Precision Warfare

Advanced network analysis driving decisive action

by Maj Mackenzie Gage & Mr. Adam Jonas

The modern operating environment is composed of many actors: friendly, enemy, and neutral. Each actor is "not a unitary mass but a complex system of interacting components."[1] Nowhere is this more apparent than in the first island chain, where the Marine Corps and Joint Force's linear thinking struggles to engage these networks to achieve a meaningful advantage. Current network engagement methods fall short in addressing Operations in the Information Environment (OIE). Effectively engaging these complex networks is critical to Target Audience Analysis, Civil Network Development & Engagement, and OIE Conduit Analysis. To influence, neutralize, or destroy key networks across the competition continuum, significant advancements in training are required.[2] A new methodology—Joint Advanced Network Analysis (JANA), anchored in network science—is essential for achieving information advantage and integrating information forces into a combined-arms approach. Although information forces may provide the solution, the issue impacts the total force.

Joint Advanced Network Analysis is a framework that allows Marines to view systems, including kill chains and influence networks, through relationships among people, locations, events, resources, and organizations. This approach helps Marine information forces identify and disrupt components within enemy systems across dimensions and domains. By exploiting relationships among the interacting components—such as the "enemy's command structure, the geographical disposition of their forces, the reliance on a particular capability, the interaction of different combat arms, the relationship of forces with the population, or an individual's belief in the cause"—JANA supports both non-kinetic and kinetic effects, including counter-targeting to disrupt adversary kill webs.[3] Unlike traditional target system analysis, JANA offers a broader framework for influencing neutral networks and targeting enemy networks.[4]

>Maj Mackenzie serves with III MEF G39.

>>Mr. Jonas works with ThreatTec LLC in Support of TRADOC G-2 Network Engagement Team.

Currently, military information support operations (MISO) detachments are unable to effectively identify and leverage key communicators within target audiences to reinforce desired behaviors or counter malign propaganda.[5] Similarly, civil affairs teams lack the training and methodologies needed to identify relevant actors and develop effective engagement plans.[6] Additionally, OIE Conduit Analysis is hindered by the absence of analytical tools to identify and model key conduits for information flow from sensors to decision makers.[7]

Network science is an applied research paradigm used to understand complex adaptive systems like influence, social movements, governance, and innovation diffusion making JANA highly relevant to MISO, civil affairs (CA), and efforts ranging from Force Design to task-organized unit C2.[8] Predecessors to JANA were initially adopted by the Marine Corps, Army, and joint special operations for targeting terror and IED cells during the Global War on Terror, where its broader applicability was recognized by forward-thinking doctrine writers.[9] Elements of advanced network analysis (ANA) have been adopted into high-level joint doctrine such as *JP 3-53 Joint Military Information Support Operations* (2024), *JP 3-60: Joint Targeting* (2024), and *JP 3-25 Joint Counter Threat Networks* (2023), *MCTP 3-02A, Network Engagement Activities* (2017, revised in 2022), *ATP 5-0.6*, *Network Engagement* (2016, awaiting revision) *FM 3-57, Civil Affairs Operations* (2021), and spreading to twenty publications across Marine, Army, NATO, and joint doctrine within a decade.

Joint Advanced Network Analysis is based on the principles of network science, a well-developed interdisciplinary field used widely in government, business, and academia to understand the complex connections among actors. Joint Advanced Network Analysis uses a data-driven approach to evaluate and affect the social, informational, and operational networks that underpin modern competition and conflict. Thus, it offers a critical capability enabling effective information operations and civil-military operations, and it provides important information supporting the fire and maneuver warfighting functions. For example, JANA provides measures that identify possible key influencers based on network structure (e.g., Key-Player, PageRank, and Closeness Centrality) and graphical representations supported by statistical analysis for information conduits (identification of shortest paths between nodes) and can algorithmically identify nested groups that may share a common identity to help refine messaging (e.g., community detection algorithms). Furthermore, JANA can be combined with data from polling, sentiment analysis, narrative detection, and other tools to gain an information advantage and assess operations.

