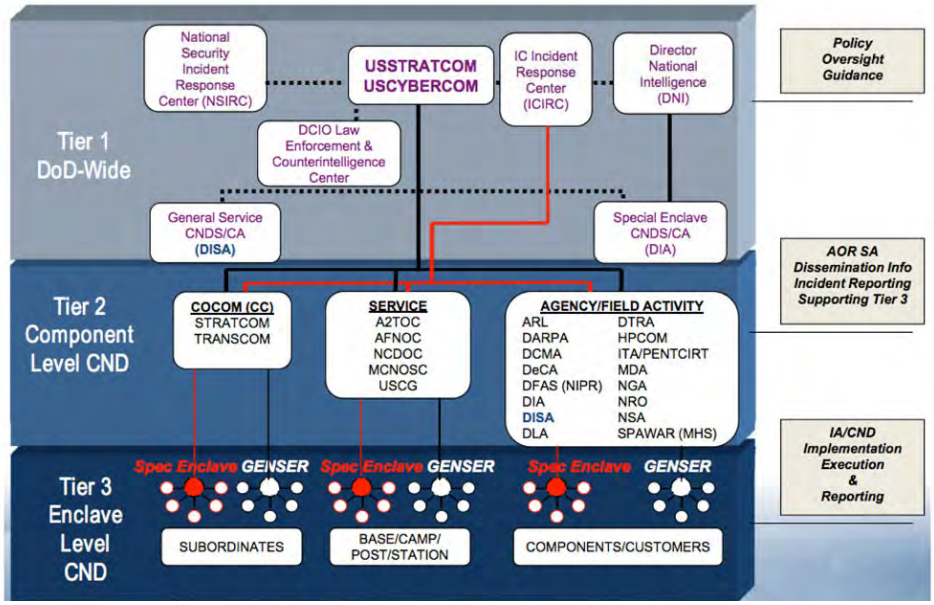

Figure 1 U. S. Cyber Command as the Tier 1 CND-SP

There are multitudes of other questions for which we need, at least approximate, answers as well as approximate first and second order effects. Asking for guidance and offering COAs to our commanders is essential—or our commanders will discover they have a set of defenses, on disadvantageous real and/or cyber terrain, that don't adjust to enemy actions as the commanders envisioned. They'll also discover

(Continued on page 8)

(Continued from page 7)

that their assumptions about the J/G/S6 just 'getting it done' can leave them reaction choices that don't fit their scheme of maneuver.

The original question of this article implied a requirement to be 'better' than the status quo. How do we know we've sufficiently met that requirement? We can recommend measures of performance and measures of effectiveness. A possible MoP could be, "a 10% reduction in loss of availability of IT systems needed for operations." A possible MoE could be, "an 80% reduction in the number of combat missions that have failed due to loss of IT systems."

With these candidate measures, we've reached a challenge in expectation management. Which 'operations'--tactical combat operations by a platoon conducting an ambush or periodic VTCs between a HQ's forward and main command posts … the transition between strategic and tactical logistics operations… or the planning and execution of a tactical resupply mission?

With a vague MoE, to establish a reduction, we have to have some idea of a baseline, or ground truth. Has any COCOM or Army unit determined how many and what types of missions have failed due to a loss of cyber capabilities? Of the many possible MoPs and MoEs, these two derive from the apparent dominance of non-availability and mission failure in the rhetoric of public discourse.

U.S. officials have repeatedly sounded the alarm about our unpreparedness for cyberspace warfare. Public figures routinely refer to the potential for loss-of-life and 'existential threats.' They often speak about the potential for devastating consequences from a large-scale cyber attack. Of note is the lack of reference to documented cases of loss-of-life, destruction of companies, or disruption of public utilities directly attributed to cyber operations. Also missing is reference to large-scale destruction of civil society in the absence of IT-enabled life. Large-scale power losses in the U.S. Northeast and U.S. Midwest-to-Eastern-seaboard suggest a greater resilience to cyber-less life than the rhetoric acknowledges. India, Estonia, Ukraine, and Georgia appear to reflect the same resilience to cyber-less and cyber-disrupted life in the long term.

The disconnect between demonstrated civil/governmental resilience to natural disaster and rhetorical predictions of cyber catastrophe makes developing and distributing relevant MoE and MoP even more critical for cyber defense planners and commanders.

Army Regulation 10-87 states that "All operational Army forces are assigned to combatant commands." Incorporating this, we can modify the original question to, "can COCOMs and their assigned Army forces plan and conduct cyber defense operations better than the status quo?"

