Nanomanagement: A Challenge to Those Combating Terrorism

By Major Tommy Sowers, U.S. Army

IN 1998, AS PART of my officer training, I recall watching a short promotional video about the future of my profession. The video starred a rotund colonel sitting in a command post of the future. The colonel shouted out orders as he literally armchaired a distant battle, watching it unfold on video monitors. The explosion of an enemy vehicle formed the triumphant conclusion. I remember thinking the actor in particular was comical, and the lesson somewhat confusing, wedged as it was between lessons promoting junior officer leadership and initiative. Yet, in the summer of 2006 in Baghdad's command center, I found myself watching the same scenario unfold in real time. I watched as a general barked orders, surrounded by plasma screens, using Unmanned Aerial Vehicle (UAV) feeds to vector in air and ground forces on a target 20 miles away. With a staff of dozens at his side, he gave commands as specific as "Follow that second truck" and "Tell them, it is the house in the center of the compound," while continually asking his legal officer, "Do you see hostile intent?" The general authorized, coordinated, executed and managed an operation foreseen eight years earlier.

Information has always been valuable in war. The difference today is in the dramatic reduction of its cost. Information Technology (IT) employed on the modern battlefield (e-mail, UAV feeds, video conferencing, GPS, vehicle trackers, sensors) enables the highest levels of an organization to directly influence and monitor the very lowest levels of an organization at increasing speeds and decreasing costs.

Much has been written about al-Qa`ida's use of modern IT and the subsequent power it draws from this medium.[1] More than utilizing IT, many terrorist organizations have either been forced or voluntarily transformed in their organizational structure from traditional hierarchies to networks, or "networks of networks."[2] Where terrorists can readily adopt network structures, for traditional hierarchical professional militaries "the challenge will be to discover how to combine hierarchical and networked designs to increase their agility and flexibility for field operations."[3] Decentralization to widely dispersed units, delegation of tasks once controlled in the center, empowerment of the most junior levels of an organization and encouraging initiative are all hallmarks of both network structure and counterinsurgency strategy, yet anathema to what occurred in the Baghdad command center.

The term micromanagement has long been used to describe a supervisor that closely monitors and controls the actions of his immediate subordinate. Today, we see nanomanagement, or the ability of a supervisor to closely monitor and control the actions of all subordinates throughout an organization. This raises three critical questions. Where did nanomanagement originate? Why is it done? What are its costs?

Military Origins of Nanomanagement: Combating Networks with Networks

The military's efforts to respond to networked enemies fall under the moniker of Network-Centric Warfare (NCW). NCW seeks information superiority, enabled by IT, and "generates increased combat power by networking sensors, decision-makers, and shooters to achieve shared awareness, increased speed of command, high tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization."[4] Moreover, "no less than the embodiment of DoD transformation," NCW provides much of the explanation behind the extensive adoption of networking tools, UAVs and sensors employed in the contemporary military arsenal.[5]

Early advocates of NCW recognized the potential hazards of the military rapidly adopting IT, including "increased potential for information overload, second guessing, micromanagement, stifling of initiatives and distraction."[6] Where information once was in short supply, a torrent of data now deluges and potentially paralyzes, and "inserting new technology into old systems and organizations may create new inefficiencies, even as some current activities become more efficient or effective."[7] Decision-makers must now process an abundance of information and also decide "when to stop collecting and waiting for information and when to take action."[8]

The issue of inefficiencies from monitoring persists in varied forms of literature—principal-agent theory, delegation theory, management theory and transaction costs. The common view throughout is that monitoring comes at a cost both to the monitored and the monitor. For the monitored, time spent quantifying efforts, writing situation reports or reporting to higher command is time spent off delegated tasks. Furthermore, persistent monitoring reduces the risks taken by subordinates, reducing their discretion and pushing up many decisions once made at their level. For the monitor, time processing the deluge of information, or waiting for a more accurate and timely report, comes at a cost. For Leonard, "Truth on the battlefield costs time, lives and supplies. Ignorance is free."[9] Now that senior leaders can nanomanage a distant action, when everyone rushes to

[1] Bruce Hoffman, "Countering Terrorist Use of the Web as a Weapon," *CTC Sentinel* 1:1 (2008). See also Evan F. Kohlmann, "Al-Qa`ida's 'Myspace': Terrorist Recruitment on the Internet," *CTC Sentinel* 1:2 (2008) and Gabriel Weimann, "Al-Qa`ida's Extensive Use of the Internet," *CTC Sentinel* 1:2 (2008).

[2] Gabriel Weimann, *How Modern Terrorism Uses the Internet* (Washington, D.C.: U.S. Institute of Peace, 2004).

[3] John Arquilla and David Ronfeldt, "Information, Power, and Grand Strategy: In Athena's Camp—Section 1," in David Ronfeldt and John Arquilla eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND, 1997), p. 5.

[4] *The Implementation of Network-Centric Warfare* (Washington, D.C.: Department of Defense, 2005), pp. 3-4.

[5] "Network Centric Warfare," Department of Defense Report to Congress, July 27, 2001.

[6] David S. Alberts, *Information Age Transformation: Getting to a 21st Century Military, Information Age Transformation Series* (Washington, D.C.: DoD Command and Control Research Program, 2002), p. 9.

[7] Norman C. Davis, "An Information-Based Revolution in Military Affairs," in David Ronfeldt and John Arquilla eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND, 1997), p. 81.

[8] Alberts, *Information Age Transformation: Getting to a 21st Century Military*, p. 57.