Although ANA techniques are in doctrine and widely used in the

private sector and academia, they remain dramatically underutilized in OIE. In 2015, the United States Army Special Operations Command (USASOC) Psychological Operations Regiment identified gaps in target audience analysis training and tools, including the inability to identify relevant actors—an issue that persists for Marine Corps information forces and USASOC.[10] To address a similar gap, the 95th Civil Affairs Brigade established human network analysis cells in 2018, with operational successes leading to civil network analysis becoming a core competency for Army special operations civil affairs.[11] However, training in human network analysis/civil network analysis remains insufficient, as noted by USASOC and civil affairs journals. Despite having similar METs among USASOC PsyOp/CA forces and Marine Corps influence forces, advanced network analysis training and skill validation are still lacking across exercises and deployment rotations.

To better engage networks in competition and modern conflicts, the Marine Corps must become proficient in advanced network analysis, but current training is inadequate. Training and Education Command's NET3C introduces foundational concepts but lacks the depth needed for operational utility at scale. This is compounded by the train-the-trainer model, limited student throughput due to high op tempo, insufficient software, and data sets to support meaningful practical application. Advanced methods are taught by the Joint National Training Center-funded Army TRADOC G-2 Network Engagement Team and by the Naval Postgraduate School's CORELab. Combined, this amounts to fewer than ten instructors for the entire Joint Force. This capacity gap leaves the United States struggling to compete with China's *Intelligentized Warfare*. China now outpaces the United States academically in network science research and has written in the official news source of the People's Liberation Army (PLA) about network science, not only for military operations but as a way to structure the PLA.[12] In this PLA publication, they aptly state the following (translated from Mandarin Chinese):

> The network information system not only can serve as a "multiplier" of "1+1>2" in aggregating combat forces that are widely distributed and have heterogeneous functional role, it can be damaged or controlled by destroying key nodes in the network information system, creating a destruction "multiplier" effect of "100-1=0,"

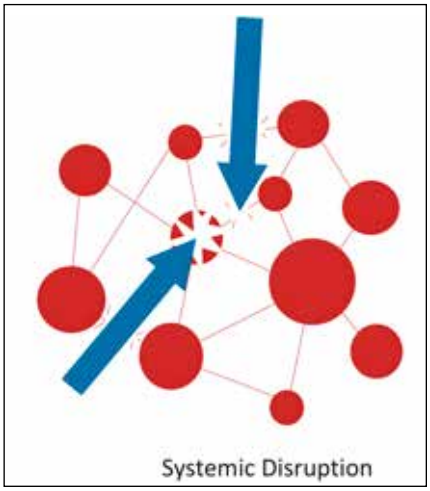

Figure 1. Achieving systemic disruption through the deletion of key nodes and linkages. *(Source: Marinus' "On Defeat Mechanisms.")*

To address this gap, influence Marines and Marine information forces should receive advanced training aligned across joint information forces within their MOS pipelines. Early integration of this training fosters a network science mindset and capability density to compete effectively with pacing threats. Applying a JANA framework at all echelons—battalion, regiment, major subordinate command, and MEF—enables decisive advantage. Joint Advanced Network Analysis maximizes the effects that can be achieved by limited forces. Figure 2 compares the doctrinal rules of allocation (ROA) for PsyOp forces with the Marine influence forces' undersized force alignment and larger mission set.[13] Joint Advanced Network Analysis, integrated at scale, is vital for OIE planners, MISO, CA, force protection/resiliency, and kinetic targeting. It offers a means to disrupt

