17

Networks at War: Organizational Innovation and Adaptation in the 21st Century

Christopher Fussell and D.W. Lee

The Evolving Landscape of Warfare

Recent observations of warfare clearly suggest that conflicts have become more transnational, longer, irregular, and network-centric.[1] Put differently, recent conflicts can be best described as protracted internal conflicts with multiple intervening state actors, networked with nonstate actors in a manner much like the multidimensional hybrid operational environment discussed in Army Special Operations (ARSOF) 2022.[2] The current conflicts in Iraq and Syria certainly meet this characterization; as do emerging crises in Ukraine, Yemen, and Libya, and longer-standing conflicts in Afghanistan, Somalia, and the Democratic Republic of the Congo. More state and nonstate actors support or sponsor movements in an intrastate conflict, making the termination of fighting very hard. For instance, the rapid resurgence of the Islamic State of Iraq and the Levant (ISIL) is largely attributed to the protracted Syrian civil war in which regional powers (including Iran, Saudi Arabia, and Turkey) as well as external nonstate actors such as ISIL, al-Nusra, and Hezbollah, to name just a few, sponsored local movements.

In essence, the complexity of warfare has increased due to the growing prevalence of networks utilized by states and nonstate actors who have found ways to countervail the kinetic superiority and hierarchical efficiency of big nation-states. This evolution demands a response from the United States and our allies, and requires a restructuring of our security apparatuses and a reframing of our definitions of preparedness and success.

Despite the changes that these threats demand, the changing nature of warfare is not a novel observation; the concept of "netwar" was coined by John Arquilla and David Ronfeldt in 1996.[3] Arquilla and Ronfeldt define "netwar" as "an emerging mode of conflict (and crimes) at societal levels, short of traditional military warfare, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age."[4] In their seminal paper, "The Advent of Netwar," the authors outline the defining characteristics of the netwar actor: it is necessarily "networked," containing nodes, clusters of nodes (i.e., cells), in a flat decentralized organizational structure. On offense, it is "adaptable, flexible, and versatile vis-à-vis opponents and challenges that arise."[5] Their now frequently coined phrase, "it takes networks to fight networks," was a clear foreshadowing of the transformation that state actors will need to go through if they hope to succeed in today's environment.[6]

This chapter explores the ways and means the United States can use to fight in this complex environment by harnessing the strategic utility of networks. Empirically, this objective is predicated upon the observation that an increasing number of external state actors overtly or covertly intervene in intrastate conflicts by exploiting various nonstate groups and networks in order to increase their respective strategic influence.[7] Similarly, nonstate actors also take advantage of interstate conflicts or political instability in their own countries and in neighboring regions.

Clearly, conflicts such as the Syrian civil war represent a sample of a larger shift in warfare toward more complex and hybridized dynamics. As of this writing, Uppsala University's world Conflict Data Program compiles data on 40 conflicts in the world for 2014. All but one of them are intrastate conflicts and 13 of them are internationalized.[8] The complexity of the current security environment is driven by an increasing number of state actors and nonstate actors who are networked to leverage and exploit the insurgent potential of multiple groups engaged in civil conflicts. Arguably ISIL, the most formidable terrorist movement of the 21st century, rose from this type of state and nonstate dynamics.[9] Defeating ISIL will require untangling the web of complex ties and competing interests between states and nonstate actors. This section explores ways and means of harnessing this complexity and suggests how such methods can be applied to help the United States fight more effectively against hybridized threats.

In order to fight in this complex hybrid environment, we argue that a deep understanding of network dynamics is critical.[10] Without understanding such dynamics, it becomes next to impossible to identify partnerships among disparate groups forming an alliance and coalition against American strategic interests. We also argue that fighting in the complex networked environment entails two interrelated innovative processes: 1) transforming our own organizations and communications to become more networked; and 2) mapping and illuminating the connective dynamics of adversarial networks.

Following the logic of netwar, we use two tales in this chapter to illustrate the sort of organizational revamping necessary to respond to modern conflicts. First we offer a narrative about the transformation of a highly specialized task force (TF) and how that organization had to force itself to adapt in the complex networked environment to safeguard the security of our nation. This is a story about fighting *ourselves* in order to become more agile and adaptive. The second story is about how we can fight more effectively against networked adversaries and strategic competitors. We argue that, within the context of organizational innovation, one effort is incomplete without the other.

Fighting Ourselves: Special Operations Task Force Transformation

The concept of organization-level change is easy in the abstract, but in most groups, real change remains strictly theoretical. Without a genuine imperative, human nature will drive each of us to resist fundamental, systems-level changes. There is a threshold of change beyond which the system can no longer revert to the known, and organizations (and the individual decisionmakers that comprise the organization) are generally incentivized

to avoid crossing this line. When they are forced to do so, they often return as quickly as possible to the previous state of perceived stability. The military is as guilty of this pattern as any large bureaucracy. As with any industry, this can be both a strength and a vulnerability.

The U.S. Army's Airborne School has gone without systematic changes for generations of paratroopers. While parachute, aircraft, and individual equipment technology continues to improve, the step-by-step approach to preparing an individual soldier for his or her first parachute jump looks largely the same in 2015 as it would have in 1970. It is, ultimately, a linear process that has reached a very high level of efficiency and effectiveness, managing appropriate throughput while controlling for expected levels of capability and safety. The so-called "Jump School" is an excellent, and highly optimized, system.

The challenge in a bureaucratic system as big as the U.S. military (or any other hierarchical, global enterprise), however, is to encourage a differentiation between problems that can be solved through linear optimization of the current organizational model, and those problems that necessitate a rewiring of the fundamental way in which the organization functions. If the Department of Defense suddenly identified the need for twice as many paratroopers, the solution would be complicated. Along with high resource costs, the solutions would map to a series of second- and third-order impacts. It would demand the focus and intellectual power of experienced leaders and planners who understand the multitude of implications of the transition. The execution of the plan would require excellent cross-functional leadership and project management skills, ideally from leaders with deep knowledge of the training environment and existing relationships that would allow them to move as a team. But ultimately, the answer to "how can we create twice as many paratroopers?" can be known, within a few degrees of accuracy, from the outset of the execution of the plan, assuming it was properly produced. Indeed, this is one of the core strengths of the U.S. military dating, arguably, to lessons of military industrialization that were learned and ingrained over generations of industrial-age warfare. These lessons have driven advances in training, programs, and growth for decades inside the ordered industrial-age military environment.

