Conceptualizing Human Domain Management: Human Network Analysis and Engagement (HNAE) Operations

Norman T. Lihou and Marisol Nieves

*SWJ Editor’s Note: This article is meant to foster dialogue regarding the definition, utility and application of Human Domain Management (HDM) and the principles of Human Network Analysis and Engagement (HNAE) Operations as a concept to be integrated throughout all phases of the planning process and ongoing course of action development.*

**Introduction**

“We cannot solve our problems with the same thinking that created them.”

- Albert Einstein

Countries find themselves in a century where conventional military adversaries are no longer the only threat to their security. Nation state stability is now challenged by drug trafficking organizations, insurgencies, black market traders, criminal organizations, terrorists, cyber-threats, and human trafficking networks to name a few. Decision-makers, policy-makers and military commanders are faced with a myriad of problems that require the identification of emerging conditions, political understanding of local/regional problems, adoption of technology for lethal and non-lethal uses, and anticipating drivers of instability.

Transnational and international problem sets mean that nation states will have to apply a full range of their instruments of national power to find solutions. These instruments usually manifest themselves as Military, Information/Intelligence, Diplomatic, Legal, Infrastructure, Finance, and Economic efforts.

While the military is designed to defend national security and support allies in times of crises; non-traditional threats and hybrid environments mean that the military has to deal with issues that are better suited for the application of a variety of the state’s instruments of power. This expands the need to understand the operational environment past the conventional military threat into the realm of politics, military/security, economic, social, information and infrastructure layers. This information can frame a high-level understanding of the variables within the environment. However, it is the comprehension of how the multiple actors, networks and organizations fit within these systems, and the causal relationships within them, that will truly provide an in-depth understanding that extends past the typical intelligence realm to give the military commander a holistic view leading to better decision making for engagement.
strategies. As the purpose of “intelligence” shifts focus to challenges imposed by new threats, new forms of warfare, new technologies, and new methods for finding peaceful solutions; there is a need to extend our understanding of the Human Domain.

A threat may start as a local disenfranchised ethnic group demanding independence or a transnational criminal organization that grows in power and turns to terroristic activities to undermine the ability of the government to protect its citizens. These irregular enemies have one thing in common; they are all comprised of human actors who seek to unbalance nations to develop a permissive environment. However, these threat networks do not operate by themselves, they are connected to cells/sub-networks and external networks that could include a country's population, ethnic groups, charities, front companies, corrupt officials, compromised border security and complicit government officials.

**The Human Domain**

“We’ve learned some hard lessons over the last 12 years. We went to war without understanding the human domain. We don’t want to make that mistake again.”[i]

- General Raymond Odierno

In his book, “The Utility of Force—The Art of War in the Modern World”, General Rupert Smith (2008), former Deputy Supreme Commander of NATO, introduces his theory of contemporary warfare: “war amongst the people”. General Smith (2008) also calls into mind that Commanders must push past the thought of the threat only being mechanized divisions, fleets of battleships and squadrons of combat aircraft.[ii] These assertions move us to introduce the concept of the “human domain” with added understanding.

The definition of Human Domain is put forth as the “physical, cultural and social environments as it relates to the sphere of human activity that exists within an area of interest, conflict, or military operations other than war”. However, the definition also acknowledges the need to understand all security threats, the social demographic groups of local populations, host nation security/government forces, friendly military forces, international non-government agencies/organizations, external support networks to all of the above, and the interconnectivity between all these elements.

While the human domain is all-encompassing of a country’s environment; friendly forces are concerned with the development of situations through human interaction that lead to the destabilization of a country. This destabilization could necessitate the deployment of international military forces as the host nation losses its capability to neutralize the threat.

The purpose of Human Domain Management (HDM) is to develop cohesive engagement strategies for coordinated interaction with the human networks that exert influence within the area of operations of deployed military forces. This management strategy should commence prior to the deployment of forces as nations seek to bolster the capability of host nations to maintain a secure and safe environment for its citizens. HDM seeks to conduct anticipatory analysis of the participating human networks to help develop engagement operations that lead to the shaping and influencing of operating environment.

**Human Network Analysis and Engagement (HNAE) Operation Fundamentals**
“We have spent the last 12 years working primarily in ungoverned spaces, trying to work out the human dimension,” including the impact of unemployment and poverty. That was necessary because “some of those ungoverned spaces became launching sites for actions against our values, our way of life. The key to the future, is how do you capture that and apply it to training and doctrine?”

- General John M. Paxton, Jr.