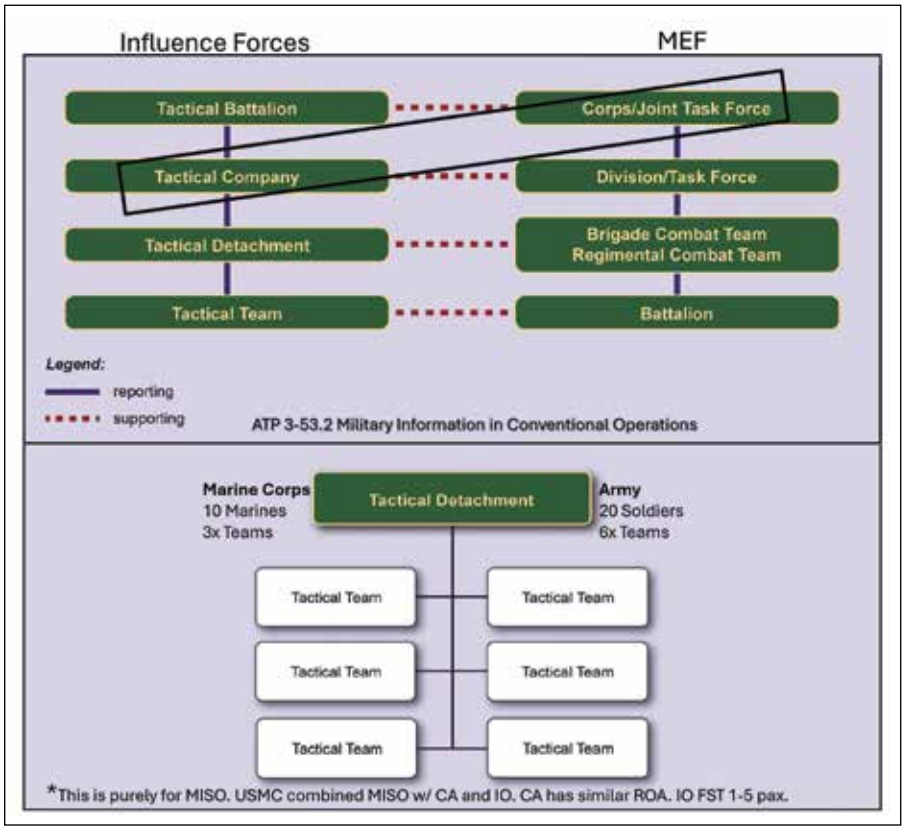

Figure 2. ROA for influence force and MEF Figure 2. *(Source: ATP 3-53.2 Military Information in Conventional Operations.)*

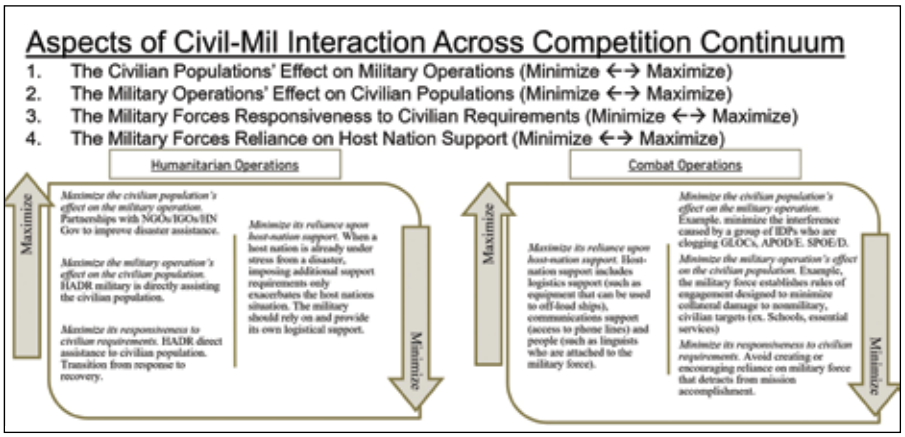

Figure 3. JANA's applicability to civilian-military operations enables precise applications of effects across this continuum. *(Figure provided by author.)*