But, as the Special Operations community learned in the early years following the attacks of September 11, the same organizational muscle that drives effective organizations toward optimization and efficiency gains can lead to organizational uncertainty and inertia around the development and implementation of viable solutions when subjected to a new military environment. The reality that the Special Operations TF encountered was that the arrival of the information age led to a level of interconnectedness between individuals around the globe that traditional systems were simply not designed to cope with. In practice, this meant that networks of al-Qaeda leaders, fighters, influencers, and financiers could connect globally and in real time, maintaining strategic context and broad alignment with the goals of al-Qaeda while constantly adapting to the demands of local conditions. The TF was facing an organic network, able to create leaderless action, and thereby quickly negate the effectiveness of predictive analysis that the American military

had relied upon for decades. Al-Qaeda's actions did not come from a strategic plan, but emerged bottom-up from the real-time thinking and planning of its numerous, highly autonomous, individual nodes. While some of the TF's tactical-level leaders could sense that conditions were changing on the ground, traditional military approaches incentivized members to attempt to frame the disorder of wholly unpredictable problems into a linear solution set; this breeds, inevitably, ill-fitting solutions to misunderstood problems. If the only thing you have is traditional enterprise thinking, you become the infamous hammer in search of a nail and your actions run the risk of creating as many problems as they solve.

None were guiltier of this than the Special Operations community in the early days of the fight with al-Qaeda in Iraq (AQI). In late 2003, it was clear that the momentum of AQI was outpacing our efforts in Iraq; by the end of the year, there had been more terrorist attacks in Iraq alone than there had been in the entire world in 2003.[11] And it only got worse. By the end of 2005, terrorism claimed 8,300 Iraqi lives; by early 2006, more than a thousand Iraqis died each month.[12] What was unclear was why this was happening. On paper, and through the accepted view of the world in 2004, this made no sense. The forces that comprised the Special Operations TF had clear and undeniable points of superiority, which included:

- capability level and training of the individual operator;
- cohesion and tactical effectiveness of small team units;
- advanced weapon systems at every level (individual operator to overhead strike assets);
- full spectrum intelligence collection and dissemination capabilities;
- ability to dominate night operations; and
- highly refined, global-reaching logistics and supply chain operations.

This list could go on. In short, the TF could move exponentially more capable forces around the globe, with superior equipment, at unparalleled levels of speed and efficiency, and place them in tactical scenarios where they held nearly every advantage. These points of superiority led to the measurable fact that, when elements of the TF were able to lock members of AQI in time and place, and then close in on them with a tactical ground force, these special operations teams demonstrated a near-perfect record of winning the engagement. However, victory in the moment in each tactical engagement was not the issue.

Despite all of these advantages, it was clear by 2004 that AQI was somehow outpacing some of the world's most highly trained and well-funded units. We were winning tactical engagements, but losing the overall war. The entire U.S. military system had, in retrospect, failed to properly weight the new variable of global interconnectivity. There was a time when state-run organizations controlled information flow, as there was a significant barrier of entry to pass information on a global scale. The TF knew conceptually, early in the fight, that modern technology was creating globally connected networks, but it did not realize that this new reality had nearly instantaneously changed the face of the battlefield.

Traditional bureaucratic systems designed around the control of information flows were not designed to handle this new reality. As in most hierarchies, the TF was grounded in the fundamental belief that information is power and that the ability to gather information from multiple silos and synthesize it into knowledge and insight that others could not produce is the source of ultimate power and respect. But playing an industrial-age game while the external system is operating by the rules of the information age adds incredible risk and is destined for failure.

By 2004, it had become clear to the senior leadership of the Special Operations community that the existing bureaucratic model was not going to allow the TF to move fast enough to keep pace with al-Qaeda. That same senior leadership also made it clear that the solution would involve a fundamental shift in how the TF operated as an organization.

In the early days of the fight with AQI, the problem was not that the TF needed exponentially more operators, helicopters, or weapon systems. The TF did not need new agencies to be invented to solve the problem, and it certainly did not need more individual data points (raw intelligence) to be collected from the field; if anything, the information-age battlefield was already overwhelming the system with data that could not be sorted and acted upon fast enough. Simply put, there was no linear solution, organization chart redesign, or any single silo within the enterprise that would somehow solve the problem. The U.S. military, quite understandably, was locked in a collective cognitive bias (more specifically, a classic status quo bias) that forced many of the TF to take complex information from the battlefield and create ways to explain it through preestablished ways of thinking that made sense according to the old norms of the organization. For example, if a detained member of al-Qaeda offered information about the person he reported to, it was difficult for the TF to understand that the person being referenced was part of a fluid network, not part of a crisp hierarchical organization chart. By the time the intelligence had become actionable, the person being described may have already moved multiple times, both in position and influence, within the self-rearranging network. But the organization's status quo bias drove the TF, at a systems level, to fixate on targeting the next person up the perceived hierarchy. Hours of planning and energy would go toward locating the reported "boss," only to find, after targeting that individual, that the new target was no more or less important that the person initially captured. And the cycle would repeat. This led, of course, to days, weeks, and months of head-scratching and to post-it note hierarchies covering the walls of outstations throughout Iraq, fruitlessly attempting to tell a story about al-Qaeda's structure that simply was not there. The TF could no more create an organization chart that defined the totality of al-Qaeda than one could create a similar document for all Facebook users.

The bias toward seeking a linear solution is obvious and reasonable, and it would have been ideal for the design of the enterprise. Much like the problem of creating twice the number of Jump School graduates, if we could have solved the math problem and declared with certainty—there are x number of al-Qaeda fighters, and we need to produce y amount of actions to defeat them—then a complicated solution would have started with: assets + personnel = y (actions). And like the Jump School plan, the TF would have increased the

first two variables until its output was moving faster than the growth of AQI. It would have been costly and difficult, but knowable and measurable. And this, predictably, is what the TF tried to achieve in the early part of the conflict. But by late 2004, there were no other assets or personnel to add to the mix, and stretched to the limit, the TF's actions could move no faster.

In retrospect, the ultimate problem was a not uncommon organizational bias against recognizing a massive shift in the external environment. The TF had been created in a complicated, but, ultimately, ordered environment where nation-states and enterprise-level systems controlled the flow of information and action. Individual actors in any space (on the battlefield, in business, etc.) could certainly exercise their free will and step outside the norms, but the risks were incredibly high and the likelihood of strategic impact very low. A soldier in World War II could sneak through enemy lines with relative ease and engage a less defended position, but the odds of returning to safe territory were low, as were the chances of engaging an enemy soldier of any strategic importance. The rational player who wanted to have significant impact, therefore, was incentivized to understand and master the rules of the system. The general officers on the battlefield, CEOs of the corporate world, or the dignitaries in nation-state interactions were the positions that consistently provided the opportunity for strategic impact. But the TF had, as a direct result of the reduced barrier of entry for global communications and the subsequent interconnectivity of billions, entered an environment dominated by disorder and complexity. No longer could the scale advantage of large systems control the entire environment. Suddenly, the individual who had not mastered the system or reached any traditional position of power or influence was able to become a strategic player based simply on their ability to connect, influence, and create action within a networked organization.