This choice allows us to separate more frequently volatile AORs from the non-operational forces and the supporting institutional base of the Army. It also avoids the interminable debates about the proper division of Service Title X and COCOM Title X responsibilities and authorities. Those debates tend to revolve around perspectives about cyber-personnel and the equipment/networks: Services extend, under their control, their capabilities into Joint and Coalition AORs versus Services provide capabilities under COCOM authority to meet theater Joint and Coalition operational requirements.

A further refinement of the original opening question can be, "Can COCOMs, and their assigned Army forces, plan and conduct cyber defense operations in all phases of operations to ensure continued readiness for and execution of military operations?" This construction

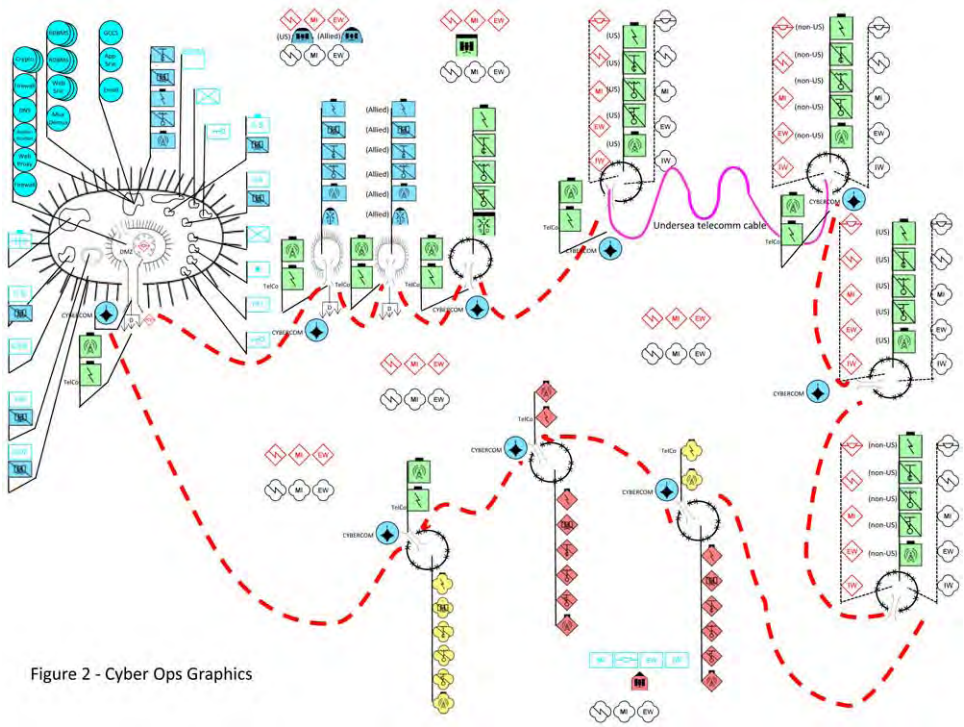

Figure 2 Operational Graphics Representing a Cyber Operation Battlespace

conforms to the theory of DoD's three-tier hierarchy for computer network defense service providers, but not as well to the implementation of that hierarchy.

Figure 1 depicts U.S. Cyber Command as the Tier 1 CND-SP. As of late 2009, no COCOM other than USSTRATCOM had created their own CND-SP, instead hiring DISA as the CND-SP for their headquarters' cyber positions. This and many others decisions have lead to a situation where, unless CND-SP actions crossed into operational channels (e.g. Operation Buckshot Yankee), the COCOMs relied upon the Services to provide CND-SP capabilities to COCOM forces. This creates a de facto line of authority between the Services and COCOM forces that does not otherwise exist in joint doctrine.