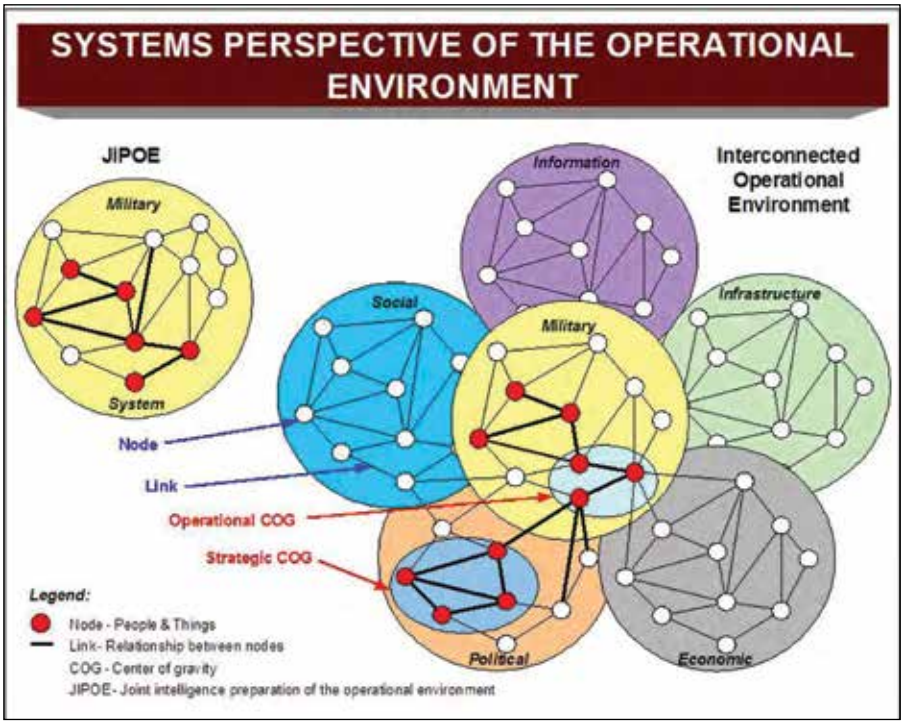

Figure 4. JANA is a toolkit for quantitative analysis across the PMESII spectrum as described by JP 3-0, JP2-01.3, and JP5-0 yet is drastically undertrained. *(Figure provided by author.)*

enemy systems efficiently. The following MISO/CA case studies, though fictional, are based on real-world JANA applications.

Case Study 1: JANA for Marine CA

Advanced network analysis enables CA teams to analyze public and commercial data (PAI/CAI) to identify key networks and relevant actors across the PMESII spectrum (see Figures 3 and 4 on following page).[14] Even in denied areas, JANA techniques, such as closeness and betweenness centrality, allow Marine Information Forces to pinpoint relevant actors, organizations, locations, and events critical for focused engagements. This creates a tangible information advantage, the ability to minimize/maximize effects from civilian-military interaction, as units prepare to enter contested areas.

Building on successful Army CA missions, this notional case study highlights how "Civil Network Development and Engagement" leveraged ANA to uncover foreign influence actors and vulnerabilities in host-nation governance and infrastructure.[15] After 40 hours of network analysis training, CA teams used a common template spreadsheet to identify relationships from engagements and PAI/CAI. This data was quickly imported into ANA tools (OEVis and Gephi), enabling rapid visualization of large amounts of data connecting actors in their area of operations.[16] Through the detailed understanding of these networks, key actors connected with adversarial countries spreading malign narratives in the area of operations were identified. The analysis enabled teams to assess the proximity and access of these actors to friendly networks, informing engagement planning to strengthen resilience in partner networks and isolate malign actors. This same framework also identifies gaps/opportunities among nongovernmental organizations, intergovernmental organizations, the private sector, and host-nation governments.[17] By focusing on friendly and neutral networks, JANA increases host-nation support available to U.S. forces, reduces civilian reliance on military aid, and improves responsiveness to the civilian population's needs when required. Collaborative data sharing among partners enhances the approach, addressing gaps created by less formal hierarchical relationships outside the military. The ability of CA professionals to develop these networks increased the host nation's capacity at little cost, mitigated malign influence, and supported other operations. This underscores the value of the JANA-network-based engagement approach to solving complex operational challenges and countering PRC Intelligentized Warfare.

The friendly/neutral focused analysis is crucial in INDOPACOM, where combined operations/coalition warfare and collective cultures predominate.[18] Combinations of bilateral mechanisms like Korea's Combined Forces Command and Japan's Bilateral Coordination Centers may leave exploitable gaps for PRC Intelligentized Warfare. However, JANA can proactively identify weak links and critical nodes in coalition structures, allowing resilience/

redundancy solutions to be implemented. Additionally, with collective cultures in the first island chain context, individuals rely heavily on known contacts and trusted in-group information and recommendations. It is essential to understand their networks to be able to effectively engage them.

