SMALL WARS JOURNAL

Capstone Commanders: Adaptability in the Complex Security Environment

By ***Clarence J. Henderson***

Journal Article | *Aug 12 2016 - 12:06am*

Capstone Commanders: Adaptability in the Complex Security Environment

Clarence J. Henderson

Through undulating canopies of reed grass the insurgents appear, then press forward to cross the river. Approaching a screen line, U.S. forces deliberately show their presence to channel the six-man team into a zone favorable for an attack. Two hours earlier this same team was identified at a distance of 1,500 meters forward of an observation post. Engaged with the Long Range Advance Scout Surveillance System (LRAS3), authentication revealed each was carrying small arms weaponry with significant loads of contraband, perhaps resupply or commodities to be utilized for monetary gain. The insurgents in this case are Mexican Drug Trafficking Organizations (MDTO) crossing the Rio Grande River; their commodity is 60 lb. bundles of marijuana per man; and the attack is a coordinated response of Civilian Law Enforcement Agencies (LEA) and Texas National Guard (TXNG) assets. The result is an apprehension of MDTOs invading the state of Texas and our country. The future complex security environment has arrived, it is present, and Soldiers at all levels are operating within it.

Whether it be combined arms maneuver, consolidating gains through wide area security, or providing support to civil authorities; complexities in the "future" security environment have begun to be revealed. The 72nd Infantry Brigade Combat Team (IBCT), Texas Army National Guard (TXARNG) fully invested in the complex security environment throughout Fiscal Year 2015 at both home and abroad. Missions included combating MDTOs by order of the Governor of Texas along the US/Mexico border; a U.S. battalion component to the Multinational Force of Observers (MFO) mission in the Sinai; and a battalion Regionally Aligned Force (RAF) mission to Guatemala, Honduras, and El Salvador to conduct Counter Transnational Organized Crime (CTOC); as well as responding to no notice all-hazard floods throughout Texas as required. Unique trends within the emerging complex security environment were revealed during these missions. This essay will discuss routine complexities that we can forecast and prepare for, operational adaptability within the future security environment, and the changing nature of conflict.

What is a Complex Security Environment

Specifying the range of threats, identifying new strategies, and applying emerging techniques and technologies will require on-going analysis of the security environments we engage. Current national security policy has applied a common theme to these security environments as more volatile, more unpredictable, and more threatening throughout the global environment.[1] As these security environments evolve from "future" to "present" our analysis must identify continuities of complexity to enable our joint force to adapt, evolve, and innovate faster than our enemies. We must also resist the temptation of developing top down rigid strategies that denies us the ability to adapt faster than our globally connected enemies.

The 2014 Quadrennial Defense Review (QDR) places emphasis on the need for innovation and the rebalancing of a smaller Joint Force.[2] Though the rebalance exacerbates complexity within the future security environment it is not the reason for its on-going evolution. Rather, threat based capabilities ranging from hybrid forces employing asymmetric approaches, to state sponsored high-end conflicts, each enabled with technologies previously unavailable, more aptly contributes to the genesis of complexity.[3] The 2015 National Military Strategy expands upon the concept of hybrid forces and state sponsored conflicts discussed in the QDR. Hybrid forces could coalesce within the Continuum-of-Conflict and include Violent Extremist Organization (VEO), state, or non-state actor(s); each blending their techniques, capabilities, and resources to achieve objectives.[4] The U.S. Army's Operating Concept moves past the vagueness of a complex theme and presents a definition. Complex is defined as an environment that is not only unknown, but unknowable and constantly changing.[5] These environments could include competing powers (China and Russia), regional powers (Iran and the Democratic People's Republic of Korea), transnational terrorist networks (transnational groups and criminals), and even cyber threats.[6] Amongst each threat within each environment enemies could employ traditional, unconventional, or hybrid strategies. The combination of these strategies or the emergence of yet to be identified new strategies remains consistent with the characteristic of unknown, unknowable and constantly changing future complex security environments.