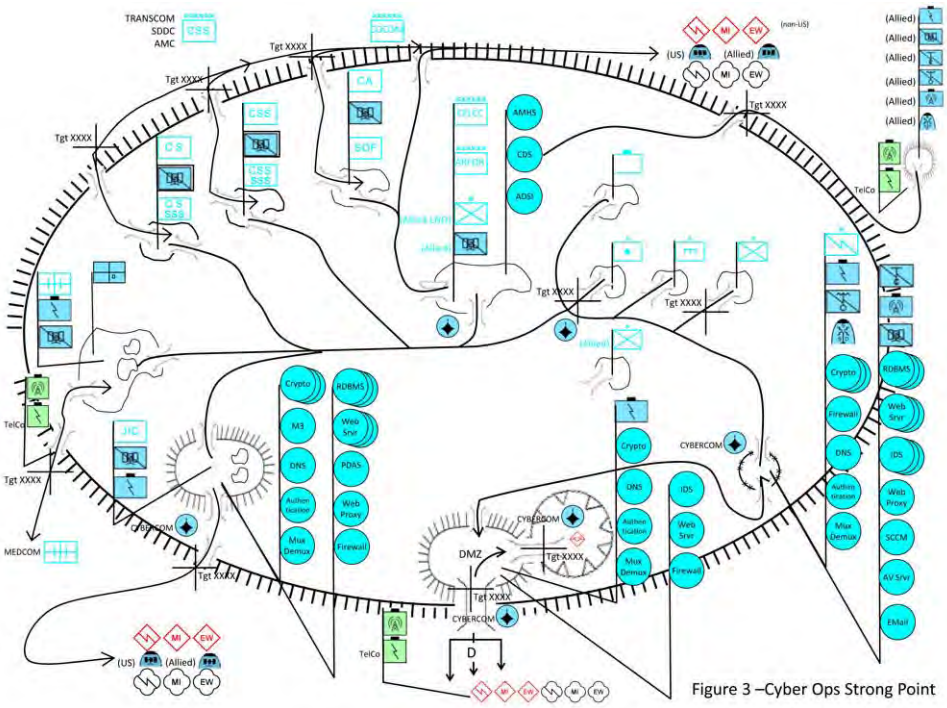

Figure 3 Cyber Strong Points

Returning to the modified question, a last refinement could be "Can COCOMs and their assigned Army forces plan and conduct a deliberate defense of cyber capabilities in all phases of operations to ensure continued readiness for and execution of military operations?" In short, instead of using the civilian-dominated language of enclaves, intrusion detection systems, and firewalls, use Joint Publication and Field Manual 1-02 language such as sensor, positions, strong points, LOCs, communications zones, deliberate defense, and deliberate operations. Though JP 1-02 defines a deliberate defense as "normally organized when out of contact with the enemy," our need to create an "extensive fortified zone" clearly applies. The definition of deliberate operation, "An operation in which a commander's detailed intelligence concerning the situation allows him to develop and coordinate detailed plans, including multiple branches and sequels…" is also clearly applicable.

This construction of the original question will face resistance, as it requires an acknowledgement that many positions of DoD, COCOM, and Army cyber infrastructure are fixed on both physical as well as cyber terrain, requiring a permanent defense. That acknowledgement stands in contrast to the central idea of Army Doctrine Publication 3-0 Unified Land Operations: "seize, retain, and exploit the initiative to gain and maintain a position of relative advantage in sustained land operations to create conditions for favorable conflict resolution." To seize initiative in permanently defensive situations will place unfamiliar demands on commanders and their staffs.

When planning a deliberate defense, or any operation, our professional military education system teaches Soldiers that the Commander is an essential figure. To help ensure commanders stay involved and interested in cyber defense planning, their subject matter experts should drop the vocabulary of Intel, Cisco, Microsoft, and other 'geek speak' and revert to traditional military operations vocabulary.

An example of this reversion is Figure 2. It is a set of operational graphics that represents a cyber operations battle space. Using Military Standard-2525C (with some allowances for different software tools and modifications to cope with the newest addition to war fighting domains), we can communicate a significant volume of relevant data to any commander. The figure uses symbol sets she/he is used and communicates the relationship of units to their cyber positions (and physical positions if placed on a map overlay). Within this strong point there is a gap in the defenses indicated by the bridge icon, with a disruption icon to indicate that cyber forces must disrupt enemy approaches into the strong point. Further, the depicted ASCC commander can see the existence and location of multiple USCYBERCOM sensors throughout the battle space. He can see and communicate to his subordinates that there are multiple enemy approaches into the strong point. The figure also communicates to the various units inside the strong point that they have their own boundaries/demarcations they must de-

(Continued on page 10)

(Continued from page 9)

o the cyber defenders and tradi-
ional Signal support units. The
graphic shows multiple units with
heir own generic tactical satellite
cons—planners can use modi-
iers to depict specific capabilities
(e.g. CSS-VSAT, JNN. There are
emplate enemy graphics as well
a software limitation prevented
use of dashed lines) as well as the
ntent to isolate enemy sensors within the DMZ. Importantly, the diagram reveals the dominance of neutral (green) telecommunications companies and telecommunications infrastructures just outside their strong point perimeters. This dominance is true even in Afghanistan and Iraq.