Case Study 2: JANA for Marine MISO

Network science is widely used for understanding and accelerating the spread of information and influence; it can be applied to combating illegal unlicensed and unregulated fishing (IUUF), a significant maritime security threat outlined in the current U.S. *National Defense Strategy*. Public and commercial data from aggregators of vessel tracking data, such as Skylight, provide large open-source datasets of IUUF ship encounters, port calls, and where ships are flagged. Using JANA and enabled with a government-owned tool, such as OEVis, an analyst can build a large network in just a few hours. The resulting visualization and detailed understanding can identify the most important ships in a network and where and when they encounter others at sea and in port. This enables precise Target Audience Analysis to focus on actors involved in IUUF. Integrating additional data into OEVis can then show linkages such as organizational ties, communications, social media ties, and co-attendance of events. This massive network can then be analyzed using measures such as PageRank. PageRank is an algorithm originally developed by Google to rank webpages, which has also been found to find individual nodes in networks that are the most central among other highly central figures key communicators among the TA's network.[19] Additionally, community detection can be employed to identify important groups based on the social structure of the network, enabling precise refinement of a target audience. It may be known that many of the workers at a given port have certain demographics, such as being males of a certain ethnic group and religion. However, mapping the network may reveal that the region people immigrated from is the most important variable in who communicates with whom. It may also reveal that demographics don't define target audiences in a particular area. Understanding these groups increases access to additional PAI/CAI, such as their social identities, groups they follow, products they buy, and media they consume. This deeper understanding guides tailored MISO series, optimizing message propagation and increasing the likelihood of behavioral change. Advanced network analysis can be applied to the network of only a key leader or a large target audience operating on a large social media platform, allowing for very specific conduit analysis and even identification of the shortest paths possible for a message to travel. This type of analysis also leaves the possibility for using agent-based models or artificial intelligence to model the diffusion of information or influence through a target audience. Lastly, the network can be used to generate measures of performance and effectiveness that can be quantitatively measured.

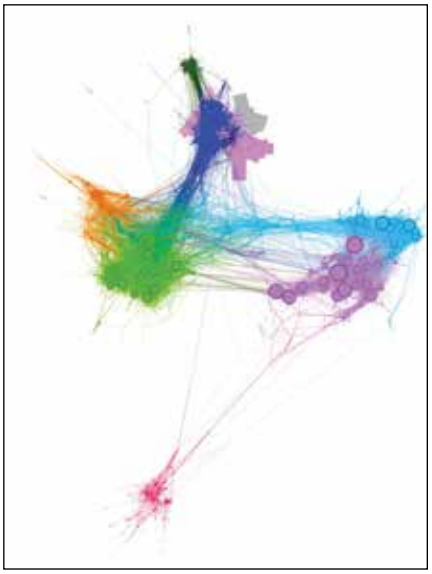

Figure 5. Network of 5,793 vessels suspected of IUUF's 26,051 at-sea encounters. Nodes are sized by being central among other highly central vessels, indicating influence (PageRank Centrality), and color is based on algorithmically defined groups (Louvain Community Detection).[20] ***(USMA CDT Angelina Pfister in support of TRADOC G-2, data is publicly available from Global Fishing Watch https://globalfishingwatch.org/datasets-and-code.)***

The precision JANA generates "second-wave propagation," which spreads behavior rapidly, especially in collective cultures reliant on social networks for trusted information.[22] Figures 5 and 6 demonstrate two applied operational uses. With robust availability even at the tactical edge due to the prominence of advertising technology and proliferation of increasingly connected technologies, it is easier than ever to enable this type of analysis.[23] Combining network science centrality measures can not only identify relevant actors and key communicators in a network but can also assist in leveraging them to generate effects.[24] When supported by intelligence activities, it can categorize the types of relevant actors and key communicators

