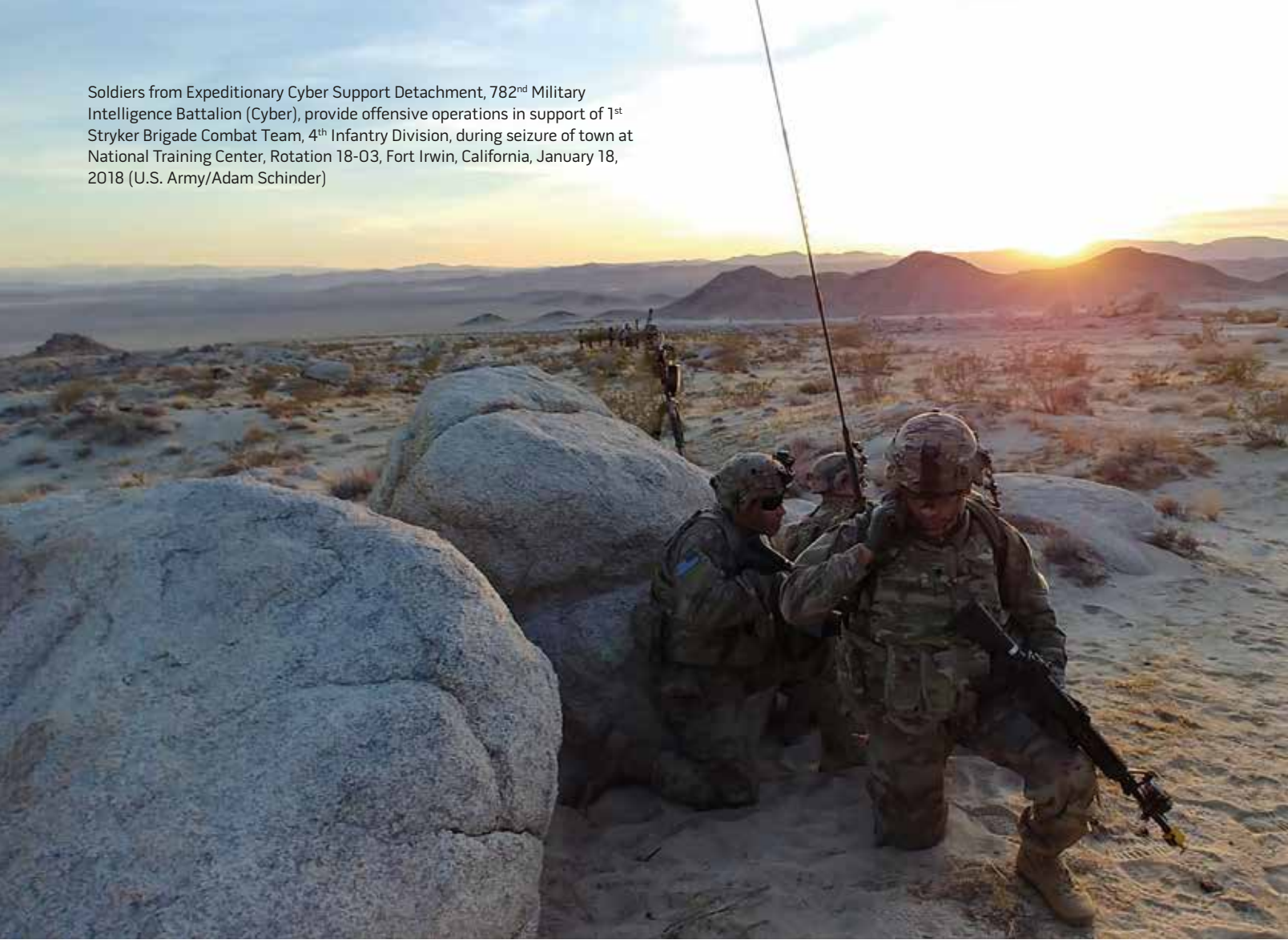

Soldiers from Expeditionary Cyber Support Detachment, 782nd Military Intelligence Battalion (Cyber), provide offensive operations in support of 1st Stryker Brigade Combat Team, 4th Infantry Division, during seizure of town at National Training Center, Rotation 18-03, Fort Irwin, California, January 18, 2018 (U.S. Army/Adam Schinder)

