2014

To Build a Network

Arquilla, John

Prism

Prism, Vol. 5, No. 1, pp. 23-33, 2014.
https://hdl.handle.net/10945/43369

PRISM

VOL. 5, NO. 1 2014

CCO
CENTER FOR
COMPLEX OPERATIONS
DIPLOMACY • DEFENSE • DEVELOPMENT

A JOURNAL OF THE CENTER FOR COMPLEX OPERATIONS

PRISM
VOL. 5, NO. 1 2014

ISSN 2157-0663

About

PRISM is published by the Center for Complex Operations. PRISM is a security studies journal chartered to inform members of U.S. Federal agencies, allies, and other partners on complex and integrated national security operations; reconstruction and state-building; relevant policy and strategy; lessons learned; and developments in training and education to transform America's security and development

Communications

Constructive comments and contributions are important to us. Direct communications to:

Editor, PRISM
260 Fifth Avenue (Building 64, Room 3605)
Fort Lesley J. McNair
Washington, DC 20319

Telephone:
(202) 685-3442
FAX:
(202) 685-3581
Email: prism@ndu.edu

Contributions

PRISM welcomes submission of scholarly, independent research from security policymakers and shapers, security analysts, academic specialists, and civilians from the United States and abroad. Submit articles for consideration to the address above or by email to prism@ndu.edu with "Attention Submissions Editor" in the subject line.

FEATURES

BOOK REVIEWS

LESSONS LEARNED

INTERVIEW

www.ndu.edu

To Build a Network

BY JOHN ARQUILLA

The fundamental dynamic of the Cold War era was an arms race to build nuclear weapons. But in the long, often covert, "cool war" against al-Qaeda and its affiliates that began in earnest after September 11, 2001, the driving force has been – and continues to be – an "organizational race" to build networks. It has grown increasingly apparent that the latest advances in information technology have greatly empowered flat, essentially leaderless groups unified more by pursuit of a common goal than any kind of central control. In the elegant phrasing of David Weinberger, co-author of a key contribution to the emerging information-age canon, *The Cluetrain Manifesto*, networks, particularly web-enabled ones, are comprised of "small pieces loosely joined."[1] Weinberger's language offers a particularly apt description of al-Qaeda today, as the group's original concentrated core, formed around Osama bin Laden and Dr. Ayman al-Zawahiri, has long since given way to a far flatter, much more widely dispersed set of relatively independent cells and nodes.