Routinely Complex: Repeating Complexities of the Present Security Environment

The unknown, unknowable and constantly changing environments should not preclude basic doctrinal concepts. We "do know" we must exploit the initiative to get to a position of relative advantage in order to win against any adversary. Thus, we must always be repositioning ourselves in the present security environment. Changes in technology and geopolitical dynamics will make this increasingly more difficult. But by combining offensive, defensive, and stability operations we can create conditions favorable to winning. Complex environments, however they are defined, reinforces the necessities to build upon our core competencies, apply the tenets of unified land operations, and link tactical actions to strategic objectives through the application of operational art. By adhering to these core doctrinal concepts we can conceive strategies, develop campaigns, and conduct operations to mitigate complexity. Waiting for complex trends to reveal themselves will only place our forces in a position of relative disadvantage.

The unknown, unknowable and constantly changing environments have begun to reveal known, knowable, and constant characteristics of the security environment. These continuities of complexity at the operational level are beginning to become self-evident. By focusing on such trends in complexity we can better align our operational capabilities and capacities to what we know is most likely to be "routinely complex". The no-notice deployment of 72IBCT personnel to the U.S./Mexico border while simultaneously conducting a RAF and MFO mission revealed these patterns of continuities in complexity. The harbinger of such continuities was revealed through the collusion between MDTOs and the criminal gangs and government officials of North and Central America. Transcending two Geographic Combatant Command regions, this collusion is symptomatic of trends that exploit global ideologies and technology. Combatting MDTOs on the U.S./Mexico border was directly related to the Counter Transnational Organized Crime (CTOC) mission within RAF in Central America. Also, the first ever IED attack on MFO Soldiers in the Sinai was directly related to the tactics and ideologies of other Islamic State syndicates throughout the Middle East.

Routine Complexity # 1. Complex Security Environments Require Campaign Strategies at Divisions and Brigades

Divisions and Brigades must develop their own campaigns in order to get to a position of relative advantage and win against any adversary. The 2015 National Military Strategy promotes strengthening our global network of allies and partners to conduct synchronized operations around the globe.[7] Divisions and Brigades will be pivotal in this campaign. Components of singular Brigades are now routinely employed in global operations ranging from Theater Security Cooperation missions in RAF, Peace-Keeping missions in MFO or KFOR, Combined Arms Maneuver and Wide Area Security in Afghanistan, and support to civil authorities in the homeland. Hybrid forces or transnational terrorist networks employing asymmetric approaches now possess the ability to adapt, pivot and change more rapidly than a theater campaign plan can be conceived or adjusted.

The unknown and unknowable threat criteria of the CTOC mission in Central America was revealed as known and knowable tactics and ideologies along the U.S./Mexico border. Two missions and two theaters; but one complex set of tactics and ideology. The MDTOs ideology of power and money permeate the drug and human trafficking corridors of Central America. Additionally, the MDTO's proxy gangs revealed their tactics in Mexico and Texas which were identical to those used in Honduras and Guatemala. In Texas, a screen was conducted within the Rio Grande Valley incorporating reconnaissance and mobility operations. Junior leaders, working with LEA partners, discerned the techniques and tactics of MDTOs and their proxy gangs attempting to enter the U.S. each night. Simultaneously, intelligence driven operations were improved amongst LEA air, ground, and maritime assets. All of this information was then discretely incorporated within the RAF mission via two senior leader seminars while maintaining focus on Operational Security (OPSEC).

The identification of the MDTO threat, recognition of their related operations in two theaters, and development of techniques to counter their tactics is precisely what needed to occur at the Brigade level. The achievement of depth, the extension of operations in time and space, became a decisive campaign effort. The RAF-CTOC mission and the interdiction of MDTOs in Texas were two distinct operations managed at a Brigade level. Each resulted in pivots of tactics when needed to stay in front of trans-national entities such as the MDTOs.