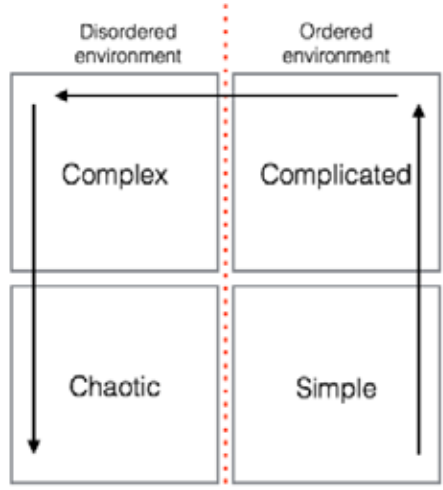
But these types of players exist outside of the ordered systems that *other* ordered systems are biased toward looking for. In the absence of seeing an ordered system in the fight against al-Qaeda, the TF worked diligently to create structure where it did not exist. This, of course, proved impossible and ultimately drove the TF to shift to an entirely new operating framework. The TF, and the large U.S. military, had moved into a world of disorder, where environmental conditions can no longer be dominated or controlled by large systems. On the battlefield, the coupling of the interconnectedness of individual nodes in the al-Qaeda network with the speed at which the global information system allows for the flow of information and ideas led to the creation of a complex system; that is, a system whose output can no longer be effectively predicted based on input variables. The output of a complex system emerges as more than a simple sum of input variables, a reality that fundamentally undermines the predictive nature of traditional military systems.

In this complicated battlefield scenario, those closest to the problem (e.g., the "front line" of the fight) were looking for a relatively small number of large data points, such as the number of enemy fighters, types of weapon systems, and estimates on supply chain capability. These large chunks of data could be effectively synthesized at the top of the hierarchy, predictive analysis done on possible and likely enemy courses of action, and

orders disseminated back to the frontline elements. These orders, for operational security reasons, could be kept relatively compartmentalized, as synchronization and de-confliction between the various frontline elements could be centrally controlled. This worked, in large part, because both sides were following the same basic set of rules even if their end states were radically different. Therefore, the side that was able to optimize their system most effectively was likely to come out victorious. This was true in the kinetic environment of World War II, and in the nonkinetic, proxy environment of the U.S.-Soviet Cold War. But when the opposition has no allegiance to a traditional system, leveraging old systems in hopes of creating a predictive analysis capability is fruitless. When the frontline elements are looking not at a few large pieces of intelligence, but instead at thousands of highly nuanced pieces of data ranging from individual relationships to shifts in tribal allegiances to community members that may float in a single day between family interactions, legitimate business work, U.S. military partnerships, and al-Qaeda relationships, synthesizing data at the top of the hierarchy and distributing useful guidance is an impossible task. When the TF tried this approach, its individual actions were accurate and successful, but their sum total was exponentially slower than was necessary.

Looking at this environment through an adapted version of the Cynefin model, first designed by David Snowden and Mary Boone, the battlefield environment had progressed from the complicated and ordered environment to the complex and disordered space (with occasional upshots into chaos):[13]

Figure 17.1. Adapted Version of the Cynefin Model



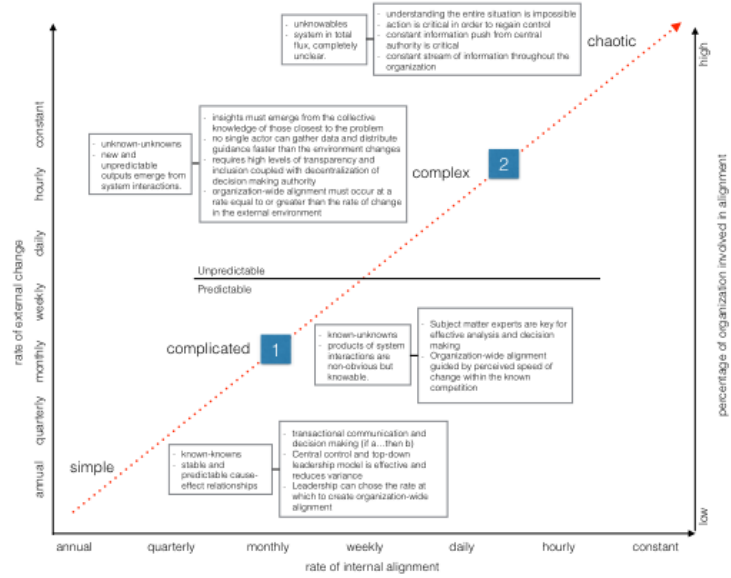
The initial reaction of the TF was to push and strain systems designed for a complicated world as far as it possibly could, but to no avail. The organization pushed assets harder than ever. Operators reviewed plans and intelligence and briefed the chain of command; elite

small teams went to work in the dark hours of night, hitting multiple targets, meticulously planning and executing each operation, sleeping for only a few hours after returning to base each morning. This process that drove the TF became known as "F3EA:" Find—Fix—Finish—Exploit—Analyze.[14]

But it was not enough. Component parts were being optimized, but the overall system was misaligned to the speed of information flow on the battlefield. In the disordered and complex environment, the TF's approach to communication, intelligence sharing, decentralization of decisionmaking rights, and ability to take autonomous action was mismatched relative to the speed and complexity of the enemy network. For its system to be effective, the TF needed to understand the pace of the problem it was facing, then index that against the speed with which it was able to move information and create action. Through that optic, it was clear that the system needed to change at a very fundamental level in order for a large, global enterprise to outpace the agile al-Qaeda network.

This level of change was an easy thing to conceptualize, but difficult to execute, as the TF realized that it was not designing a temporary measure to account for a sudden change in the enemy's approach; rather, that it had stumbled upon a fundamental shift in the operating environment, so its change needed to be permanent, not a patch. An early realization was that its pace of communication would need to increase exponentially if it hoped to match the speed of a complex environment. The graph below, an adaptation and extension of the Cynefin model, shows an *x*-axis representing increasing time separation between moments of organization-wide strategic alignment, a *y*1-axis showing an increasing rate of change in the external environment, and a *y*2-axis showing the percentage of the organization that must be pulled into broad communication forums in order to match the speed of the external environment.

Figure 17.2. Adaptation and Extension of the Cynefin Model



This graph maps the entire construct, but the majority of the problems in the counterterrorism fight against AQI sat at the transition point between "complicated" and "complex." The new reality that the arrival of the information age brought with it, for the foreseeable future, is an external environment in a regular state of disorder. Speed and interconnectivity of millions of individual nodes have created a constant state of complexity. The crossing of that horizontal divide from order to disorder is what the TF had to accept as the new reality of the world we all now live in. The implication was that the organizational norms and leadership behaviors of the optimization- and efficiency-based models that dominate an ordered environment were no longer relevant.