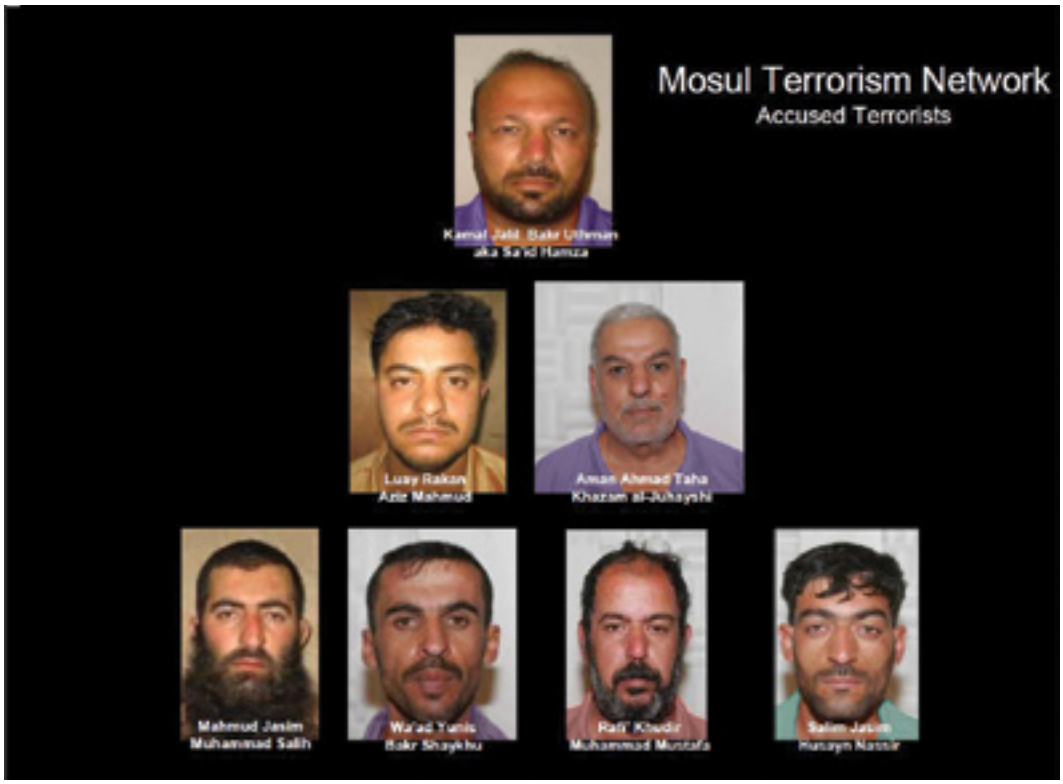
Thus has the world's premier terrorist network survived over a dozen years of major efforts aimed at its eradication. Indeed, far from being on "the verge of strategic defeat," as former defense secretary Leon Panetta was wont to say,[2] al-Qaeda has thrived by redesigning itself away from any serious reliance on central leadership. In this way, the targeted killings of any number of "high-value targets," including of course bin Laden himself, have had little effect on the organization's viability and vitality. So today a handful of American forces are back in Iraq fighting the al-Qaeda splinter group ISIS – and the country is burning. In Syria, al-Qaeda, ISIS and others are leading the fight against the Assad regime, much as terrorist networks played a similar role in the overthrow of Libyan dictator Moammar Qaddafi – and may have been involved, at least tangentially, in the humiliation inflicted upon the United States by the attack on the American diplomatic mission in Benghazi.[3] The al-Qaeda network is operating in many other places, too: Algeria, Mali, Mauretania, Nigeria, Somalia, and Yemen – to name just a few locales.

It is as if the death of bin Laden opened up al-Qaeda's "strategic space," creating room for the networked global insurgency envisioned a decade ago by its leading strategist, Abu Mus'ab al-Suri, in his *Global Islamic Resistance Call*. Over the past few years, al-Qaeda has taken on almost

Dr. John Arquilla is Professor and Chair in the Department of Defense Analysis at the Naval Postgraduate School He is the author of many articles on a wide range of topics in military and security affairs. His books include Network and Netwars and Afghan Endgames.

all of the characteristics of al-Suri's "call." He was captured in Pakistan in 2005, and later turned over to the Assad regime – his *nom de guerre* means "the Syrian."[4] Rumor intelligence suggests that al-Suri was released in the wake of the rebellion in Syria, but there have been no confirmed public sightings. This hardly matters. As he himself would no doubt say, it is the leaderless network concept that is important. There is no need to have a great man at the head of the organization. No one is in charge and, for a "dark network" of terrorists, it is far better to operate without a formal leadership structure. As al-Suri makes clear in his writings, the flatter the network, the better.[5]

Clearly, al-Qaeda is fully invested in the organizational race to build networks. That terrorists would take so well to networking is something my long-time research partner David Ronfeldt and I have been worrying about for the past two decades. Our response back in the mid-1990s to the then-embryonic threat from terrorist networks was to contend that, in a great conflict between nations and networks, the generally hierarchical structure of nations would not serve them well in efforts to come to grips with networks. And so from early on we saw a need to enter the organizational race by starting to build networks of our own. Our key point: "It takes networks to fight networks."[6] Many have taken up this mantra in the eighteen years since we first intoned it, most notably General Stanley McChrystal, perhaps the most network-oriented of all American military leaders.[7] Sadly, some loose comments by a few of his subordinates about



2007 al-Qaeda in Mesopotamia (AQIM) network chart in Mosul.

senior political leaders led to his dismissal. Thus an articulate voice in favor of taking a more networked approach was removed from the fight – a terrible self-inflicted wound from which the U.S. military has yet to recover fully.

And the problem goes well beyond the armed services. In the realm of intelligence, for example, the most significant organizational change made in the years since 9/11 was to add yet another vertical layer to the existing hierarchy by creating a directorate of national intelligence. The commission members charged – by the President and Congress – with finding potent remedies to the lapses that contributed to the surprise attacks on America in 2001 were in total agreement about calling for much greater inter-organizational cooperation and information sharing. Nevertheless, their policy recommendation was to create an entity that would wield ever greater central control.