Routine Complexity # 2. Complex Security Environments Possess a Nexus of Threats that Exceed DOD Land Component Capabilities

Complex security environments will include persistent factors such as terrorism, narcotics, smuggling, and international criminal networks. Each of these factors contain threat based capabilities capable of providing a nexus to hybrid warfare which may transcend international boundaries. Therefore, success in exploiting U.S. land power advantages must incorporate interagency organizations that possess unique skill sets in dissuading the nexus of threats. The ability to achieve unity of effort amongst the myriad of agencies each possessing specific skill sets becomes the challenge. The desire is to facilitate collaborative efforts and align interests at the operational level to achieve unity of effort toward a common goal.

An interagency command structure at the operational level would enhance collaborative efforts. However, relationships between military and civilian agencies cannot be equated to military command authorities such as OPCON or TACON relationships.[8] An existing model that enables operational synchronization in the absence of a mandated interagency command structure is the Partnership Archetypes proposed by the 2014 Quadrennial Homeland Security Review.[9] Such a model can facilitate the supported and supporting roles between military and civilian agencies. Developed for partnership practices between the Department of Homeland Security (DHS) and the private sector, these archetypes align interests, identify shared outcomes, and are expandable based on the complexity of the problem.

The Partnership Archetype begins with Information-and Data-Sharing. Senior military planners were incorporated early with Law Enforcement staff and established integrating and functional cells to broaden the usage of information. The next Archetype was Coordination to Align Complimentary Activities. This occurred via a "Plans and Tactics" meeting between operational commanders of the TXNG and law enforcement officials and served to synchronize operations of agency members. Operational Linkages to Integrate Activities was the third Archetype and was conducted by LEAs and TXNG Battle Captains working shoulder-to-shoulder to integrate ground, air, and maritime maneuver elements. The final two Archetypes were Co-Investment to Consolidate Financing and Resources, and Co-Production to Create New Products. Each resulted in the usage of TXNG assets such as aircraft and reconnaissance equipment as well as financing by the state legislature to fund operations.

Routine Complexity # 3. Complex Security Environments Require Joint Forces Capable of Rapid Transition from One Operation to Another

As a member of the Joint Force the U.S. Army must gain and maintain proficiencies in support to civil authorities, humanitarian assistance and disaster response, counter-insurgency, combatting terrorism, and security cooperation.[10] Assuming a greater range of operations will require a greater level of readiness and response capabilities as land components maintain regionally engaged and globally responsive force postures. The ability to concentrate power rapidly, operate interoperable with coalition partners, and acquire information to develop situational understanding is necessary to rapidly transition to multiple operations.

The expeditionary maneuver of 1000 Soldiers and Airmen to the U.S./Mexico border constituted a rapid response to achieve strategic objectives. Tasks included designing a Joint Task Force, manning the task force and screening non-deployable personnel, development of new Rules and Use of Force (RUF), training the force; and recovery, reconditioning, and deployment of equipment. However, the ability to rapidly respond and deploy relied mostly upon the mobility of the force constituting both air and land assets. This capability was necessary to gain positions of relative advantage and defeat the adaptable MDTOs. In addition, interoperability challenges transcended each of the three dimensions of human, procedural, and technical aspects.[11] Capitalizing on a large number of Soldiers who were civilian law enforcement officers and Spanish speakers greatly enhanced the capability to build relationships and trust within the RAF mission. However, the procedural control policy and doctrine were vastly different between the U.S. and countries within the RAF mission; as well as between the TXNG and the LEAs. Key to success was to accommodate best practices from each force. Technical interoperability habitually centered upon secure communications. Cross training on equipment alleviated this concern but required more equipment sets for issue.

Finally, a unique challenge in information collection has become the rapid acquisition of information and data due to enhanced information systems. The increase in the speed of information and the compression of the decision cycle made it essential to streamline decision processes to integrate intelligence into operations. Collecting, inputting, sharing, and analyzing information from multiple informational devices and systems necessitated the development of processes and procedures with coalition partners.