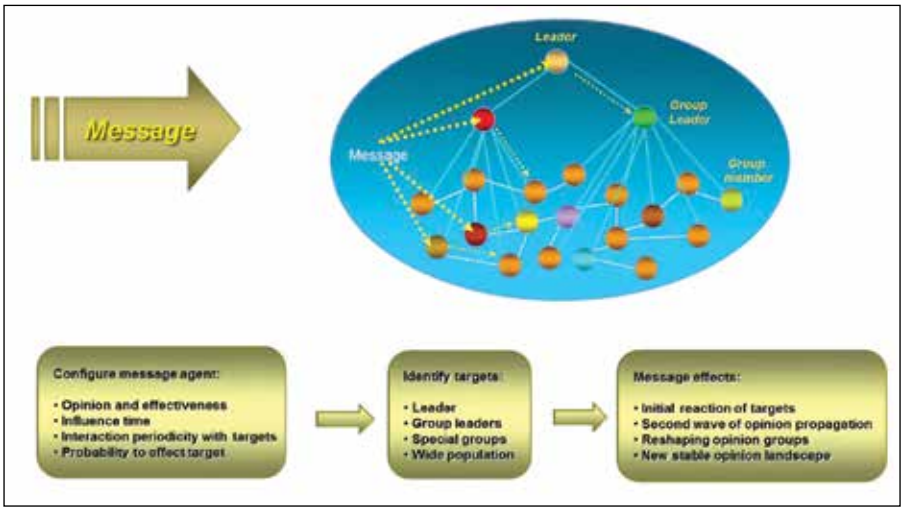

Figure 6. Using ANA to track message propagation and impact across a social network from Casebeer 2018.[21] ***(Photo credit: Casebeer 2018.)***

based on how they interact with the rest of the network.[25] Without advanced techniques, relevant actors and key communicators are identified superficially using subjective methods that may be highly inaccurate. Additionally, ANA enables influence Marines to distinguish the difference between an effective adversary propaganda campaign and ineffective noise in the information environment. People and organizations within the network that are effectively spreading a counter-narrative can be identified and mitigated, while those that can propagate our narrative may be enhanced to drive the desired behavior in the target audience. This can be done through identifying the overlaps between friendly, adversary, and neutral networks, compared to where messaging is injected into the network by adversary or friendly forces.

For the Marine Corps to achieve success at this level, investment is required across the capability-based assessment framework.

The Way Ahead

Successful implementation of JANA allows Marine information forces to identify and assess networks that can threaten, hinder, or support military operations within a defined area. Once a network is discovered, opportunities can be identified to further develop and engage it. Specifically, friendly networks must be amplified, reinforced, or protected, while neutral networks are optimized as necessary to support the commander's objectives and intent. Threat networks, on the other hand, must be mitigated or monitored. For the Marine Corps to achieve success at this level, investment is required across the capability-based assessment framework. This is not a materiel solution; rather, it is an investment in humans over hardware.

Doctrine already exists outside the Marine Corps to provide an excellent starting point for the Information Maneuver community to adopt this comprehensively across Marine Corps doctrine. Examples include the *Civil-Military Engagement Development-Joint Targeting/Non-Lethal Handbook*, *Soldier Training Publication (STP) 41-38R-SM-TG for Civil Reconnaissance Sergeants (MOS 38R), ATP 3-57.30 Civil Network Development and Engagement*, and *ATP 5-0.6 Network Engagement*. Organizationally, the Information Maneuver occupational field, specifically MOS 1751 and 1707, provides the resident structure to integrate these TTPs at echelon across the FMF. Training would likely be a short two-week investment in the existing Influence PMOS production pipeline; this could likely be offset by removing redundant periods of instruction on the Marine Corps Planning Process. The Marine Corps Planning Process, although important, is taught by Education Command at resident and non-resident schools, and is a simple planning process that can truly be learned by doing, as most MEU component staffs do. In the 2024 Influence PMOS pipeline, it is taught both at the Civil Affairs School and at the MAGTF OIE Practitioners Course. This is in addition to being taught the Army's version—Military Decision-Making Process at Psychological Operations Qualification Course. The key to effective training is the practical application available, as well as the appropriate instructional personnel. A team including a network science subject-matter expert and an individual with robust joint/interagency operational experience using network analysis is likely the right fit. The Army's TRADOC G2 Network Engagement Team models this structure. It provides unmatched training on social network analysis (using a government-owned tool—OEVIS—and robust real-world datasets. Funded by the Joint Staff Joint National Training Capability, it provides training across the Joint Force. This is an essential requirement—using the same network science approaches enables global interoperability to win a global competition across combatant commands.

Note

1. Marinus, "On Defeat Mechanisms Manueverist Paper No. 10," *Marine Corps Gazette* 105, No. 7 (2021).

2. *NAVMC 3500.124A* contains the collective event "MIG-OPNS-8002 Direct Network Engagements" as a key event enabling MCT 5.14 Conduct OIE. There are no individual training and readiness events to provide information for the baseline to contribute to this. In a 2015 Naval Postgraduate School Paper, "Bridging the Gap: Enhancing SNA within the Marine Corps Intelligence Community," Robert Schotter identified gaps with Marine intelligence professionals' ability to support this as well. To date, the training and readiness manuals for these communities also do not address it, with only references to doctrine for the intelligence community—*NAVMC 3500.100C*—and one T&R for the signals intelligence community in *NAVMC 3500.105C.*

3. "On Defeat Mechanisms Manueverist Paper No. 10."