The wiring diagram for the new directorate makes this abundantly clear in the final report of the 9/11 Commission.[8] And the one other major organizational change made to the U.S. government was the creation of a Department of Homeland Security – yet another massive, bulky hierarchy. Its sheer size and complexity contributed significantly to the slow, confused response to the Hurricane Katrina disaster back in 2005. But if the civilian departments and agencies of the U.S. government have had a difficult time grasping the art of building networks, the military, by way of contrast, has shown a considerable and growing aptitude for doing so.

Some military-oriented examples of network-building

Given that small but key groups of civilian and military leaders accept the notion that the best tool for countering a hostile network is a network of one's own, the central issue has come to revolve around exactly how one should go about building a network. The mixed experiences with creation of a directorate of national intelligence and the homeland security apparatus imply that fruitful insights into networking are perhaps more likely to be found "out at the edges" rather than at the policy-making core. And sure enough, even a modest amount of investigation quickly yields very interesting results. For it is "out there" that counterterrorist networks have formed up and have achieved some quite remarkable results.

One of the lesser known but more successful network enterprises operates out of a former French Foreign Legion base, Camp Lemonnier, in Djibouti in the Horn of Africa. From here just a few thousand soldiers, Marines, and civilians operate in conjunction with allies and many departments of the U.S. government to illuminate dark terrorist networks as a first step toward eliminating them. *New York Times* reporters Eric Schmitt and Thom Shanker have thoughtfully assessed the operation in this way:

> *To an unusual degree, the mission has lashed together the government's entire national security structure. Officers there describe a high level of cooperation among conventional military forces, the more secretive special operations teams, and the American intelligence community. Representatives from other government agencies, including customs and agriculture, routinely pass through.*[9]

With a decade of counterterrorism successes to its credit, along with major contributions to humanitarian aid and demining operations, the network operating out of Djibouti has gained official acceptance – after some

early efforts by the Pentagon to close it down – and is seen as "the centerpiece of an expanding constellation of half a dozen U.S. drone and surveillance bases in Africa, created to combat a new generation of terrorist groups across the continent, from Mali to Libya to the Central African Republic."[10]

In short, Camp Lemonnier serves as the key node – the hub, in fact – of a hub-and-spokes network that ties together civilian and military personnel from the United States and its allies in the war against al-Qaeda and its affiliates. And the results achieved with relatively minute manpower and but a tiny fraction of the level of material resources devoted to, say, the campaign in Afghanistan,[11] have been remarkable. With amazing economy of force the Djibouti operation has played a key role in helping to inflict defeats on al-Qaeda and affiliates in Somalia, Yemen, and other locales that fall within its area of responsibility.

Moving from the Horn of Africa to the Philippines, one can find another excellent example of successful networking. With around 600 soldiers, the Combined Joint Special Operations Task Force – Philippines (CJSOTF-P) has worked closely with the Armed Forces of the Philippines to inflict stinging blows on the Moro Islamic Liberation Front and the related but more criminally-oriented Abu Sayyaf Group. Beyond its successes in counterterrorist field operations, the CJSOTF-P has also played a key role in ensuring the completion of civic improvement projects that have built schools, roads, and medical and disaster relief facilities. Its work has drawn high praise from the NGO community as well. Mark Schneider, a senior vice president with the International Crisis Group, views the CJSOTF-P "as a success story, especially in terms of winning hearts and minds through civic action and medical assistance projects."[12]

Another key networking success "at the edge" unfolded in, of all places, Iraq. From the outset of the mass uprising that began in earnest in August 2003, the insurgency there proved nettlesome, with levels of violence against innocent Iraqis mounting precipitously by 2006, a time when nearly 100 non-combatants were being killed each day.[13] Yet, by the end of 2008, the violence had receded, with civilian deaths decreasing by about three-fourths, to the 9,000/year range. And the casualty rates continued to drop sharply until U.S. forces left at the end of 2011. However, the violence arose once again in the wake of the American departure, with losses in 2013 amounting to the worst level in the past five years.[14] The conventional wisdom about why things got dramatically better seven years ago was that President George W. Bush's decision to send an additional 28,000 troops to Iraq – "the surge" – finally gave commanders sufficient resources to deal effectively with the insurgency.[15]