Outmatched

Shortfalls in Countering Threat Networks

By David Richard Doran

Our adversaries employ threat networks to create conditions in the operating environment that undermine international order and rule of law—without triggering a decisive military response. Taking a cue from Sun Tzu, in many areas they are winning without fighting, but by employing means that we consider nonmilitary. These persistent simultaneous efforts unbalance joint force footing by causing regional instability, damage to legitimacy, degraded access, conduits for weapons and fighters, and ultimately pathways for attacks against the homeland. Understanding how adversaries use threat networks globally to compete with us below the threshold of traditional armed conflict is a critical first step to identifying opportunities to exploit, disrupt, or degrade threat networks. However, the increasing convergence of legitimate and illicit networks complicates our ability to gain the level of understanding required to do this effectively. A dilemma thus ensues: Commanders are encumbered with problems for which the optimal

Lieutenant Colonel David Richard Doran, USA, is a Joint Strategic Planner in the Office of Irregular Warfare, Joint Staff J7.

(or only) solutions are often nonmilitary, representing a condition that is anathema to our culture and, as such, incongruent with our processes.

The joint force is not postured to effectively counter these threat networks at a level that matches, or much less overmatches them. Historically, when faced with emerging challenges that could not be addressed using extant practices, processes, or capabilities, such as the proliferation of improvised explosive devices or weapons of mass destruction, we did not accept a casual, disjointed approach to countering them. Accordingly, we should not attempt to counter threat networks through ad hoc ways and means but rather adopt a deliberate approach, rooted in policy, enshrined in doctrine, instilled in our institutions, and understood throughout the joint force.

Leaders and planners must embrace a deeper understanding of the role that threat networks play in shaping the global environment so that they can effectively counter them and prevent adversaries from threatening U.S. interests. Achieving this seismic shift in how we think about threat networks will allow us to harden our blue network, closing gaps and seams that adversaries are otherwise able to exploit. It requires a comprehensive approach—spanning organizational, functional, and institutional boundaries—to develop an integrated framework for countering threat networks (CTN).

Threat networks are described in joint doctrine as those whose size, scope, or capabilities threaten American interests. These networks may include the underlying informational, economical, logistical, and political components to enable these networks to function. These threats create a high level of uncertainty and ambiguity in terms of intent, organization, linkages, size, scope, and capabilities. They also jeopardize the stability and sovereignty of nation-states, including the United States.[1]

Consider Russian organized crime, Chinese drug trade, North Korean weapons proliferation, Iranian terror exportation, financing, and recruiting by the so-called Islamic State. What do all of these have in common? Among other things, they actively employ nonmilitary enabling networks to achieve strategic objectives within what we call the Gray Zone, Phase 0, and competition short of armed conflict.[2] Joint planners must navigate an operating environment made increasingly more complex by the deliberate employment of these networks. Decisionmakers rely on analysts and planners to develop comprehensive threat pictures and associated response options and plans, but these are often incomplete for several reasons. First, these networks often manifest across the spectrum of threat activities as decentralized, fluid, and resilient webs of loosely connected nodes, making them hard to illuminate. This is further complicated by the diverse natures of these networks, which range from illicit to legitimate or somewhere in between, making them difficult to target. Finally, military adversaries use them to avoid direct military engagement (even attribution) while gaining relative advantage against the joint force, making them hard to defeat.

As a military function, CTN is somewhat of an orphan. It is not exclusively a problem that the joint force owns outright, but one requiring integration of military and nonmilitary applications of national power. Threat networks are not exclusively a counterterrorism problem. We cannot waive it off as an unconventional warfare problem or one with a special operations forces solution. We certainly cannot shrug it off as simply a diplomatic or law enforcement problem. We also cannot afford to pigeonhole CTN into one or two lanes or job jars; there must be *cross-functional* ownership.

We have to operationalize key players from within each element of national power to work together in a concerted effort, combining their unique skills and authorities. It is this constellation of organizations and entities that makes up the enterprise involved in countering threat networks. While there is a broad range of capabilities that can be brought to bear in the effort, CTN skill-sets generally fall into the following disciplines:

- threat network targeting
- counter-threat finance
- law enforcement
- counter-message
- counter–transnational organized crime
- counternarcotics
- counterinsurgency
- counter–weapons of mass destruction
- friendly network engagement
- counterterrorism
- social network exploitation
- publically available information exploitation
- cyber operations
- information management
- counterintelligence.