The requirement was to move the organization from point 1 to point 2, as shown in the graph provided, shifting from a structure capable of dealing with complicated and predictable problems to one comfortable handling a complex and unpredictable environment at the enterprise level. Long a trait of small Special Operations teams, the ability to adapt in near real time to an ever-shifting landscape had never been seen as a requirement at the global-system level, where scale and efficiency have always seemed to matter most. Consider any place along the red line in the graph shown, the point at which a sufficient amount of the enterprise is aligned on strategy to allow those closest to the problem set to take independent action without creating strategic-level errors. The Special Operations TF's optimization/efficiency model did this well, but far too slowly. The TF was stuck in the ordered/complicated space, while AQI was operating in the disordered/complex world that was the actual battlefield.

To move from point 1 to point 2 above, the TF needed to execute two major change functions. First, it needed to acknowledge that it was now in a fundamentally unpredictable environment, which meant building a network of all stakeholders involved in the fight. Without a physical center of gravity in Iraq, it was necessary to interconnect parts of the organization that would have preferred to remain siloed from one another, even within the Special Operations community itself (i.e., cultural and operational divisions between Navy SEALs, Army Rangers, and other specialized units). In a complicated environment, each of these components would own a piece of the battlefield and the section of the problem that was contained therein; but in the complex environment, the al-Qaeda problem flowed quickly and rapidly between these self-constructed boundaries. Therefore, the TF needed its operational elements to be interconnected at an unprecedented level. But al-Qaeda was a global network that was in a constant state of change, so it was necessary to expand the network model well beyond the military units involved in the ground war. An al-Qaeda network involved in recruiting, radicalizing, and moving foreign fighters into Iraq demanded of the Department of Defense a real-time relationship with the Department of State, as the problem would extend through multiple countries before reaching the declared theater of war. Understanding the interconnection between intelligence source networks and the al-Qaeda fighters being targeted by tactical units would require seamless connectivity with the various intelligence agencies involved in the fight. The list of key relationships would grow over time, and ultimately, it became a true interagency effort on

a global scale (arguably the only time the United States has successfully established and maintained such a model for an extended period).

Second, the TF needed to significantly increase its speed of communication, minimizing the amount of time needed to cultivate organization-wide alignment. Al-Qaeda was not adjusting its plans based on any master plan; rather, it was a complex system whose actions emerged bottom-up from the input variables in the environment. Those input variables were immeasurable, from local conditions on the ground to tribal politics, number of new recruits to disputes within the network, and from the raids the TF was conducting against them on a regular basis to the success or failure of their own operations. The AQI system changed daily, not based on any centralized strategy, but by the very nature of it being an organic network. Therefore, the TF needed to match the agility of the enemy if it hoped to eventually overtake the speed of AQI. As the TF's own network grew, it simultaneously increased the speed at which it ensured organization-wide alignment. This was accomplished by steadily increasing the number of participants included in, and the precision with which it was executed, a daily global video teleconference meeting titled, "Operations and Intelligence Update" (O&I).

During the peak periods of violence in Iraq between 2006 and 2007, daily attendance on this video teleconference numbered in the thousands; attendees were scattered around the globe, and every interagency organization critical to the fight was represented. Because of the tempo of this forum (roughly an hour and a half everyday), it was critical to have large numbers in attendance. If the forum had been attended only by the top level of leadership, the conversation would have been limited to mostly strategic discussion, and the organization would have spent many of the remaining hours of the day simply cascading information down through a series of small, siloed meetings with inconsistent context being distributed at varying levels of effectiveness (normal bureaucratic behavior that resembles a giant game of telephone). But by the time important strategic information hit the tactical level of the organization, many layers of filters would have interpreted it and passed down their view on what was and was not relevant, and the time remaining in a 24-hour operational cycle would be severely constrained. The system simply could not have moved as fast as the al-Qaeda network under that constraint. The ultimate decision was simple in theory, challenging in practice. Everyone needed to hear the same truth, simultaneously, at a rate that moved as fast as, or faster than, changes within the al-Qaeda network. In retrospect, we refer to this change as the creation of "shared consciousness" within the organization.

Creating shared consciousness was a critical step in establishing enterprise-level alignment across the TF with consistency and speed. By pulling together large numbers of individuals representing all of the critical geographic locations, intelligence organizations, leadership teams, and tactical arms of the organization, the TF was able to create broad awareness around critical changes ranging from the strategic to the tactical.

Two aspects in particular were essential to this transformation. First, instead of the traditional well-rehearsed brief by a junior member followed by black-and-white questions

(e.g., "How many *x*?"), our dialogue became broader and more participatory in order to glean the context (e.g., "Why are you thinking *x*?"). Second, until the revamping of the O&I meeting, the work done by operators and intelligence analysts was inextricably linked, yet siloed—the two groups had on organizational blinders in the name of efficiency and compartmentalization of information, which hampered attempts to build relationships and effectively cooperate in real time. The O&I meeting tore down these barriers, fused operations and intelligence—O and I—for the first time, and connected the purpose of both groups' efforts.[15]

With shared consciousness (driven by the O&I) in place, the organization developed a consistent level of what we will now refer to as "empowered execution." That is, the expectation was established that operational- and tactical-level elements would move with high levels of speed and autonomy during the periods between organization-wide synchronization (O&I sessions). In real terms, this meant that the elite small teams within the global enterprise were now interconnected as part of a network, given access to a daily forum to gain near complete levels of strategic alignment, then empowered, expected, and held accountable for their ability to move quickly and autonomously for the remaining 22 hours of the operating cycle. It was the informed autonomy that high performance organizations and aggressive leaders naturally desire, but rarely put in place.

As the Greek philosopher Heraclitus tells us, you cannot step in the same river twice. That became an apt way to describe the operations cycle once the enterprise was locked in shared consciousness and driven by empowered execution. What happened inside the remaining 22 hours of the operating cycle was never the same thing twice, as the organization had become more than the sum of its parts. As an interconnected network with decentralized authorities to create and adjust relationships, shift assets between units, share new intelligence in real time, and drive autonomous action, a global force of thousands was suddenly moving faster in its analysis-decisionmaking-action cycle than the small pockets of fighters in the al-Qaeda network. Goliath had maintained his strength, but was now more agile than David, and the scales began to shift.

Fighting the Enemy: The Human Domain Approach

Adapting in the complex environment of multiple interacting components is a daunting challenge for nation-states. The previous tale demonstrates how challenging it can be to defeat highly networked and adaptive adversaries. This section demonstrates that fighting in this highly dynamic and potentially chaotic environment requires a deep understanding of both the context and the structure of node, ties, and boundaries.[16] Following this logic, this section explores how to understand complex networks without losing sight of their inherent dynamics.

Illuminating the complexity of networked adversaries begins with a broad collection of information about the conditions that underpin the networks, key influencers that keep the networks connected, and affiliated social and political organizations. Insurgent or terrorist movements do not emerge just because of economic grievances or governance

vacuums. Rather, they emerge by manipulating existing conditions of grievance and ties between and across cohesive networks.[17]

Following this observation, there is a growing consensus on the necessity of mapping complex social dynamics to understand the social foundations of insurgent movements as early as possible. For instance, the new Army Operating Concept emphasizes the need to understand the human dynamics prior to the outbreak of violence.[18] It acknowledges that such an understanding is a must, in order to be able to shape and manipulate the operational environment during the conflict.[19] In other words, harnessing the complexity of the modern security environment can begin with understanding the relational dynamics of comprising entities.