But what turned the campaign in Iraq around was not simply the addition of five brigades. There was also a critically important shift to a new concept of operations based on the idea of getting off the few dozen large forward operating bases (FOBs) on which most U.S. troops were posted and redeploying them – in platoon-sized packets, with similar-sized friendly Iraqi forces – to well over a hundred small outposts in areas where the violence was worst. Thus a physical network emerged, one comprised of many small nodes, improving the response time to attacks, the intelligence-gathering process, and overall relations with the populace.

The physical outpost network was complemented by the rise of a social network that grew from reaching out to many of the Sunni insurgents who had been fighting the occupiers for years. Some 80,000 of them switched sides, becoming the "Sons of Iraq" who formed such a big part of the Awakening Movement that drove a serious wedge between al Qaeda operatives and the Iraqi people. The "surge brigades" were not really necessary to achieve these results, as there were never more than about 10 percent of the troops in-country operating from these outposts, or more than about another 10 percent involved in supplying them, or protecting them from nearby "overwatch" positions. The key had simply been the willingness to adopt a network-building turn of mind, something that many platoon and company commanders, and their immediate superiors, had begun to do at the grassroots level, even before the surge.[16]

By 2008, with the additional surge brigades now gone, it was clear to all that the counterinsurgency was not primarily a numbers game. The key was to populate the physical network with platoon-sized outposts and to keep reaching out to the Iraqi people. This was the way to "illuminate and eliminate" the enemy network. General Petraeus put the matter best in his commander's guidance of June 2008:

> *You can't commute to this fight. Position Joint Security Stations, Combat Outposts, and Patrol Bases in the neighborhoods we intend to secure. Living among the people is essential to securing them and defeating the insurgents.*
>
> *We cannot kill our way out of this endeavor. We and our Iraqi partners must identify and separate the "reconcilables" from the "irreconcilables" through engagement . . . We must strive to make the reconcilables a part of the solution, even as we identify, pursue, and kill, capture, or drive out the irreconcilables.*
>
> *Defeat the insurgent networks . . . Focus intelligence assets to identify the network.*[17]

Thus was a network built that defeated the al-Qaeda network in Iraq, and kept the levels of violence down – for years, until after the American withdrawal and the subsequent alienation of the Sunnis by the Baghdad government, which gave the terrorists the opportunity to come back.

Network-building from the Byzantines to the Battle of Britain

Clearly, the central organizational insight into network-building is the notion of being willing to create a large number of small units of action, and allowing them to operate relatively freely in pursuit of a common goal – even if in the absence of any serious degree of direct central control. While the recent examples of network-building described in the previous section are both interesting and valuable, it is important to mine earlier history as well for ideas about networking. "Looking back" is a very useful way to "look ahead." The way to do it is to search for examples of the creation of systems comprised of many small nodes, cells, or units of action. And, while not particularly abundant, there are indeed some quite salient examples.

The security strategy of the Byzantine Empire comes easily to mind. Constantinople outlasted Rome by a thousand years. How? In part by making the most of its limited

resources. For centuries, the extensive eastern land frontier – the western part of the empire was shored up by Byzantine naval mastery – was subject to continual raids and invasions. There were never enough troops to maintain a preclusive, perimeter defense. So instead the Byzantines resorted to an extensive system of small outposts whose mission was to detect and pass the word of incursions – by couriers, with signaling mirrors, fire at night and smoke by day – to military "hubs" where armored cavalry striking forces were at the ready. In this way, attackers gained only a minimal advantage of surprise, and were soon beset from many sides (I would say, "swarmed") by quick-reaction forces.[18]