2017 CTN Study

The Joint Staff J7 Office of Irregular Warfare (OIW) conducted a study to review and optimize the enterprise

From Coordination to Collaboration to Integration

"After 9/11, the U.S. Government was compelled to confront its weaknesses in interagency coordination, and while we have made tremendous progress in the intervening years, I believe we have mostly exhausted the strategic value we could derive from improved coordination. This explains why, over the past several years, we have increasingly been using the word *collaboration*—which requires far more than just information-sharing and operational synchronization. It requires doing things together as an interagency team for temporary but important purposes. We have made even more strategic progress because of our transition to collaboration, but I believe we are starting to see the limits of how far interagency elements temporarily doing things together can take us.

"My personal view is that the next necessary phase, which will admittedly be harder than both coordination and collaboration, is integration. This will require us to more permanently bring previously disparate elements and efforts of the interagency community together into enduring structures and strategic missions, where more government elements spend large portions of their careers working outside of their originating organization or agency. This will be both difficult and uncomfortable for many of us, but I believe that a world in which our future adversaries and challenges will defy both our geographic models and our department-by-department practices on a global (as opposed to country or even regional) scale demands this of us."

—Lieutenant General Michael K. Nagata, USA
Director for Strategic Operational Planning
National Counter Terrorism Center

involved in countering threat networks.[3] The director of the Joint Staff tasked OIW to examine joint force CTN operations and activities, with the goal of strengthening transregional collaboration and integration with U.S. Government and other mission partners.[4] The study included a literature review and an extensive series of site visits and stakeholder engagements with representatives from the combatant commands and other governmental organizations.

The study identified five areas in which the joint force is not optimized to empower our components, institutions, and partners to work in concert in a deliberate, integrated approach to address the global array of threat networks. In short, while there are eddies of CTN excellence within the joint force, our collective efforts to confront threat networks remain mostly aspirational and our commitment to be a good partner in this endeavor is imperfect at best.

First, we are not adequately integrating CTN into strategy and plan development. A common misstep by joint planners is to lump CTN and its associated activities into some sort of catch-all subset of counterterrorism. As demonstrated in previous examples, CTN applies to all challenges within the current threat framework and conceivably any that might emerge. Given this common link that spans the challenges presented in the National Military Strategy, it is critical to infuse both the approach and the capabilities into our overarching strategy guidance and ensure effective translation and nesting in subordinate plans at all levels.[5] These plans (for example, global as well as combatant command campaign plans) should effectively address the ways our adversaries have successfully operationalized military and nonmilitary instruments of national power to achieve objectives. Once CTN is firmly rooted in plan and campaign development, regular assessment of how we are doing should follow.

Second, we are employing an ad hoc approach to CTN. The joint force, and the U.S. Government generally, does not organize CTN activities through a deliberate approach designed to maximize the benefits of combining joint force and partner capabilities. We tend to look at individual aspects and segments of threat networks through functional "soda straws." We orient and fixate on the commodity and do not pay sufficient attention to the enabling networks. This is akin to treating the symptom and ignoring the disease. Moreover, a holistic regimen for treating a disease should take advantage of all appropriate approaches, not only those remedies that relieve the symptom for a time. Threat networks are like complex, adaptive, and resilient organisms that evolve in order to survive. The approach to treat them must be robust enough to be formidable, yet agile enough to keep up with their changing modes and methods. This requires an organizational construct that coordinates policy and processes, prioritizes resources, and integrates with other departments, agencies, international partners, and even the private sector and academia.

Third, we should become comfortable in supporting roles. The joint force cannot defeat threat networks alone. In the same vein, we cannot effectively compete with our military competitors without addressing the threat networks they employ. Traditionally, we have a bias for immediate, decisive action on the objective. However, defeating threat networks often requires a modicum of patience and will not normally result in a military finish. Thus, we have to depend on our partners and allies to fill roles that we cannot. Interagency teaming is critical to countering and defeating threat networks.

The joint force must become comfortable with bringing resources to bear in support of an interagency partner because the optimal finish might be an arrest and prosecution—and the action arm might be a law enforcement agency. This requires enormous trust and confidence across organizational lines. It cannot be surged, but rather, it must be cultivated over time in an environment that compels something more than coordination and collaboration—true *integration*. Furthermore, planners cannot develop the full range of options available against

threat networks without meaningful partner involvement in all phases of planning. We need cross-cutting, specific policy guidance directing increased integration with partners across the range of activities, exercises, planning, and execution. Most important, we need authority, flexibility, and permission to support, rather than lead, in most CTN efforts.