United States Special Operations Command (USSOCOM) recently published a concept paper that emphasizes cultivating soldiers "with the knowledge, skills, and abilities to understand and influence human actions and activities."[20] In addition, the same concept stresses the need to link these activities to creating desired effects in the human domain.[21] In other words, understanding how to operate in the human domain will be a critical part of future fighting. Much like one would not think about going to war without detailed physical maps of the terrain and topology of the operational environment, human domain mapping can provide the initial social, cultural, and political dynamic understanding that can help the United States fight networked and complex adversaries. What remains largely unexplored is the type of methodology needed to fight effectively in this complex human environment.

A good analogy to describe the utility of these processes would be countering vehicle-borne improvised explosive devices (VBIED). In order to counter and prevent attacks from VBIEDs, intelligence work typically focuses on the overall terrain, roads, and key junctions. Instead of solely tracking only potential vehicles that may carry explosives, it makes sense to factor in the local road system with possible entry and exit points from known areas under insurgent control. In addition, one can also overlay known IED-manufacturing sites and insurgent activities onto the overall topography of the environment. By integrating the road system, known insurgent sites, and potential support elements, one can achieve a better understanding of how to deploy the Intelligence, Surveillance, and Reconnaissance (ISR) element more surgically, thus, improving the probability of early detection and interdiction. In fact, most counter-IED strategies do factor in environmental and topological variables.[22]

Operating in the complex human environment can be conceptualized in a similar vein. In other words, it entails collecting and analyzing information pertaining to three broad categories: mapping key conditions of insurgency development, pathways of interaction, and nodes of influence.[23] These are well-supported in the literature of social movement theory and social network analysis (SNA). For instance, Doug McAdam shows that robust insurgencies emerge from existing ties. ISIL's organizational growth shows similar patterns where preexisting ties of old Baathists and Republican Guards comprised the infrastructure of the movement to expand in Syria. In essence, AQI's weakened leadership developed ties with other inmates at Camp Bucca, which later became the overall leadership structure of

ISIL.[24] Expanding in Syria, ISIL exploited the local conditions of lawlessness and divided opposition groups by first identifying key influencers of major fighting groups and then either co-opting existing social structures or replacing them. By establishing *Dawahs*, or charity groups, first, ISIL embedded itself within existing social networks before it began to exert its social and political control. From this brief description, it becomes clear how conditions, pathways of interaction, and influential nodes are critical categories of information in fighting in the human domain.

The Conditions: Context of Network Development

The first step of mapping the human domain begins with the identification of conditions that are highly associated with the emergence and development of radical collective action.[25] As David Kilcullen points out, powerful insurgent movements emerge from a coalition of disparate groups when certain conditions compel them to work together.[26] In order to anticipate and counter emerging insurgent movements, it is critical that intelligence preparation of the battlefield begin by analyzing what conditions exist in the operational environment.

Social movement theory suggests four major types of antecedent conditions: political, economic, social, and ideological. Political conditions can be factions within the regime or the existence of political opposition groups. Going back to the expansion of the ISIL, Nouri al-Malaki's systematic persecution of the Iraqi Sunni population created a very permissive political environment that allowed the remnants of AQI to mobilize a great many Sunni groups in Iraq.

Certain economic conditions are highly associated with the onset of radical movements. Typically, these conditions include income inequalities, underemployment, unemployment, inflation, or income stagnation. Note that it is often external shocks that trigger the exacerbation of these conditions.[27]

Ungoverned or underregulated economics can also provide a fertile ground for insurgent groups to generate resources to sustain themselves. These unsanctioned economic areas typically have built-in informal or autonomous channels of resource extraction and redistribution. The autonomy of the bazaar in Iran was a major factor of success during the Iranian Revolution of 1979.[28] The bazaar provided much needed resources to key organizers of the movement when the regime had cut subsidies and stipends to students and academics.[29]

It must be stressed that economic conditions themselves are rarely sufficient for resistance to emerge or take hold. For instance, while the overall economic conditions of the Middle Eastern states were generally comparable in the 1980s and 1990s, insurgent movements emerged in only a select few countries.[30] While all major macroeconomic indicators were comparable in Algeria, Egypt, Jordan, Morocco, and Tunisia between 1980 and 1992, only the first two countries experienced major insurgent movements. This observation is not uncommon in the literature.[31] Assessing individual grievances is an important part of understanding how radical elements become networked to form a

broader movement. What is critical to understand is the process through which individual grievances are transformed into a group narrative. In other words, grievances become instrumental when they are exploited and framed by groups or networks actively seeking to create opportunities for collective mobilization.

Social divides and existing dissident networks provide great potential for resistance. In particular, external actors can leverage these social conditions to establish a robust organizational platform. It is no coincidence that most robust resistance movements emerge from preexisting ties and networks. These preexisting ties typically have built-in mechanisms to coordinate information and action across civil society. Ethnic divides can be a powerful location from which collective action emerges. The cohesiveness of existing socio-ethnic divides can also generate resources to create a broad coalition of insurgent movements as opposed to just focusing on one cohesive group.

Ideological conditions are based on existing grievances stemming from economic disparities or structural strains such as income inequalities, unemployment, underemployment, or discrimination. In essence, these conditions often stem from social, economic, or political strains. They also include existing norms of collective action and violence that can be utilized to justify mobilizing large groups for resistance. For instance, a sense of victimization is often used by Islamists to justify jihad.[32] Typically, insurgents will try to align their ideology with socially accepted themes of expressing dissent.[33] Instead of treating resistance ideology as a monolithic worldview, it is more useful to approach it as a set of grievances specifically framed to motivate and justify collective action.[34]

The Pathways

Once the context of a network is analyzed, then we can start mapping the internal components. The second process of illuminating the human domain begins by understanding how various groups are connected with other groups as well as external actors. Social movement theory suggests that existing ties and channels between social and political organizations play a critical role for the growth and expansion of insurgent movements.[35] In essence, existing relations function as the path of least resistance between groups and actors. As individuals try to disseminate new information and find others to join them in collective action, informal ties are instrumental to collecting and distributing resources and ideas. Figure 17.3 illustrates the importance of understanding existing ties to harness the complexity of networked entities.