[9] Robert R. Leonard, *Principles of War for the Information Age* (New York: Ballantine Publishing Group, 1998), p. 252.

the sounds of the guns, who is planning, who is thinking, who is directing what will occur when those guns go silent?

Why Nanomanagement?

With these costs, why nanomanage? There are three explanations. Some claim that uncertainty conditions the level of monitoring. Wilson argues that when effort and outcomes are clear, authority can be pushed to the front line. Yet when fighting networks, few pitched battles are fought, front lines formed or penetrated, or progress of winning hearts and minds easily measured. In these uncertain environments, "more discretionary authority in an agency is pushed upward to the top."[10]

In the past, perfect information was limited by time, distance and technology, leading Clausewitz to state, "In war everything is uncertain."[11] Through this fog of war, commanders have peered, leading Van Creveld to argue that "from Plato to NATO, the history of command in war consists essentially of an endless quest for certainty" about the environment, enemy and "last but definitely not least, certainty about the state, intentions, and activities of one's own forces."[12] From these thoughts, nanomanagement can be seen as just another in a long line of efforts to dissipate the fog of war. A UAV feed or hourly reports can easily be justified in providing at least the patina of certainty.

Another explanation sees monitoring as less a response to uncertainty, but motivated by liability and accountability and a natural result of an "accountability culture"[13] and "the audit explosion."[14] With increasing levels of scrutiny, both by superiors and persistent media, "If the administrator is going to get into trouble for what an operator does, the former will find ways of making the decision for the latter."[15] Actions must be visible, traceable, quantified, known and ultimately defensible.

Occam's razor might explain a third and most troubling cause for persistent monitoring by distant superiors—they can, so they do. In professions, especially in the military, senior officers rise through the ranks. Now at the pinnacle of their careers, the tasks of generals shift toward tasks of budget, management, external relations, long-term planning and administration. In short, as professionals rise in organizations, they do less work that forms the heart of the profession.

The ability to nanomanage now allows these senior officers a choice—work on the budget and watch endless PowerPoint slides, or fire a Hellfire missile and watch the action on a plasma. When taking action defines the profession, where the warrior ethos is inculcated, technology now allows those distanced to drift into the fight. Indeed, with the industrial revolution, complexity, distance and scale forced generals to retreat from the front lines. Today, however, the information revolution allows them to stride back to the virtual front.

Nanomanagement and Professions: A Question of Trust

While the above costs and justifications may impact any organization, nanomanagement threatens the essential quality of professional organizations—trust. Wilson summarizes the differences between a bureaucratized and a professionalized workforce in terms of the monitoring of their work, or how much they are trusted. Where the former is highly supervised, the latter focuses on restrictive hiring but once hired leaves the professionals to their methods.[16] More trust equals less monitoring and less costs, a fundamental benefit of training, recruiting and investing in professionals as opposed to bureaucrats.[17] Furthermore, professionals are trusted to use qualitative judgment as opposed to quantitative assessment.[18] The subjective is the purview of the professional. The rise of IT-enabled monitoring, and the insistence on quantifying both efforts and outputs can be seen as an encroachment on professional judgment. How does one quantify and report the shaykh's tone, or how a neighborhood feels? For professions, O'Neill sees the impact of constant monitoring and accounting of actions as severe, "*distorting the proper aims of professional practice* (original emphasis) and indeed as damaging professional pride and integrity."[19] When a senior leader nanomanages a distant battle, or demands ever more accurate and by definition quantified reports, they take back the autonomy so central to professional work.

Conclusion

Nanomanagement—to overcome uncertainty, as a response to increasing accountability, or simply because it provides an escape from the mundane—brings with it costs to any organization. For professional organizations, nanomanagement threatens trust, the *sine qua non* of what it means to be a professional. When fighting networks, adoption of networking technology is not enough. This must be concomitant with organizational change focusing on empowerment and delegation, not centralization and monitoring. In the contemporary fight, the challenge will be learning the right lessons from the rotund colonel.

Major Tommy Sowers is an instructor of American Politics, Policy and Strategy in West Point's Department of Social Sciences. He has served two tours in Iraq as a Special Forces officer. Commissioned through ROTC, he holds a BA in Public Policy from Duke University and an MSc in Public Policy from the London School of Economics. He is currently researching his Ph.D. dissertation through LSE, "Nanomanagement: Technology, Trust and the Death of Professions." He can be reached directly at Thomas.Sowers@usma.edu.

[10] James Q. Wilson, *Bureaucracy: What Government Agencies Do and Why They Do It* (New York: Basic Books, 2000), p. 133.

[11] Carl von Clausewitz, Michael Eliot Howard and Peter Paret, *On War* (Princeton, NJ: Princeton University Press, 1976), p. 156.

[12] Martin L. Van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985), p. 264.

[13] Onora O'Neill, *A Question of Trust* (Cambridge: Cambridge University Press, 2002).

[14] Michael Power, *The Audit Society: Rituals of Verification* (Oxford & New York: Oxford University Press, 1997).

[15] Wilson, *Bureaucracy: What Government Agencies Do and Why They Do It*, p. 133.

[16] Ibid., p. 149.

[17] Jeffrey H. Dyer and Wujin Chu, "The Role of Trustworthiness in Reducing Transaction Costs and Improving Performance: Empirical Evidence from the United States, Japan, and Korea," *Organizational Science* 14:1 (2003).

[18] Gary A. Klein, *The Power of Intuition: How to Use Your Gut Feelings to Make Better Decisions at Work* (New York: Currency/Doubleday, 2004).

[19] O'Neill, *A Question of Trust*, p. 50.