Fourth, we do not educate, organize, train, and manage people to conduct CTN activities. Joint force leaders and planners often fail to link threat network activities directly to national security interests. Consequently, they fail to see how countering these networks can achieve military objectives. This may be because we have not educated our people about the importance of these adversaries or the capabilities resident in the joint force and its partners. Additionally, there is no meaningful demonstration or wargaming as to how these capabilities can be integrated into operational planning to achieve desired outcomes, such as a scenario where the finish is not a major military operation, but one that still achieves its military objectives.

We do not invest in the development of joint force personnel with specialized CTN skills as we do with more conventional or special operations specialties. In the few areas where we have invested in training (for example, counter-threat finance, counternarcotics, border security), we have not developed career tracks and incentivized our people to stay in them long enough to become experts. Furthermore, we do not prioritize or synchronize liaison officer (LNO) placement to or from our partners and allies. This means that the person representing DOD to our partners may not be properly qualified to deliver a message consistent with Secretary of Defense and Chairman of the Joint Chiefs of Staff guidance. Likewise, LNOs whom our partners embed with us may or may not be in the best position to effectively represent their organizations' capabilities or authorities within critical processes, such as campaign development or operational planning.

Air Force KC-10 Extender aircraft refuels F-22 Raptor aircraft over undisclosed location, September 26, 2014, before strike operations in Syria (DOD/Russ Scalf)

We need to improve joint doctrine, training, education, and leader development to institutionalize general and specialized CTN knowledge and better integrate CTN into professional military education. Likewise, we need to improve career management in these skill-sets. We also need to optimize our LNO exchanges through a coordinated process that ensures the messenger, and thus the message, are properly placed.

Fifth, we do not manage and share information well. This is not exclusively a joint force problem, but we can at least improve our own foxhole. The lack of common data management across combatant commands, between commands and Service components, and with

Sailor stands watch in combat information center on dock landing ship USS *Harpers Ferry* in South China Sea, August 4, 2016, supporting security in Indo-Asia-Pacific region (U.S. Navy/Zachary Eshleman)

partner organizations at best impedes efforts to synchronize plans, activities, and assessments. At worst, it is the critical point of failure in successfully illuminating and dismantling threat networks. Because these networks operate across functional and geographic boundaries, they stress the Intelligence Community's collection and analysis networks, challenging our capacity to triage and disseminate meaningful intelligence. Vital intelligence then dies on the vine of disjointed information structures and outdated data management and sharing policies.

This severely degrades the most elemental CTN function: illumination of the networks we need to target. Consequently, it prevents planners and leaders from seeing the entirety of a given threat, including its connections to enabling networks. We need an in-depth study of DOD information management policies, practices, and capabilities that looks across communities (intelligence, diplomatic, law enforcement, military, and so forth), anticipates technological advancement, and is concerned with enabling a globally connected joint force—and mindful of a globally connected and unconstrained threat.

How to Strengthen a Broader CTN Effort?

It is important to recognize that the joint force is not required or expected to do it all when it comes to CTN; it would be impractical to try. Interdependence with our partners should be part and parcel of our paradigm. However, we must be willing to bring to bear our strengths that serve to empower partners, even if it seems like the heaviest lift in the effort at times. This does not obligate us to take on a leading role every time, despite expectations to the contrary.

At the same time, however, we should leverage our ability to put a problem on the table and pull in relevant stakeholders to do more than just admire the problem together, but, rather, coalesce around it and form viable solutions. Joint force leaders should capitalize on this capacity and look for opportunities to gain consensus regarding various problem sets and elucidate their potential as serious national security threats.

The joint force has inherent strengths that include the capabilities to provide force protection; mobility; secure communications; intelligence, surveillance, and reconnaissance support; operational planning; and logistics. The joint force can apply these capabilities to contribute to the effectiveness of a friendly network by

- providing planning frameworks and support
- identifying, locating, understanding, illuminating, and targeting threat networks

- assisting mission partners in counter-threat finance
- building partner capacity
- denying safe haven
- conducting direct action, including capture operations and the use of lethal force against lawful targets
- assisting mission partners in countering threat mobility and cross-border movement, including detection and interdiction
- identifying and understanding the capabilities, interests, will, and intent of friendly networks
- conducting information operations that attack, disrupt, sabotage, subvert, and deceive adversary capabilities
- conducting offensive and defensive cyber operations
- supporting and complementing U.S. strategic messaging and communication activities.[6]