In Figure 3, the cyber strong point diagram puts details to the phrase defense-in-depth. Figure 3 shows an overall protective perimeter, a controlled entry point, a cyber turning obstacle to route attacks to an isolation area, as well as responsibility for interior perimeters defense. To a maneuver commander, this depiction should start a detailed discussion about likely enemy avenues of approach, primary, alternate, contingency, and emergency positions and cyber actions on contact—all conventional plans even though its non-traditional terrain.

A commander can pre-plot cyber fires that allow her/him to interdict or destroy enemy activity on internal routes between units. There is the visual cue that internal cyber routes need periodic clearance to remain under friendly control. Several units have redundant communications paths through the installation telecommunications facilities as well as their own tactical satellite access. This redundant capability suggests the need for increased security and monitoring at additional 'holes in the wire' to avoid weakening the overall strong point.

Like Figure 2, the diagram levies implied tasks on cyber operations units and Soldiers. It is essential to know which cyber capabilities belong to which units. The diagram emphasizes the reliance on neutral telecommunications companies. The diagram also illustrates planning considerations for cyber defenders that are often overlooked: Army provisioning of network access (NIPRNet and SIPRNet) to coalition partner liaison officers and elements; having dedicated routes for shared ADA situation awareness; having MI-owned strong points supporting JWICS; setting up and rehearsing the response to call for cyber-fires on pre-planned targets; setting up an isolation area(s); physical defense of satellite downlink stations, telecommunications and radio relays at the technical control facility; units within the perimeter that are collocated but not otherwise under the command authority of the ASCC (e.g. SDDC, AMC); and

Advantages	Disadvantages
•Rapid information sharing via use of standardized JP I-02 and FM 1-02 vocabulary and iconography •Visually combines area defense and point defense coordination of entry/exit points, PACE routes and capabilities, and mutual reliance for security •Within area defense, emphasizes template enemy presence throughout the cyber-LOCs, with implicit requirement to reduce or mitigate the enemy's presence •Operational requirement to control friendly and enemy cyber-LOCs becomes obvious •Depicts requirement for cyber-coordination between units •CAN planning at appropriate echelons will have better SA of impacts within an AOR •Helps plan and visual enemy cyber attack points, approaches, locations for friendly effects/obstacles (e.g. canalize, turn, disrupt, isolate)	•Map/graphics reading and interpretation is a perishable skill •Not all Soldiers from all warfighting functions are comfortable with MIL-STD-2525C •Threat type differentiation (e.g. nation state sensor vs. cyber criminal vs. teenager in Paris/Des Moines) requires icon modifiers •MIL-STD-2525C has no way of reflecting equipment/capability dependencies except through co-location •Map/graphics overlay requires maintenance effort
If control of cyber LOCs is not feasible due to neutrality, then •Guard the friendly entrances and exits that tough those LOCs •Pre-plan targets on the LOCs with permission from higher •Gain clarity on neutrality of cyber-LOC providers	•Cyber Intel applicable to AOR and units becomes yet another product unit J/G/S2 has to find/generate •Geo-plotting every device may have a low ROI for many units/locations
•React to enemy cyber contact may become faster •SA of units/capabilities not using Signal assets •SA of units/capabilities using Signal assets •Combined with capabilities such as host based security services (HBSS), should increase per IT SA as well as per unit cyber SA •Geo-plotting makes command responsibility immediately clear •Helps pre-plan cyber fires for units within an AOR and for units outside the AOR •Rehearsals of target/fires increase confidence in response time and probability of gaining effects •Should help in clearing offensive/defensive fires across unit boundaries	•Commanders at wrong echelons may perceive greater latitude for offensive and defensive cyber operations than exists •Requires targeting process participants to gain familiarity with •cyber targeting, cyber effects, cyber BDA (e.g. artillery destroy !=cyber destroy; cyber deny!=engineer deny) •processes established for cyber fires by USCYBERCOM and CYBER-JIATF •Will likely cause an increase in templating and requesting cyber fires for defense and offense •USCYBERCOM may not be capable of supporting quantity of requested fires •USCYBERCOM may reprioritize local targets in favor of strategic targets of interest
Unit boundaries can align with IA demarcation points for systems and enclaves, e.g. bridges in/out of theater enclaves, JTF enclaves division or brigade enclaves.	Clean alignment of physical boundaries and demarcations may not be feasible. DISA Tier 0 network equipment is frequently co-located with P/C/S TCF

Advantages and Disadvantages of using JP 1-02 vocabulary and concepts

he heavy reliance by CS and CSS units on non-Signal-provided capabilities.