4. Countering adversary kill webs only requires a deeper application of network engagement doctrine and a revision of concepts from the "Attack the Network" teams and The Asymmetric Warfare Group, many of which are available in the Joint Lessons Learned.

5. This gap was originally identified in a 2015 gap assessment by the Psychological Operations Regiment as reported in Ashley Franz Holzmann, "Artists of War: A History of United States Propaganda, Psychological Warfare, Psychological Operations and a Proposal for its Ever-Changing Future," (thesis, US Army Command and General Staff College, 2020). The possibilities of leveraging advanced network analysis to identify key communicators are covered in depth in: Andrew A. Sadoun, "PSYOP and Social Networks," (thesis, Naval Postgraduate School, 2018). As well as: Mariah Yager, "What Do Others Think and How Do We Know What They Are Thinking?" *Joint Staff Strategic Multilayer Assessment Whitepaper* (2018).

6. Aside from the current existing doctrine, *ATP 3-57.30 Civil Network Development and Engagement*, readers are encouraged to seek out:

Office of the Secretary of Defense, *Civil-Military Engagement Development-Joint Targeting/Non-Lethal Handbook* (Washington, DC: 2016).

7. See the following for a rudimentary but detailed and data-backed example from violent extremist organizations and government forces in the Democratic Republic of Congo: Patrycja Stys, Judith Verweijen, Papy Muzuri, Samuel Muhindo, Christoph Vogel, and Johan H. Koskinen, "Brokering Between (Not So) Overt and (Not So) Covert Networks in Conflict Zones," *Global Crime* 21, No. 1 (2020).

8. For the direct application of ANA to MISO see: Adam Jonas, Patricia DeGennaro, Christopher Worret, and Randall Munch, "Social Network Analysis for Influence & Intervention to Advance Military Information Support Operations: Combining the Social and Bio-Cognitive," *Strategic Multi-Layer Assessment (SMA).* Joint Staff, October 2016. See Nick Crossley and Mario Diani's chapter "Networks and Fields" in *Wiley Blackwell Companion to Social Movements* (Hoboken: Wiley, 2017). For applicability to *Force Design* or similar efforts, there are reports available in JLLIS (Joint Lessons Learned) by searching "Expanded Organizational Mapping Background" and "Organizational Mapping." For an example covering how organizational mapping can be applied to C2 see: Robert J. Houghton, et al. "Command and Control in Emergency Services Operations: a Social Network Analysis," *Ergonomics* 49, 10 (2006). The authors can provide organizational mapping results upon request.

9. Recommend reading, *How Behavior Spreads* by Damon Centola as an introduction to how advanced network analysis applies to these and their related military fields.

10. See Headquarters Department of the Army, *FM 3-24, Insurgencies and Countering Insurgencies* (Washington, DC: 2006); David Knoke, "It Takes a Network: The Rise and Fall of Social Network Analysis in U.S. Army Counterinsurgency Doctrine," *Connections* 33, No. 1. (July 2013); and Brian Reed, "A Social Network Approach to Understanding Insurgency," *Parameters* 37. No. 2 (Summer 2007).

11. See Ashley Holzman, "Artists of War," (master's thesis, Command and General Staff College, 2020); and Patrick McKinney, "PSYOP Technical Manual to Address the Complexity of Influence," *Special Warfare* 32, No. 1 (2019).

12. Department of the Army, *FM 3-57, Civil Affairs Operations* (Washington, DC: 2021); Department of the Army, *ATP 3.57.30, Civil Network Development and Engagement* (Washington, DC: 2023); and Roland Molontay, and Norbert Nagy, "Twenty Years of Network Science: A Bibliographic and Co-Authorship Network Analysis," (2020).

13. See *Chinese Strategists Consider Weaponizing "Complexity Science"* by U.S. Army TRADOC G-2 Foreign Military Studies Office 2024. Available at https://fmso.tradoc.army.mil/2024/chinese-strategists-consider-weaponizing-complexity.