The solution is to develop a Human Network Analysis and Engagement (HNAE) Operations discipline that is comprehensive, agile, and adaptable to scenarios ranging from hybrid warfare environments to humanitarian support missions. Understanding of the Human Domain will enable combatant commanders to maintain information dominance and become anticipatory vs. reactive in nature. Lessons learned from the involvement in Iraq and Afghanistan are stark reminders of the need for comprehensive human network analysis and engagement operations, but we must avoid a “tunnel vision” approach regarding the utility of this concept. The goal is to maximize the body of knowledge that will be developed to support any type of mission where our troops will find themselves engaged in a populated area. Conceptually, HNAE Operations are designed to support understanding of the human domain and development of network engagement practices based on an individual nation’s powers and authorities in singular and multinational areas of operation.

In order to shape the area of operations to deny these networks a permissive environment, a unified engagement strategy is needed that takes into account the entire Human Domain. Current doctrine and thought that permeates the government and the military is a concentration on the threat and its activities. Focusing on the threat limits the understanding of the entirety of networks by relying on targeting as the solution to the complex problem. There is a need to go beyond targeting and figuring out the second and third order effects to the other networks as a course of action. Instead operational planners need to engage the threat network while simultaneously engaging the other connected networks to have a holistic approach for setting favorable conditions. In some cases, engagement of the friendly and neutral network may have a higher priority than the threat network to set an environment which limits the ability of the threat network and its reaction. This foundational approach of engagements will require a comprehension of the interconnectivity of the networked environment and the action and reaction between the threat, friendly and neutral networks involved.

**Human Network Considerations**

“To make effective decisions, a person must understand which kind of systems he or she is dealing with, one that is structurally complex or one that is interactively complex. The two systems require fundamentally different decision-making approaches. Structurally complex systems allow for analytical decision-making while interactively complex systems require intuitive decision-making. Extremely difficult problems, sometimes called ‘wicked problems’, are always a result of interactive complexity; they call for systemic decision-making.”

- Lieutenant General Paul Van Riper

Experiences with the study of networks drive a need to highlight the following statements for consideration:
I. Networks are complex adaptive systems that change based on multiple internal/external influences, operational needs, interactivity with other networks/organizations and the changing environment at the tactical, operational and strategic levels.

II. Networks are a complex system of interconnected systems. Networks can be mutually beneficial/sustaining/degrading to other networks; when you affect one part of the system there are secondary and tertiary order effects upon the other networks in the environment.

III. Targeting actions of the leadership or singular actions/tactics against threat networks do not result in any significant degradation of the network’s capabilities. Threat networks are not limited by the rules, regulations, laws, and authorities that friendly and neutral networks have to operate.

IV. Analysis of the threat network alone does not constitute a holistic analysis of the operational environment. We must understand and develop engagement strategies for threat, friendly and neutral networks if we are to shape the area of operation in support of the mission.

V. Engaging networks requires operational cooperation and modalities for lethal, non-lethal and influence operations.

VI. Threat networks can have global effects as technology allows them to acquire weapons of mass destruction and enjoy global connectivity which is equivalent to a nation state. This is accomplished by connections to a multitude of internal and external illicit support networks.

VII. Threat networks find safe harbor and take advantage of contested spaces, neighboring countries that lack the ability or will to engage the threat and vulnerable populations that emerge in unstable environments.

VIII. Network engagement strategies and actions must be designed, developed and carried out with tactical, operational and strategic level coordination to ensure synchronized efforts lead to specified mission support and are in line with Commander’s intent.

IX. The power of networks is the ability of individual actors’ and cells competency to apply personal knowledge, skills, abilities, and resource connections to overcome environmental constraints to accomplish the idea of the network goals. While the network is guided by human behavior, it is not guided by one set of human behavior rules which makes it hard to conduct predictive analysis.

The Ten Basic Principles of HNAE

“**In counterinsurgency, killing the enemy is easy. Finding him is often nearly impossible. Intelligence and operations are complementary. Your operations will be intelligence driven, but intelligence will come mostly from your own operations, not as a “product” prepared and served up by higher headquarters. So you must organize for intelligence.”**

- Dr. David J. Kilcullen

1. Human Network Analysis is led by Intelligence as it fuses information and intelligence to produce anticipatory analysis for engagement operation support while Human Network Engagement is an Operations led cross-coordinated plan of action designed to set favorable conditions for the commanders or decision-makers planning and execution process.

2. HNAE is an Intelligence driven process, however both parts must be synchronized if the engagement is to be effective.

3. Clear understanding of the desired end-state is required for effective prioritization of efforts and resources for HNAE and must be unified/coordinated through engagements at all levels of operations.

4. HNAE must be addressed throughout the five phases of the Operational Planning Process.

5. Every Network Engagement Plan (NEP) must clearly define the lines of effort (LOEs) applied to
each network: Friendly, Threat, Neutral. These lines of effort must support the Commander’s intent. Each activity within a line of effort must contain a description of the authorities, coordination, logistics, collection, engagement capabilities and measure of performance /measure of effectiveness for that specific line of effort.