Figure 17.3. Network Map of the Power Structures of Iraqi Kurdistan[36]

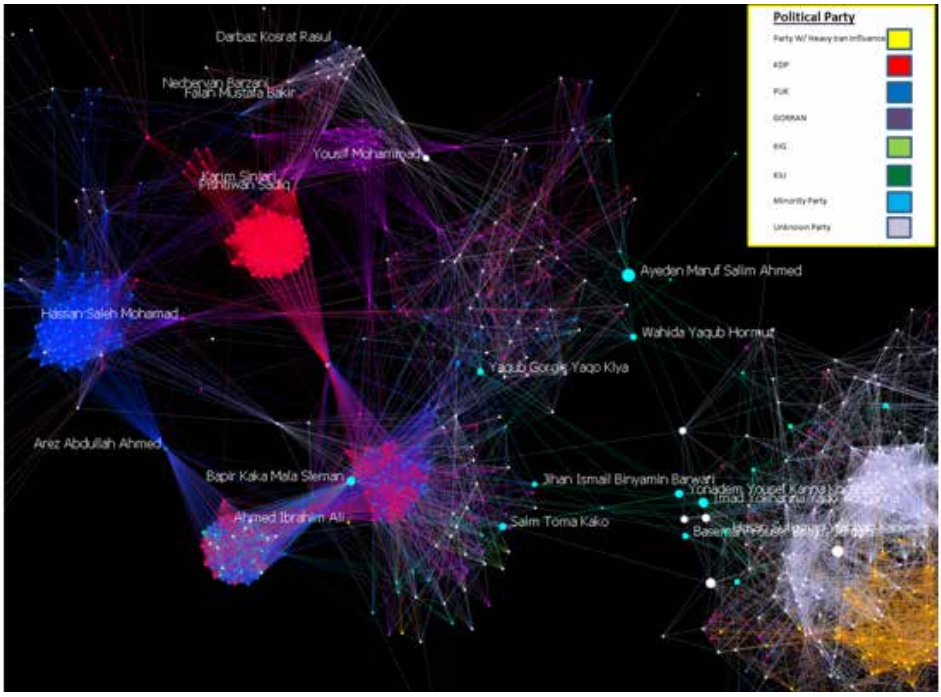


Figure 17.3 provides a graphic representation of observed individuals and relations among them. In SNA, this type of visualization is called a "sociogram."[37] In essence, the sociogram depicts a map of existing ties between several political factions in Iraqi Kurdistan. It captures four types of ties between the members of the Iraqi parliament and major Kurdish political movements: ties with nonpolitical organizations, political movement affiliations, shared government organizations, and shared military ties. Each political affiliation is color-coded.[38] The Kurdistan Democratic Party (KDP) and the Patriotic Union of Kurdistan (PUK) are well-known to the outside world, whereas Gorran is a new political movement within Iraqi Kurdistan.

The sociogram includes both current and past interactions, such as working in the same committee or for the same project.[39] Understanding and mapping past relations is a critical part of mapping a complex network with multiple subgroups, as movements typically emerge by activating old ties.[40] Especially for political influence, it frequently follows existing human relations as building new rapport can be too conspicuous or costly. From the sociogram, we can see that the overall political landscape in Iraqi Kurdistan is characterized by identifiable and cohesive political parties connected by less conspicuous connective tissue.

By following existing pro-Iranian individuals within the Iraqi government and their prior associations with Kurdish politicians, we can illuminate existing relational pathways between and across major political groups in Iraqi Kurdistan. It is worth noting that

Iranians are leveraging existing interpersonal and interorganizational ties within the Iraqi government in an attempt to extend their access and placement in Iraqi Kurdistan. While the PUK has had a stronger relationship with the Iranians and the Shia militias they back, such as the Badr Brigades, the actual pathways utilized by the Iranian Revolutionary Guard Corps (IRGC) to exert influence in Kurdistan indicate that Iran is also diversifying its ties within Iraqi Kurdistan. Pathways of influence can often be fluid and dynamic. In this regard, mapping the key pathways that connect external actors and organic networks should also focus on temporal changes in the network to anticipate how their interconnectivity changes over time.

The Influential Nodes

Once the overall structure of key pathways is analyzed, we start identifying critical brokers and influencers between and across subgroups in order to understand key individuals who sustain the network. The purpose of this process is twofold. First, it illuminates and identifies those who are important in sustaining the network but not well-known to the outside world; they are often called "emergent nodes."[41] Understanding who the emergent nodes are can broaden options to leverage and shape the network. Second, it establishes quantitative social network metrics to assess each key individual's type of influence as well as relative measure of influence. Once the emergent nodes are estimated with specific metrics, then outside actors can prioritize and select a few to optimize the process of building access and placement within the network.

In Iraqi Kurdistan, it is true that traditional power brokers and leaders of the PUK and KDP still wield an enormous amount of power. However, the perceived concentration of power among these few leaders makes influencing the regions quite challenging. Upon a careful network analysis of the sociogram, we can see that there are other individuals who occupy key locations within the network. Many of those individuals, who have long worked various groups while representing Iranian interests, are not widely known influencers. However, their relative influence can be measured by computing their activities and relations with well-established social network metrics. This is where the quantitative aspect of SNA can be increasingly insightful. For instance, the IRGC seems exceedingly pragmatic in that they have established ties with minority leaders who have organic relations with other major parties, such as the Kurdistan Regional Government (KRG) and PUK in the region.

Table 17.1 summarizes the highest valued agents according to several important metrics, as well as overall key influencers in the overall network. It is worth noting that Yousif Mohammad and Bapir Kaka Mala Sleman are both members of minority parties, who function as brokers within Kurdistan's government.[42] In other words, SNA can reveal highly influential nodes who are not necessarily the most obvious.

Table 17.1. Key Actor Values [43]

Rank	Node	Key Actor Value
1	Ayeden Maruf Salim Ahmed	0.048
2	Sabah Jalloub Faleh Hami Al-Sa'idi	0.043
3	Imad Yokhanna Yaqo Yokhanna	0.037
4	Mathhar Khader Naser	0.032
5	Bapir Kaka Mala Sleman	0.031
6	Safiyah Taleb Ali Alsouhail	0.028
7	Yonadem Yousef Kanna Khoshaba	0.027
8	Mahmous Ali Othman Omar	0.022
9	Salim Toma Kako	0.021
10	Kathem Atiyah Alshammari	0.021
11	Yousif Mohammad	0.02
12	Yaqub Gorgis Yaqo Klya	0.02

It is worth noting that the minority groups have ideally positioned themselves to be able to access major political factions, indicated by their high boundary spanner potential. Boundary spanner potential indicates structural positions that allow access or influence across multiple groups.[44] Put differently, boundary spanners have great potential to bridge and connect multiple subnetworks.[45] It is also noteworthy that Iran seems willing to work with those with the most potential for connecting multiple groups as opposed to those who are just politically aligned with Iranian interests.

Given that these minority groups' leaders have shown a great deal of pragmatism by working with various major factions, these potential brokers provide great opportunities for the United States to enhance its influence in the region as well. Being able to identify and locate these key brokers can be a critical step toward minimizing and undermining adversarial influence in Iraqi Kurdistan. For example, Yousif Mohammad can potentially provide multiple avenues of approach to the KDP or Gorran to counter Iranian influence within the KRG.