14. Figure 2 is from *ATP 3-53.2 Military Information in Conventional Operations* with adjustments made to show the variance between this doctrinal ROA and Marine Corps Information Force Design. Figure 3 created by SSgt Duncyn Neta, 3d Information Maneuver Company, III MIG, III MEF. Derived from *Special Warfare* Summer 2000, "The Minimize-Maximize Continuum and the Civil Military Operations Mission." Figure 4 from *OSD CMED-JT/NL (Civil-Military Engagement Development-Joint Targeting/Non-Lethal) Handbook.*

15. Examples of applications PMESII spectrum. For Political see: Margaret Mikkelsen, "Policy Network Analysis as a Strategic Tool for the Voluntary Sector," *Policy Studies* 27, No. 1 (2006); and Michael M. Atkinson and William D. Coleman, "Strong States and Weak States: Sectoral Policy Networks in Advanced Capitalist Economies," *British Journal of Political Science 19,* No 1 (1989). For Military see Michael C. Case, "An Organizational Network Analysis of the Sprawling US Department of Defense Innovation Ecosystem" (PhD Dissertation, MIT, 2024). For Economic see Yun-Jung Lee, Su-Do Kim, Jang-Pyo Hong, Hwan-Gue Cho, and Seong-Min Yoon, "Industrial Network Analysis Using Inter-Firm Transaction Data," *Indian Journal of Science and Technology 9,* No. 26 (2016); Fernando DePaolis, Phil Murphy, and M. Clara De Paolis Kaluza, "Identifying Key Sectors in the Ional Economy: A Network Analysis Approach Using Input-Output Data," *Applied Network Science 7,* No. 1 (2022); Jianxi. Luo," The Power-of-Pull of Economic Sectors: A Complex Network Analysis," *Complexity* 18, No. 5 (2013); Theodore Tsekeris, "Network Analysis of Inter-Sectoral Relationships and Key Sectors in the Greek Economy," *Journal of Economic Interaction and Coordination* 12 (2017). For information, see Jukka Hallikas, Jari Varis, Heli Sissonen, and Veli-Matti Virolainen, "The Evolution of the Network Structure in the ICT Sector," *International Journal of Production Economics* 115, No. 2 (2008). For Infrastructure see Citra Ongkowijoyo and Hemanta Doloi, "Determining Critical Infrastructure Risk Using Social Network Analysis," *International Journal of Disaster Resilience in the Built Environment* 8, No. 1 (2017).

16. Department of the Army. *FM 3-57, Civil Affairs Operation*s (Washington, DC: 2021), Department of the Army, *ATP 3.57.30, Civil Network Development and Engagement* (Washington, DC: 2023).

17. For more on the TRADOC G-2 Network Analysis Tool OEVis see oe.tradoc.army.mil/oe-vis-operational-environment-visualization. For more on the French open-source Network analysis tool Gephi, see gephi.org.

18. This approach is often used to enhance business performance and is referred to as organizational network analysis (ONA). This article outlines how it can be accomplished simply by using email traffic as the data source: John Graham and Daniel B. Horn, *Technical Report 1218, IkeNet: Social Network Analysis of Email Traffic in the Eisenhower Leadership Development Program* (Fort Belvoir: U.S. Army Research Institute for Behavioral and Social Sciences, 2007).

19. This measure is a more modern replacement for Eigenvector centrality, which is mentioned in doctrine to help identify potentially influential nodes.

20. Geert Hofstede, Gert Jan Hofstede, and Michael Minkov, *Cultures and Organizations: Software of the Mind. 3rd Ed* (New York: McGraw-Hill, 2010).

21. Visual developed by USMA CDT Angelina Pfister for TRADOC G-2 from publicly available Global Fishing Watch data on vessels suspected of IUUF https://globalfishingwatch.org/datasets-and-code/2024.

22. William D. Casebeer, "Narrative Technology to Detect and Defeat Adversary Ideological Influence," *Strategic Multilayer Assessment (SMA)* White Paper (March 2018).

23. Andrew A. Sadoun, "PSYOP and Social Networks," (thesis, Naval Postgraduate School, 2018).

24. These measures could include betweenness/eginvector/closeness centrality and degree of centrality.

25. Malcolm Gladwell, *The Tipping Point: How Little Things Can Make a Big Difference* (New York: Little, Brown and Company, 2000). Gladwell identifies three types of actors that are key to driving behavior change.