Conclusion

Our adversaries purposefully use threat networks in diverse and innovative ways to unbalance military efforts and hold at risk our partnerships, objectives, and even our national interests. But where there is risk, there is often opportunity. The joint force can take advantage of the complex and chaotic operating environment by pushing hard for increased integration of efforts across the U.S. Government and with international partners. This enhanced state of interorganizational integration will pay dividends in the long term, particularly against state adversaries who can force their own whole-of-nation unity of effort. Operation *Gallant Phoenix* demonstrates how we can capitalize on an opportunity to bring diverse functional and organizational capabilities to bear on a problem, and then apply this model across numerous threat networks, irrespective of the commodity the network moves. The expansion and convergence of global threat networks demand that we adapt, and the joint force is in the best position to lead that effort to shift the collective paradigm. We can bring great operational capacity and a coalescing propensity to the table, laying the foundation for a formidable network of cross-functional partnerships. Some organizational introspection is certainly required before we can truly embrace a more integrated model. To prevail against our adversaries in this ubiquitous struggle, however, we need to be open about our limitations, address our shortcomings, and become comfortable with and proficient in our role as the best enabler we can be, propelling our partners to score the big wins. **JFQ**

CTN in Action

Operation *Gallant Phoenix* is a task force comprised of law enforcement, military, and intelligence professionals from the United States and over 20 partner nations. International and interagency mission partners are collocated in a fusion center where they benefit from the diversity of functional experts, a collective of legal authorities, and an environment conducive to real-time information-sharing. Stakeholders all share a common purpose and build enduring relationships based on trust. The operation leverages unique partner capabilities, authorities, and access in order to develop intelligence into usable information or unclassified legal process that enables partners to finish a target through the application of appropriate mechanisms. While the joint force leads and facilitates this model, the interagency and international partners are included at every opportunity to develop the greatest and broadest impacts against adversaries.

Notes

[1] Joint Publication 3-25, *Countering Threat Networks* (Washington, DC: The Joint Staff, December 21, 2016), 1-1.

[2] David A. Broyles and Brody Blankenship, *The Role of Special Operations Forces in Global Competition* (Arlington, VA: Center for Naval Analyses, April 2017).

[3] *Countering Threat Networks Study, Phase I Report* (Washington, DC: The Joint Staff, November 17, 2017, draft report ver. 7).

[4] The Office of Irregular Warfare team visited over 40 commands and organizations. Engagements with larger organizations generally included multiple discussions with subordinate staff elements to gain both executive and mid-level perspectives. The following lists many of the key engagements: U.S. Africa Command, U.S. Central Command, U.S. European Command, U.S. Northern Command, U.S. Pacific Command, U.S. Southern Command, U.S. Special Operations Command, Special Operations Command–Africa, Special Operations Command–Central, Special Operations Command–Europe, Special Operations Command–North, Special Operations Command–Pacific, Special Operations Command–South, Central Intelligence Agency, Defense Intelligence Agency, Drug Enforcement Administration, Drug Enforcement Administration–Special Operations Division, Joint Special Operations Command, National Counter Terrorism Center, National Guard Bureau, Joint Task Force (JTF) Ares (U.S. Cyber Command), JTF-North, JTF-West (Department of Homeland Security), Joint Interagency Task Force (JIATF)–National Capital Region, JIATF-South, JIATF-West, Joint Improvised-Threat Defeat Organization, Joint Information Operations Warfare Center, Joint Intelligence Operations Center (U.S. Pacific Command), Joint Intelligence Operations Center–Europe, Global Engagement Center (Department of State), Narcotics and Transnational Crimes Support Center (Department of Defense), National Joint Terrorism Task Force (Federal Bureau of Investigation), National Targeting Center (Customs and Border Protection), Organized Crime and Drug Task Force (Department of Justice), Army Terrorism and Crime Investigative Unit, Center for Advanced Defense Studies, Counter-ISIL Finance Cell, El Paso Intelligence Center, National Intelligence University, Operation *Gallant Phoenix*, U.S. Council on Transnational Organized Crime.

[5] The Chairman of the Joint Chiefs of Staff's Five Priority Challenges: 4+1 refers to China, Russia, Iran, North Korea, and violent extremist organizations.

[6] *Countering Threat Networks Campaigning*, White Paper (Washington, DC: The Joint Staff, December 8, 2016).