Capstone Commanders: Applying Operational Adaptability in the Future Security Environment

The Army Capstone Concept emphasizes operational adaptability as a talent our force must embrace to negotiate the future complex security environment. Operational adaptability is the ability to shape conditions and respond effectively to changing threats and situations with appropriate, flexible, and timely actions.[12] The Army Operating Concept goes on to discuss adaptability in terms of leaders applying critical thinking and accepting prudent risk.[13] Leaders within the future security environment are in essence "Capstone Commanders" as they implement the precepts of operational adaptability within each of these Capstone documents. These Capstone Commanders become our Soldiers aligned across all ranks possessing the initiative and authority through mission command to develop situations through action. They will identify and respond to both the known routinely complex problems previously mentioned; as well as develop solutions to the unkown and unknowingly characteristics of future security environments. There is no other way – Due to dispersed and expeditionary operations our Capstone Commanders will be the innovators, managers, mediators, and owners of future complex security environments.

The predominance of Capstone Commanders operating in the future security environment will be of junior rank. Their experience base will be more limited yet their needed skills can approach that of a field grade staff officer as they seek to define complex problems. Often, these Capstone Commanders will be displaced within the expeditionary environment and must continually assess the situation to develop innovative solutions with little oversight. Understanding the environment and driving the operations process through visualizing, describing, directing, leading, and assessing will enable operational adaptability. These two criteria are necessary tenets of decentralized control within mission command. However, when applied to defining complex problems the Capstone Commander must grasp these criteria even though his or her professional education has not yet arrived to this point. Therefore, more experienced commanders must provide guidance to facilitate the junior Capstone Commander's ability to define complex problems without limiting operational adaptability. A shared understanding is a responsibility of the commander when implementing mission command.

Analysis of the operational variables enables a better understanding the environment. Eight interrelated variables of political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT) will enable visualization of threat, friendly, and neutral actors. More experienced commanders must teach and mentor the junior Capstone Commanders as they integrate these variables within the Operations Process. "When does a criminal become an insurgent" was a question that emerged early in the analysis of the environment within the Rio Grande Valley of Texas. The relevance of the question lies in the ability to use counter-insurgent techniques, should a criminal in fact be defined as an insurgent, as opposed to treating a MDTO cartel member only as a criminal. Local academia was solicited and contributed to the analysis as intelligence staff officers assisted the Capstone Commanders. Once the PMESII-PT analysis produced the appropriate understanding of the environment, problem framing was able to begin.

Operational Design is the methodology to conduct framing to visualize, and describe complex problems. Framing will enable the Capstone Commander to develop a plan for execution. As stated earlier, junior Capstone Commanders may not have arrived to this point of proficiency within their careers. To accommodate a lack of experience within operational design we found it necessary to add a fourth step to the Operations Process. A "decide" step was added. Thus, to understand the environment, we must visualize, describe, "decide", and then direct. Junior Capstone Commanders needed assistance in arriving to their conclusions. Decision tools ranged from the products of MDMP to the products of integrating and functional cells. Commander's Critical Information Requirements spanning both the LEAs (agency lead) and TXNG (supporting agency) was an example of one product that required re-visitation and continued emphasis for civil-support operations within Texas.

Capstone Insurgents

Capstone Commanders must be capable of defining complex problems in depth and continually moving to a position of advantage to seize and retain the initiative. But as we begin to identify trends in complexity we must be aware that the threat actor will constantly change his actions. He is also a creative thinker who is comfortable with ambiguity and change, probably more so than us. Whatever action we take, the Capstone Insurgent will have the ability to plan around it and reveal a new strategy.