I have not included a figure that incorporates maneuver graphics and AOR boundaries but they could easily help reduce misplaced perceptions of responsibility while bringing home to units their actual contributions to cyber defense operations. Every COCOM has a number of physical and cyber strong points within their geographical or functional AOR, connected by ground, air, and cyber LOCs. Those cyber-LOCs enter and exit their AOR at physical points as well as logical points—those points can become coordination points/icons, targets, and sensor emplacement points. Plotting units and capabilities physically and logically also supports more rapid clearing of defensive cyber fires as envisioned in what USCYBERCOM calls 'active defense,' and reduces the likelihood of unintended consequences.

Figures 2 and 3, and the figure described above, communicate a complex but traditional military operation, on non-traditional terrain. This approach supports Commanders and staffs ability to think about the cyber domain in approximately the same terms as their air and land domains. Commanders will learn where pre-planned defensive cyber fires exist, their probable operational impact when fired, and can plan compensation measures. Through awareness of dependence on civilian infrastructure, they can build and rehearse PACE plans for communicating to and with higher and lower units. There are a multitude of potential advantages listed in Table I, and for balance's sake, predictable disadvantages as well. Though I make no claim the list is comprehensive, it should at least provoke reflection on the collective wisdom of abandoning a common lexicon and adopting a 'new' one—for whatever the reasons.

Table I Advantages and Disadvantages of using JP 1-02 and FM 1-02 vocabulary and concepts

There is a strong underlying message in my assertion that cyber defense is a traditional military operation: decentralized COCOM operations, as inefficient and chaotic as they are, should remain the order of the day. Defending a set of inter-connected strong points in a region is not a military operation that the COCOMs or the Army trains to conduct via centralized execution. Instead they nest task and purpose to support the intent of centralized planning without the inflexible application of centralized approval. This nesting allows for dealing with the surprises of 'reality' vs. 'the plan.' The nesting allows COCOM commanders to assess and balance risks and operations as close to their operations as feasible while allowing other COCOMs and potentially effected commands options to reduce their own exposures to those risks. Indeed, if the job of balancing regional and global or Service perspectives is centralized, its more likely than not that the needs of the many will always outweigh the needs of the few—to the detriment of the minority conducting highly volatile operations. Unfortunately, there is a multitude of past and current trends, policies, personalities and efforts within the Joint arena and the Army to make defense of cyber strong points and LOCs centrally executed. This is in contradiction to our national willingness to decentralize most combat operations, clearly a matter of life-and-death. Historians often cite that willingness, indeed the apparently ingrained inability to do centralized execution, as one of our greatest military strengths. Our growing unwillingness to resource and execute decentralized cyberspace operations is disconcerting. The efforts to move toward centralized execution are, in actuality, grand experiments, with as little proof of future success as this article has presented. I submit to you that the burden of proof when advocating wholesale change is on the advocates of that change. I've not seen evidence in classified or unclassified realms that convinces me of the added value of creating unique-to-cyber processes and vocabulary. Nor have I seen evidence of the value of abandoning graphical depictions used so successfully in the other warfighting domains.

I have been exposed to two schools of thought for involvement of operational force commanders in cyber defense planning and execution. Paraphrasing, one such school is that cyberspace is far too important and complex to leave to maneuver commanders. The other school is that cyber defense will not succeed without commanders. I clearly subscribe to the second school despite copious evidence of disinterested commanders and staff leading to poor cyber outcomes. I've also seen even more evidence that excluding maneuver commanders from cyber defense and planning leads to, predictably, worse outcomes than had those commanders been involved.

I submit to the readers that we, formally the Army's cyber-SMEs, must use the language of our maneuver commanders if we are to succeed in engaging their interests. I have proposed use of a traditional planning method and traditional doctrinal vocabulary (with minor updates) for planning and executing cyber defense for operational forces. I have proposed that staying in that realm of vocabulary and iconography is more likely to retain the interest, understanding, and resource commitment of commanders than by 'going geek' on them.