The "field manual" of the time, the Tenth Century C.E. *De Velitatione* – which translates as *Skirmishing* – makes clear that a networked defensive system can also be used on the offensive – particularly if coupled with the vibrant intelligence networks that the Byzantines nurtured along the edges of their empire. Edward Luttwak's recent research into this security system has led him to conclude that it enabled a "military renaissance" a millennium ago that gave the Byzantine Empire a new lease on life. As Luttwak puts it so well, about the more proactive aspect of the strategy, "the aim is to do much with little, with raids by relatively small forces that magnify their strength by achieving surprise."[19] Bernard Montgomery, one of the great captains of the 20th century, expressed much admiration for the Byzantine ability to use swarm tactics, offensively and defensively, noting how the network of outpost garrisons and mobile strike forces succeeded against a range of adversaries, from Avars to Arabs.[20]

A modern historical example that featured elements quite similar to the Byzantine network can be found in the defensive system propounded by Air Chief Marshal Hugh Dowding of the Royal Air Force – whose Fighter Command won the Battle of Britain in 1940. German military forces, fresh from a string of *blitzkrieg* victories culminating with the fall of France, found themselves unable to cross the English Channel – so an attempt was instead made to try to bomb Britain into submission from the air. Pre-war estimates of the destructive potential of strategic air attack had been particularly dire, and there was much debate about the correct defensive organizational form to adopt and the right combat doctrine to employ.

A major point of view was the "big wing" school of thought, whose goal was to mass as much defensive force as possible – in practical terms, this meant crafting units of action comprised of three squadrons, some 75-90 fighters – against enemy bomber streams. The problems with this system were two-fold: *Luftwaffe* leaders were clever about where they were going to strike next, often switching direction after crossing the British coast; and, even when the target areas were known, big wings would take a long time to come together from scattered airfields. One of Dowding's chief subordinates – and a key supporter – was Air Vice-Marshal Keith Park, who argued that "the assembling of large formations of fighters was both time-wasting and unwieldy."[21]

Instead of this approach, Dowding and Park preferred to allow single squadrons of just two dozen fighters to engage the large attacking bomber formations – and their fighter escorts – independently, as soon as information that flowed in about German intentions from any of the forty Chain Home radar stations positioned along the coast was confirmed by the relevant outposts of the

thousand-node Observer Corps network that was sprinkled all over southeastern England.[22]

It turned out that Dowding and Park were right; the networked, swarm-oriented approach won out. Dowding, however, nicknamed "Stuffy," had made many enemies, and was sacked as soon as the crisis passed. Prime Minister Winston Churchill and most of Britain's senior military leadership may not have properly valued or rewarded Dowding for what he had achieved, but official German war documents make clear that the *Luftwaffe* had a correct understanding of how and why their campaign failed:

> *The defense was forewarned of each attack by an unbroken chain of radar stations, which made surprise almost impossible. This and astute ground control saved the British fighter arm from being knocked out and German air sovereignty being won.*[23]

The 30,000 civilian volunteers of the Observer Corps – the human nodes in the vast early-warning network formed to help defend their country against air attack – made out better than Dowding. They refused to be paid for their services; but in April 1941 King George VI made them the *Royal* Observer Corps in recognition of the contribution they made to victory in the Battle of Britain.[24]

A Systematic Approach to Network-Building

It should be clear from the foregoing examples – both the more recent and ongoing ones, as well as instances from earlier eras – that network-building hardly requires resort to alchemy. The foundational requirement, organizing into Weinberger's "small pieces, loosely joined," is fairly simple to meet – if institutional opposition is overcome – and the power of the "small and many" can be seen in all the cases considered. But there is surely more that is necessary to build strong, effective networks. For David Ronfeldt and me, there are four additional areas beyond organizational design that must be addressed in the network-building process: the network's narrative; its social basis; the operating doctrine employed; and the technological "kit" required.[25]

The *narrative* is the story that draws people to the network – and keeps them in it, even in adversity. Of the examples considered in this article, the Iraqi Awakening Movement provides perhaps the most salient case wherein a whole counterinsurgent network was energized and enlivened by a narrative about how al-Qaeda operatives were exploiting Iraqis, and that coalition forces were coming to outposts right among the people to protect, serve, and liberate. A measure of the effectiveness of this narrative was the fact that many tens of thousands joined the Sons of Iraq in support of this effort. The sharp drop in violence – mentioned earlier – that soon followed is yet another indicator that this narrative had positive effects.