Conclusion: Changing Nature of Conflict

The complexity of the future security environment will require Army forces who possess the capability to conduct missions in the homeland or in foreign lands.[14] The unknown, unknowable and constantly changing parameters of the security environment seems to suggest we are condemned to a reactionary operational process. However, continuities of complexity are beginning to be revealed. By focusing on emerging “routine” complexities we can begin to develop the specific strategies required for military campaigns that are developed at Divisions and Brigades. Additionally, by integrating the inter-agency partner and building a capacity to rapidly transition from one operation to another we can maintain an expeditionary capability required to defeat adaptable enemy forces.

People do not fight today for the same fundamental reasons identified by Thucydides long ago: fear, honor, and interest.[15] An emerging credible threat is the trans-national entity that possesses a nexus capability to hybrid warfare. His fundamental reason for fighting is power, profit, and ideology (pick your ideology). Criminal Drug Trafficking Cartel members have no honor. They will kill, kidnap, assault, and intimidate whoever stands in their way for the acquisition of money and power. They dedicate their lives to implement their ideology and will include terrorism and violence to achieve their means. Diffusion of technology and globalization accommodates their pursuit of power, and they will kill each other with impunity. The pursuit of their ideologies will drive them to expand operations across countries and expand to the U.S. homeland.

The Joint Force demands leaders who can adapt in the security environment of tomorrow.[16] Our Capstone Commanders will be the advantage against adaptable threat forces. They possess the creativity and ingenuity to identify complex problems and devise their solutions. However, the Capstone Commanders deployed in an expeditious manner to remote regions will require assistance from more experienced commanders as they seek to frame complex problems. The enemy will use global advantages to rapidly change. Our Capstone Commanders must embrace operational adaptability to stay in front of the enemy’s global advantage. To do so will require continuity in education and experiences as junior Capstone Commanders will be required to adapt at a faster pace than ever before.

End Notes

[1] Chuck Hagel, Quadrennial Defense Review (Washington, DC: U.S. Department of Defense, February 2014), iii.

[2] Quadrennial Defense Review, 27.

[3] ibid., vii.

[4] U.S. Joint Chiefs of Staff, National Military Strategy of the Unites States of America, (Washington, DC: February 2015), 4.

[5] U.S. Department of the Army, The Army Operating Concept, TRADOC PAM 525-3-1 (Ft. Eustis, VA: TRADOC, October, 2014), iii.

[6] Army Operating Concept, 10.

[7] National Military Strategy, 1.

[8] U.S. Joint Chiefs of Staff, Inter-Organizational Coordination During Joint Operations, Joint Publication 3-08 (Washington, DC: U.S. Joint Chiefs of Staff, June 24, 2011), xi.

[9] Jeh Johnson, The 2014 Quadrennial Homeland Security Review, (Washington, DC: U.S. Department of

Homeland Security, 2014), 60.

[10] National Military Strategy, 11.

[11] North Atlantic Treaty Organization Allied Joint Publication 01(D), Allied Joint Doctrine (Brussels, Belgium: NATO, 2010), 3-4.

[12] U.S. Department of the Army, The Army Capstone Concept, TRADOC PAM 525-3-0 (Ft. Eustis, VA: TRADOC, December, 2012), 38.

[13] Army Operating Concept, 19.

[14] ibid., 14.

[15] Strassler, Robert B., Jr. ed. The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War. (New York: The Free Press, 1996), 43.

[16] Martin E. Dempsey, Chairman’s 2nd Term Strategic Direction to the Joint Force, (Washington, DC: U.S. Joint Chiefs of Staff, June 24, 2015), 5.

About the Author

Clarence J. Henderson

Colonel Clarence J. Henderson commands the 72IBCT within the Texas Army National Guard. He holds a B.S. in Botany and an M.S. in Soil Science from Stephen F. Austin State University, and an M.S.S. from the U.S. Army War College.

Available online at : http://smallwarsjournal.com/jrnl/art/capstone-commanders-adaptability-in-the-complex-security-environment

Links:
{1} http://smallwarsjournal.com/author/clarence-j-henderson
{2} http://smallwarsjournal.com/comment/reply/49755#comment-form