Table 17.2. Key Influential Brokers[46]

Rank	Node	Boundary Spanning Value
1	Kardo [last name redacted]	0.034
2	Mawlood Murad Mohyeldin	0.033
3	Yousif Mohammad	0.027
4	Mustafa Sayid Qadir	0.025
5	Kamal [last name redacted]	0.024
6	Pishtiwan Sadiq	0.022
7	Farsat Ahmad Abdullah	0.022
8	Salar Mahmud Murad Ali	0.021
9	Suzan Shahab Nuri	0.019
10	Abdullah Mahmud Muhammad	0.019
11	Arez Abdullah Ahmed	0.018
12	Bapir Kaka Mala Sleman	0.017

Mapping the Kurdish political landscape in Iraq yields powerful insights relevant to how to operate effectively in the complex networked environment. It demonstrates that mapping relational dynamics is critical to lifting the fog of complex operational environment. SNA, when properly executed, can shed much light on not only the pathways used for coordinating operations and narratives, but also inconspicuous yet key individuals who perform such functions. Key is understanding both the underlying concepts and techniques that reveal the hidden structures and interactions of networks.

Understanding the complexity of networked adversaries is a daunting task. Part of the methodological and conceptual challenge is to reduce the complexity without degrading our ability to cope with its contextual nuance. As shown in the Kurdistan example, it is possible to understand how state actors actively try to leverage existing or emerging networks to increase their influence in that environment. However, it does require a conceptual understanding of what comprises such networks and what methodological tools are available to illuminate key pathways and key brokers that keep that connective tissue functioning.

SNA, combined with a deep understanding of the sociopolitical conditions that enable network emergence, can be particularly powerful. It should be noted that mapping social relations has its limitations, such as a high dependency on data fidelity and availability and a potential temporal lag between observation and changes in network dynamics. However, such weaknesses typically apply to all analytic procedures, and not exclusively to SNA. What should be stressed instead is the need to develop an intelligence system that analyzes interconnectivity of networked adversaries by continuously mapping and updating relational data. Just as the TF transformation is characterized by extensive interconnectivity and distributed decisionmaking, the same logic must be applied to how

we understand and analyze the dynamics of network connectivity within a broad human domain, characterized by both transnational actors and localized influencers. As rapid and routinized communication helped the TF form a collective consciousness of the mission and the battlespace, it is also critically important to map and analyze how individual and parochial narratives are aligned to support the ideological appeal of networked adversaries. Again, such mapping and analysis is not infeasible. The CORE Lab at the Naval Postgraduate School has repeatedly utilized various mapping techniques from social media outlets and shown in detail how ISIL has adapted its narrative to align itself with various warring factions in Syria.[47] Much like physical relational ties, insurgent and terrorist narratives can be understood as a system of themes, idioms, and resonating cultural norms.[48] This is not a trivial observation. Part of fighting in the complex networked environment is waging "battles of the story" and understanding how stories of battles are composed and aligned with political and strategic interests.[49]

Conclusion

As the TF transformation and the Kurdish example of mapping the human domain suggest, the fog of complex networks can be lifted; change is not necessarily followed by chaos. Our ability to harness this complexity can be enhanced by mapping and analyzing the conditions that underpin network dynamics, interaction pathways, and key influencers. This is in essence a two-prong race. On one hand, it hinges on how we internally network our organizations and collective awareness in order to increase our adaptive agility against networked threats. On the other hand, it also requires a concerted effort to map and illuminate the environment, comprising nodes, ties, and boundaries of networked adversaries.

The TF transformation strongly indicates that it is entirely possible, albeit often painfully slow and opposed, for the United States to function and fight as a networked force pursuing a unified objective through shared consciousness. Our adversaries have harnessed the strategic utility of this organizational innovation. The sheer complexity of various alliances between nonstate actors and external sponsors is just a symptom of a much larger pattern of warfare characterized by increasingly transnationalized, protracted, movement-centric, and networked conflicts.[50] There is no doubt that we are late to the game. Powerful states typically do not have the luxury of agile adaptation frequently associated with less powerful states leveraging nonstate actors. "The (b)end of history," as John Arquilla described it, where states and networks coexist for strategic competition, cannot be won by linear thinking and hierarchical execution.[51] We hope that the TF transformation and the human domain approach we have discussed in this chapter pave the way forward for our nation to harness and utilize the strategic utility of networks. The era of organizational innovation will favor those who outpace others in learning how to interface and interact with networks toward their strategic objectives.[52]

Notes

[1] Glenn Johnson and Doowan Lee, "Revisiting the Social Movement Approach to Unconventional Warfare," *Small Wars Journal* 7, no. 11 (2014).

[2] U.S. Army Special Operations Command, *ARSOF 2022* (Fort Bragg, NC: United States Army John F. Kennedy Special Warfare Center and School, 2013), 3.

[3] John Arquilla and David Ronfeldt, *The Advent of Netwar* (Montclair, NJ: RAND Corporation, 1996), available at <http://www.rand.org/pubs/monograph_reports/MR789.html>.

[4] Ibid., 6.

[5] Ibid., 11.

[6] Ibid., 81-82.

[7] Note that internal conflicts can be a civil war or an internal political confrontation, or both.

[8] Department of Peace and Conflict Research, "Uppsala Conflict Data Program," *Uppsala Universitet,* available at <http://www.pcr.uu.se/research/ucdp/>.

[9] Christopher Reuter, "The Terror Strategist: Secret Files Reveal the Structure of Islamic State," *Spiegel*, April 18, 2015, available at <http://www.spiegel.de/international/world/islamic-state-files-show-structure-of-islamist-terror-group-a-1029274.html>.

[10] In the SOF community, this is conceptualized as "operating in the human domain."

[11] Found in: General Stanley McChrystal, Tantum Collins, David Silverman, and Chris Fussell, *Team of Teams: New Rules of Engagement for a Complex World* (New York, NY: Penguin, 2015), 22*,* referencing the U.S. State Department annual terrorism reports, which reported 198 "significant" terrorist incidents in Iraq in 2004, compared with the worldwide total of 175 in 2003, 22 of which occurred in Iraq.

[12] Of the 20,000 deaths worldwide from terrorist attacks, 65 percent were in Iraq (13,000 deaths). Found in: McChrystal et al., *Team of Teams,* 22; referencing: National Counterterrorism Center, *Report on Terrorist Incidents - 2006,* April 30, 2007, available at <http://www.fbi.gov/stats-services/publications/terror_06.pdf>.

[13] David Snowden and Mary Boone, "A Leader's Framework for Decision Making," *Harvard Business Review*, November 2007, available at <https://hbr.org/2007/11/a-leaders-framework-for-decision-making>.