In terms of the *social aspect* of the network-building process, the great challenge is in bringing together actors from diverse places and making the network the focus of their loyalty. Militaries in most countries bring in recruits from all over their societies and create cohesion in service to "the nation." Terrorist organizations like al-Qaeda have been able to do this sort of thing, too, the difference being that they instill a loyalty to *the network*. In al-Qaeda's case, and among its affiliates, the ability to do this has been aided, quite often, by skillful exploitation of religious and kinship ties. Nation-states seldom have similarly strong social bonds; and social cohesion is further complicated by the fact that members of

networks are generally drawn from organizations, services, or the various departments of government to whom they continue to feel primary loyalty.

Dealing with the social component is not easy, but I would say that the U.S. Special Operations Command (SOCOM) provides an example of the successful creation of a sense of community among military elites drawn from all of the services. While all retain the outer trappings and many of the inner practices of their parent services, there is at the same time a crucially important sense of social fraternity and trust that goes beyond the color of their uniforms.

The current challenges for SOCOM at this social level of networking are to: 1. foster a strong sense of common identity among members of the relatively recently created United States Marine Corps Special Operations Command (MARSOC); and 2. make a similar social connection with international military elites in pursuit of the "global special operations network" that Admiral William McRaven has made the centerpiece of his long-term SOCOM strategy. As he put it in June 2013 when his plan was first unveiled;

> *I need to get the military buy-in first, and then very quickly we move to the interagency (community), and then very quickly we move to our partners and allies.*[26]

Clearly, he understands that network-building requires a very sound social foundation.

The doctrine, or concept of operations, that networks of all sorts employ – from mass popular movements like the Arab Spring to insurgents and, increasingly, even conventional traditional military operators – is to "swarm." Their many small elements become habituated to coming together, often from several points of the compass, to converge upon a particular place and/or opponent. For a social swarm this might be Tahrir Square; for an outpost-and-outreach counterinsurgent network the convergence could come on a more operational scale – as was the case in Anbar Province in Iraq several years ago. Even the early historical cases considered herein reflected use of swarm tactics. Both the Byzantines on their eastern frontier and the Royal Air Force in the Battle of Britain swarmed their opponents. *Networks swarm*. If you intend to build one, make sure it has a capacity for swarming.

Technological "kit" is the final foundational element to which network-builders should be attentive. It is crucially important that a network's communications be capable of great throughput, but with a high level of security. Sad to say – from a counter-terrorist perspective – al-Qaeda and its affiliates have learned to use the world wide web and the Internet ubiquitously and securely. The network of nations aligned against the terrorists has sufficient levels of connectivity, but not yet the degree of security needed for the most efficient operations. The Byzantines offer an interesting example here: when they wanted to send out warnings of incursions without the raiders knowing, they used riders to pass the word – reasoning that smoke or fire signals would alert their enemies. Less technology may, at times, make for better security.

But even with the availability of high-throughput, secure communications will prove ineffective if the organizational design of a network is vertically- (i.e., hierarchically-) rather than horizontally-oriented to maximize linkages among the many, small nodes that form the best networks. Thus in closing this

discussion of key factors in network-building, we return to the theme of "small pieces, loosely joined," the implication being that organizational design is first among equals. If the organizational structure is not right, even the greatest narrative and a strong, trust-based social ethos will end up being sub-optimized.

What next for networks?

Clearly, Admiral McRaven's effort to build a global special operations network is the broadest, boldest effort under way at present. But another interesting network-building enterprise was forming up, albeit on a smaller scale, in Afghanistan. The village stability operations (VSO) concept there has been very much an exercise in network-building. The core idea is quite similar to the outpost-and-outreach system that emerged in Iraq, beginning in 2006: small American detachments live with Afghan locals and operate from their villages.

The VSO concept tacitly recognizes that the center-outward nation-building experiment in Afghanistan should take a back seat to an "edges-inward" network-building approach. The original plan was to have over 100 of these "small pieces" in place, but this goal has fallen victim to the Obama administration's desire to depart from Afghanistan as swiftly as possible. Perhaps events in Iraq will encourage some rethinking, and the original VSO plan will be reinstated. While some resist the idea hat the networked approach taken in Iraq can also be used to good effect in Afghanistan, others have argued forcefully that the most important, usable lesson from Iraq is that "it takes a network to fight a network."[27]

MC1 Jeffery Williams

A U.S. Soldier assigned to Combined Joint Special Operations Task Force-Afghanistan where patrols were designed to deter insurgent operations and engage residents.