6. Engagement activities should include all interconnected networks that affect the desired end-state objectives; engagement types may include lethal (targeting), non-lethal and influence operations. Engagement recommendations must take into consideration 2nd and 3rd order effects upon the realm of all networks (friendly, threat, neutral).

7. HNAE efforts must be coordinated through all levels (tactical, operational, strategic)

8. HNAE requires a “whole of governments approach” that should include joint, inter-agency, inter-governmental and multinational coordination and cooperation.

9. HNAE requires a coordinated Staff effort that extends past the J2/J3.

10. HNAE has a set of critical capabilities required for the performance of this process:

a. The capability to detect/collection information regarding networks of interest
b. The capability to conduct analysis for local, global and regional network threat assessments
c. The capability to comprehend causal relationships between local, global and regional threat networks
d. The capability to share and disseminate information
e. The capability to engage all connected networks to obtain a desired effect
f. The capability to obtain meaures of performance and measures of effectiveness

Summary

“Operations in the “human domain” provide a unique capability to preclude and deter conflict through shaping operations that leverage partners and populations to enhance local and regional stability. [vi]“

- General Raymond T. Odierno, US ARMY, Chief of Staff
- General James F. Amos, USMC, Commandant
- Admiral William H. McRaven, Commander, USSOCOM

While there may be those who claim that these types of activities are carried out during Counter-insurgency (COIN) or counter-terrorism (CT) operations, and this is nothing new, the truth is that COIN and CT historically focus their efforts on reactive engagement of the threat networks.

HNAE Operations for Human Domain Management are designed to support the greater concept of Strategic Land Power; not concentrating on only the combatant threat network, but looking to provide the Commander/policy maker with a holistic picture of the activities and resources required to engage the human networks prior to deploying their forces. This is a change of perspective which requires concentration on indicators of emerging issues in an area that could turn into a focus of transnational and international problem sets. It also entails the need to expand our ideas of threats and warnings to include developing disputes that could sway populations to galvanize towards violent action or become victims of disenfranchised networks who seek to harm others.

To engage the networks is to use lethal and nonlethal means to support, influence, or neutralize network members or cells or an entire network.[vii] This concept moves far beyond lethal targeting of individuals
to apply a holistic approach of understanding the human terrain in support of Human Domain Management. We must learn from our experiences that it is necessary to engage the Friendly, Threat and Neutral networks simultaneously in order to expedite achievement of a desired end state where deployed military forces can return the area to host nation and local authority. This is a “whole of governments” effort requiring specific capabilities a nation may or may not have. Any network engagement plan (NEP) must take into account the deployed nation’s or nations’ authorities, capabilities, powers and national restrictions or limitations.

End Notes

[i] General Raymond Odierno, Army chief of staff, at an Oct. 23 forum on Strategic Land Power at the Association of the United States Army’s Annual Meeting and Exposition at the Washington Convention Center.


[iii] Gen. John Paxton, Assistant U.S. Marine Corps Commandant, in a panel moderated by Gen. Robert Cone, Commanding General of the Army Training and Doctrine Command. In opening the forum, Cone said the panel was part of the joint effort to “see if we can capture some of the lessons on strategic land power” learned in the 12 years of conflict.


[v] David Kilcullen is renowned for his expertise on counterinsurgency and was lead advisor to General David Petraeus in Iraq. He authored “The Accidental Guerrilla” and also serves as an advisor to NATO.

[vi] Strategic Landpower: Winning the Clash of Wills


About the Authors

Norman T. Lihou

Norman T. Lihou has twenty-seven years of experience as an intelligence professional in the Intelligence Community. With multiple deployments to Iraq and a tour of Afghanistan, he has worked the terrorism/threat network problem set since 1985. Recent analysis concentrated on cross-boundary network analysis of key individuals whose connections enabled multiple insurgency capabilities and threats in Afghanistan and Pakistan. He has taught at the US Army Intelligence Center of Excellence, Defense Intelligence Agency, National Defense University, Army War College, NATO C-IED Center of Excellence and the Joint Forces Training Centre.
Marisol Nieves

Marisol Nieves is a master training specialist with 15 years of experience developing and delivering military education and training programs for the Army, Navy and Marine Corps. She is a prior Navy Senior Enlisted with experience supporting Marine units in the Iraqi theater of operations. Her experience includes assignments at the Office of Naval Intelligence, National Ground Intelligence Center and currently as Chief of the Curriculum Development Branch at the Counter-IED Operations Intelligence Integration Center (COIC).

Available online at: http://smallwarsjournal.com/jrnl/art/conceptualizing-human-domain-management

Links:
{1} http://smallwarsjournal.com/author/norman-t-lihou
{2} http://smallwarsjournal.com/author/marisol-nieves

Copyright © 2014, Small Wars Foundation.

Select uses allowed by Creative Commons BY-NC-SA 3.0 license per our Terms of Use. Please help us support the Small Wars Community.