[14] F3EA was derived from similar targeting and decisionmaking processes, such as the well-known OODA loop (Observe—Orient—Decide—Assess) that was associated with fighter pilots. Found in: McChrystal et al., *Team of Teams,* 50.

[15] Ibid., 169-170.

[16] Johnson and Lee, "Revisiting the Social Movement Approach to Unconventional Warfare."

[17] David Kilcullen, *The Accidental Guerilla: Fighting Small Wars in the Midst of a Big One* (New York, NY: Oxford University Press, 2011).

[18] Emphasis added by author. TRADOC Pamphlet 525-3-1, *The U.S. Army Operating Concept* (Washington, DC: Department of the Army, 2014).

[19] Derek Raymond, "Human Domain Mapping in the 21st Century," *Small Wars Journal* (2015); TRADOC Pamphlet 525-3-1, *The U.S. Army Operating Concept*.

[20] United States Special Operations Command, *Operating in the Human Domain, Version 1.0* (Tampa, FL: USSOCOM, August 2015), 38.

[21] Ibid.

[22] For a detailed comparison of counter-IED strategies, see: Lora Weiss, Elizabeth Whitaker, Erica Briscoe, and Ethan Trewhitt, "Evaluating Counter-IED Strategies," *Defense and Security Analysis* 27, no. 2 (2011).

[23] These processes are mostly informed by social network analysis and social movement theory.

[24] Derek Raymond, "Combating Daesh: A Socially Unconventional Strategy" (Master's thesis, Naval Postgraduate School, June 2015).

[25] An antecedent condition can be defined as "a phenomenon whose presence activates or magnifies the action of a causal law or hypothesis." Stephen Van Evera, *Guide to Methods for Students of Political Science* (Ithaca, NY: Cornell University Press, 1997), 9-10.

[26] Kilcullen, *The Accidental Guerilla.*

[27] Doowan Lee, "A Social Movement Approach to Unconventional Warfare," *Special Warfare Magazine* 26, no. 3 (2013): 30.

[28] Benjamin Smith, "Collective Action with and without Islam: Mobilizing the Bazaar in Iran," in *Islamic Activism: A Social Movement Theory Approach,* ed. Quintan Wiktorowicz (Bloomington, IN: Indiana University Press, 2004), 187-9.

[29] Ibid.

[30] Mohammed M. Hafez, *Why Muslims Rebel* (Boulder, CO: Lynne Rienner Publishers, 2004), 10-16.

[31] Doug McAdam, *Political Process and the Development of Black Insurgency, 1930-1970* (Chicago, IL: University of Chicago Press, 1982), 11-16.

[32] David A. Snow and Scott C. Byrd, "Ideology, Framing Processes, and Islamic Terrorist Movements," *An International Quarterly Review* 12, no. 1 (2006).

[33] David A. Snow, E. Burke Rochford, Jr., Steven K. Worden, and Robert D. Benford, "Frame Alignment Processes. Micromobilization, and Movement Participation," *American Sociological Review* 51, no. 4 (1986): 467-76.

[34] Ibid.

[35] Mario Diani and Doug McAdam, ed. *Social Movements and Networks, Relational Approaches to Collective Action* (New York, NY: Oxford University Press, 2003), 7.

[36] The nodes are sized by each person's potential to bridge different groups. In this case, we are using a specific social network measure called "boundary spanning," that captures intergroup and intragroup ties. Research was conducted by Christopher Couch and Doowan Lee at the Naval Postgraduate School in Monterey, California. This project was initiated to support U.S. Special Operations Command Central in Tampa, Florida. The sociogram was generated with ORA Software, Kathleen M. Carley, Center for Computational Analysis of Social and Organizational Systems, and Carnegie Mellon University. Copyright 2001-2011. A full analysis can be found in Christopher Couch, "Aghas, Sheiks, and Daesh in Iraq, Kudish Robust Action in Turmoil" (Master's thesis, Naval Postgraduate School, June 2015).

[37] Stanley Wasserman and Katherine Faust, *Social Network Analysis: Methods and Applications,* (Cambridge: Cambridge University Press, 1994), 12.

[38] The yellow nodes represent the political entities closely aligned with Iran, the red nodes represent members of the KDP, the blue nodes show members of the PUK, the purple nodes denote members of the newly formed Gorran Party, the green nodes represent the two Islamist Kurdish parties, and the light blue nodes show minority political parties. The light purple nodes denote an unknown party affiliation. The resulting network is composed of 919 individuals and 32,030 ties.

[39] The dataset is coded from every article on Kurdistan in the Al-Monitor newspaper written in 2014 and various other online sources. A full list of sources is available upon request.

[40] Donatella della Porta, "Recruitment Processes in Clandestine Political Organizations: Italian Left-Wing Terrorism," *International Social Movement Research* 1 (1988).

[41] Kathleen Carley, "Destabilization of Covert Networks," *Computational and Mathematical Organization Theory* 12, no. 1 (2003).

[42] ORA calculates the top-ranked agents in terms of the following metrics: Emergent Leader, In_the_ Know, Clique Count, Eigenvector Centrality, Eigenvector Centrality Per Component, Hub Centrality, Authority Centrality, Betweenness Centrality, How they Connect Groups, and Group Awareness.

[43] Data Generated by ORA. Reproduced with author's permission from Couch, "Aghas, Sheiks, and Daesh in Iraq, Kudish Robust Action in Turmoil." Full names can be obtained by contacting the authors.

[44] For a detailed discussion of how brokers shape and sustain networks, see: Mario Diani, "'Leaders' or Brokers? Positions and Influence in Social Movement Networks," in *Social Movements and Networks*, *Social Movements and Networks, Relational Approaches to Collective Action*, ed. Mario Diani and Doug McAdam (New York, NY: Oxford University Press, 2003); Shin-Kap Han, "The Other Ride of Paul Revere: The Brokerage Role in the Making of the American Revolution," *Mobilization: An International Quarterly* 14, no. 2 (2009).

[45] BSP technically is a calculation of the betweenness centrality of a node divided by the degree centrality of that node.

[46] Data generated by ORA. Reproduced with author's permission from Couch, "Aghas, Sheiks, and Daesh in Iraq, Kudish Robust Action in Turmoil." Full names can be obtained by contacting the authors.

[47] Gregeory Freeman and Robert Schroeder, *Social Media Exploitation: An Assessment* (Monterey, CA: Naval Postgraduate School CORE Lab, September 2014).

[48] Snow and Byrd, "Ideology, Framing Processes, and Islamic Terrorist Movements."

[49] John Arquilla, "The (B)end of History," *Foreign Policy*, December 15, 2011, available at <http://foreignpolicy.com/2011/12/15/the-bend-of-history/>; Lee, "A Social Movement Approach to Unconventional Warfare."

[50] Johnson and Lee, "Revisiting the Social Movement Approach to Unconventional Warfare."

[51] Arquilla, "The (B)end of History."

[52] Ibid.

This chapter was written with assistance from Jessica Craige.