Thus the hypothesis about the value of network-building in the fight against terrorists and insurgents is undergoing a quite rigorous "field test" right now in Afghanistan. Wouldn't it be useful if there were also such a test for networking closer to home, in the area of governance? Given the very low approval levels that elected officials currently suffer under, perhaps one thing that even bitter partisans might agree upon would be to try something bold, in terms of organizational redesign of government. There is even a bit of a blueprint in place, thanks to the work of Leon Fuerth, formerly the national security adviser to Vice President Al Gore.

Since 2001, Dr. Fuerth has been exploring the possibility of moving to a nimbler, more networked model of American governance – and has knitted together his own network of experts along the way. His and his team's work addresses clearly all five of the network-building factors that David Ronfeldt and I think are essential. So in addition to Admiral William McRaven's global initiative, and the emerging VSO network in Afghanistan, I would very strongly recommend pursuit of a third experiment in network-building based on Leon Fuerth's ideas about "anticipatory governance."[28]

Given the evidence presented in this article of cases of successful network-building – both recently and in the more distant past – and the clear evidence that insurgents and terrorists have been racing to expand and improve their networks, we can only hope that our leaders make a firm decision to enter the "organizational race" as well. PRISM

Notes

[1] David Weinberger, *Small Pieces Loosely Joined* (Cambridge: Perseus Publishing, 2002), pp. ix-xi.

[2] See Craig Whitlock, "Panetta: U.S. 'within reach' of defeating al Qaeda," *The Washington Post*, July 9, 2011.

[3] The most recent reporting on the Benghazi attack suggests that the al Qaeda core network did not play "a significant role" in it. See David D. Kirkpatrick, "Deadly Mix in Benghazi: False Allies, Crude Video," *The New York Times*, December 29, 2013.

[4] His given name is Mustafa bin Abd al-Qadir Sitt Maryam Nasar.

[5] The most extensive analysis of al-Suri's work is Brynjar Lia's *Architect of Global Jihad* (New York: Columbia University Press, 2008). Aside from analyzing al-Suri's writings, Lia also provides a thoughtful biography of this engineer-turned-terrorist.

[6] John Arquilla and David Ronfeldt, *The Advent of Netwar* (Santa Monica: RAND, 1996), p. 82.

[7] Stanley McChrystal, "It Takes a Network," *Foreign Policy Magazine*, February 22, 2011.

[8] See the *Final Report of the National Commission on Terrorist Attacks Upon the United States*, authorized edition (New York: W.W. Norton & Company, Inc., 2004), p. 413.

[9] Eric Schmitt & Thom Shanker, *Counterstrike: The Untold Story of America's Secret Campaign Against al Qaeda* (New York: Henry Holt and Company, 2011), p. 190.

[10] Craig Whitlock, "Remote U.S. base at core of secret operations," *The Washington Post*, October 26, 2012.

[11] Which, even now, in the last year of direct combat operations, will see some $80 billion spent there. Overall spending in Afghanistan since 2001 has totaled about $1 trillion.

[12] Cited in Thom Shanker, "U.S. Military to Stay in Philippines," *The New York Times*, August 20, 2009.

[13] See the *Report on Human Rights Violations*, prepared by the United Nations Office of the High Commissioner for Human Rights, and the *United Nations News Service* story that called out the figures just for Iraq from the larger report, "Over 34,000 Civilians Killed in Iraq in 2006" (January 16, 2007). The report notes also that over 36,000 Iraqi civilians were injured in 2006. Even taken together, these figures are dwarfed by the British *Lancet* report that

pegged Iraqi deaths and injuries at far higher levels – though it came under much criticism for faulty methodology.

[14] Casualty figures cited herein for 2008 and 2013 are also from the *United Nations News Service*, which has sometimes reported slightly greater numbers of deaths than other monitors, like Iraq Body Count – but which is always far below the levels suggested by the British *Lancet* study.

[15] Thomas E. Ricks, *The Gamble: General David Petraeus and the American Military Adventure in Iraq, 2006-2008* (New York: The Penguin Press, 2009), especially pp. 106-124, gives equal credit to Generals David Petraeus and Raymond Odierno for embracing the surge plan – despite opposition from some other senior military leaders – and to President Bush for deciding to proceed with it.