I have offered no proof that this approach to planning will actually make COCOM and assigned Army forces better at cyber defense. Indeed, the absence of proof in cyber defense policy, advocacy, efficacy, and efficiency discussions is endemic within the DoD—we frequently substitute passion and hyperbole for evidence, use measurable quantities (e.g. costs) as proxies for inherently qualitative assessments, and break into

(Continued on page 12)

(Continued from page 11)

advocacy camps convinced of our own righteousness. We use short-duration joint and warfighting experiments that don't allow long-term, significant, and effective disruption of cyber capabilities in the actual experimental networks. We conduct C3I experiments that allow disruption, with insufficient operational impact assessments by commanders—I've attended simulations where a 'glitch' led the players to go to lunch, instead of continuing the experiment. I've seen decisions to implement PACE plans for cyber capabilities be furiously argued as the staff and the commanders weigh the immediate pain of rehearsal with the promise of being more resilient to non-specific threats of denial or degradation. Anecdotally, these examples are not unique, though I have no sense of their relative frequency. It's my assessment that we have a Joint and Service shortfall in our ability to conduct long-term cyber experiments as well as organization redesign in reaction to cyber events experiments—how to address that shortfall is an article for another day, though I strongly suspect agent-based socio-cultural simulations and dynamic socio-network analysis is a key enabler we inadequately use.

There are at least five conclusions we can draw from this discussion: 1) operational force commanders are essential for operational force cyber defense; 2) we can plan and execute cyber defense by considering the mission a traditional deliberate operation on non-traditional terrain; 3) this approach will be uncomfortable to portions of the CND communities; 4) advocates for centralizing cyber defense have the burden of proof to justify violating operational norms; and, finally, 5) simulation or proof of future success is beyond our current institutional ability.

***LTC Michael Lanham**, IN, is a FA53 in Advanced Civil Schooling pursing a PhD in a field of Computer Science. He has served as a Theater IA Program Manager at ARCENT, a CNO plans officer at ARFORCYBER and JFCC-NW and deputy Chief Information Officer at JFCC-IMD. He has bachelor's degrees in Computer Science and Computer Engineering and a master's degree in Computer Science.*

Join the Discussion
https://signallink.army.mil

Acronym QuickScan

ADA – Air Defense Artillery
ADP – Army Doctrine Publication
ADSI – Air Defense Artillery System Interface
AMHS/M3 – Automated Message Handling System
AOR – Area of Responsibility
ASA – Assistant Secretary of the Army
CC – Combatant Command
CC/S/A/FA – Combatant Command, Service, Agency, Field Activity
COMMZ – Communications Zone
CPN – Command Post Node
CND-SP – Computer Network Defense Service Provider
COCOM – Combatant Command
CS – Combat Support
CSS – Combat Service Support
DEMUX – De-multiplexor
DEPORD – Deployment Order
DISA – Defense Information Systems Agency
DHS – Department of Homeland Security
DMZ – Demilitarized Zone
DNS – Domain Name Service
FA – Field Activity
FOB – Forward Operating Base
FCC – Functional Combatant Command
GCC – Geographic Combatant Command
HBSS – Host Based Security Services
HQDA – Headquarters, Department of the Army
IA – Information Assurance
IP – Internet Protocol
ISEC – Information Systems Engineering Command
IT – Information Technology
NLT – No later than
P/C/S – Post / Camp / Station
JIATF – Joint Inter-Agency Task Force
JNN – Joint Network Node
JP – Joint Publication
JPG – Joint Planning Group
JS – Joint Staff
JTF – Joint Task Force
JWICS – Joint Worldwide Intelligence Communications System
LOC – Line of Communication
LNO – Liaison Officer
MDMP – Military Decision Making Process
METT-C – mission, enemy, time, terrain, civilians
MIL-STD – Military Standard
MoE – Measure of Effectiveness
MoP – Measure of Performance
MUX – Multiplexor
NCO – Non-commission Officer
NIPRNet – Non-secure Internet Protocol Network
NGB – National Guard Bureau
OBY – Operation Buckshot Yankee
OPCON – Operational Control
PACE – Primary, Alternate, Contingency, and Emergency
PME – Professional Military Education
ROI – Return on Investment
SA – Situation Awareness
SECDEF – Secretary of Defense
SIPRNet – Secure Internet Protocol Network
SME – Subject Matter Expert
TACON – Tactical Control
TCF – Telecommunications Facility / Technical Control Facility
TelCo – Telecommunications Company
TTP – Tactics, Techniques, and Procedures
USSTRATCOM – U.S. Strategic Command
USCYBERCOM – U.S .Cyber Command
VSAT – Very Small Aperture Terminal