[16] An excellent account of how this process began to unfold in an almost spontaneous fashion can be found in Niel Smith, "Anbar Awakens: The Tipping Point," *Military Review* (March-April 2008).

[17] From General David Petraeus, "Multi-National Force-Iraq Commander's Counterinsurgency Guidance," 21 June 2008 (unclassified).

[18] See George T. Dennis, ed., *Three Byzantine Military Treatises* (Washington, D.C.: Dumbarton Oaks Texts, 2009), which treats each element of this strategic concept in detail.

[19] Edward Luttwak, *The Grand Strategy of the Byzantine Empire* (Cambridge: Harvard University Press, 2009), p. 340.

[20] Field-Marshal Viscount Montgomery of Alamein, *A History of Warfare* (New York: The World Publishing Company, 1968), pp. 135-146.

[21] Cited in Derek Wood and Derek Dempster, *The Narrow Margin: The Battle of Britain and the Rise of Air Power*, 1930-1940 (New York: McGraw-Hill, 1961), p. 309.

[22] For details about this process, see Richard Overy, *The Battle of Britain: The Myth and the Reality* (New York: W.W. Norton & Company, 2001), pp. 43-45.

[23] Cajus Bekker, *The Luftwaffe War Diaries*, edited and translated by Frank Ziegler (Garden City, NY: Doubleday & Company, Inc., 1968), p .182.

[24] The Observers helped foster a continuing interest in plane-spotting which has resonated even into recent times, with spotter networks playing a key role in uncovering the secret flights that carried suspected terrorists as part of the "extraordinary rendition" process. See Gerard Seenan and Giles Tremlett, "How planespotters turned into the scourge of the CIA," *The Guardian*, 9 December 2005.

[25] These dimensions of network-building are discussed in detail in our *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica: RAND, 2001), especially pp. 323-343.

[26] Cited in Paul McLeary, "Admiral: Global Special Operations 'Network' to Be Unveiled This Fall," *Defense News*, June 12, 2013. The plan was indeed "unveiled" before Congress last fall – an event that has sparked debate.

[27] See especially the thoughtful analysis by General Stanley McChrystal, "Lesson from Iraq: It Takes a Network to Defeat a Network," *LinkedIn*, June 21, 2013.

[28] See Leon Fuerth and Evan M.H. Faber, "Anticipatory Governance: Winning the Future," *The Futurist*, Volume 47, Number 3 (July-August 2013). For a more complete exposition of the concept, see the full report, same title, published by the National Defense University's Institute for National Strategic Studies in 2012.

Center for Complex Operations (CCO)

Enhancing the U.S. Government's Ability to Prepare for Complex Operations

CCO, a center within the Institute for National Strategic Studies at National Defense University, links U.S. Government education and training institutions, including related centers of excellence, lessons learned programs, and academia, to foster unity of effort in reconstruction and stability operations, counterinsurgency, and irregular warfare—collectively called "complex operations." The Department of Defense, with support from the State Department and U.S. Agency for International Development, established CCO as an innovative interagency partnership.

CCO Was Established to:

- Serve as an information clearinghouse and knowledge manager for complex operations training and education, acting as a central repository for information on areas such as training and curricula, training and education provider institutions, complex operations events, and subject matter experts
- Develop a complex operations training and education community of practice to catalyze innovation and development of new knowledge, connect members for networking, share existing knowledge, and cultivate foundations of trust and habits of collaboration across the community
- Serve as a feedback and information conduit to the Office of the Secretary of Defense and broader U.S. Government policy leadership to support guidance and problem-solving across the community of practice
- Enable more effective networking, coordination, and synchronization to support the preparation of Department of Defense and other U.S. Government personnel for complex operations
- Support lessons learned processes and best practices compilation in the area of complex operations
- Identify education and training gaps in the Department of Defense and other Federal departments and agencies and facilitate efforts to fill those gaps.

Visit the CCO Web site at: http://ccoportal.org

Subscriptions for individuals: http://bookstore.gpo.gov


NATIONAL DEFENSE UNIVERSITY