JEM

Network-centric emergency response: The challenges of training for a new command and control paradigm

Lt. Col. Mark Stanovich, USMCR

ABSTRACT

The last two decades have seen technological innovations that have revolutionized the collection and transfer of information, permitting access to and dissemination of massive amounts of data with unprecedented speed and efficiency. These innovations have been incorporated into virtually every aspect of modern society, from personal communications, to commercial and business processes, to governmental function and military operations. The concept of network-centric warfare (NCW) grew out of these new capabilities and has been a prominent topic in strategic and operational discussions in the US military since the late 1990s.

In recent years, the concepts behind NCW have been increasingly applied to emergency response, particularly as responders prepare for an increasingly complex threat spectrum in a post-9/11 world. As emergency responders adopt the technological innovations and organizational concepts that enable network-centric operations, attention should be paid to the lessons learned by the US armed forces in the application of the network-centric approach to war-fighting. Emergency operations centers (EOCs), incident command centers (ICCs), and field personnel will require extensive training and experimentation to sort out the impact of this new technology. They must develop protocols and procedures to leverage maximum advantage, while avoiding the undesirable and damaging effects of that technology improperly applied. Because most emergency response organizations lack the vast training resources of the US military, they must be innovative and adaptable in taking advantage of every opportunity to train their personnel in the assimilation of this new technology.

Key words: network-centric, technological innovations, emergency response, emergency operations centers, incident command centers

INTRODUCTION

The first real tests of the concept of network-centric warfare (NCW) in Afghanistan and Iraq have shown some serious drawbacks and flaws in the theories behind NCW and its impact on traditional paradigms of command and control.

In a January 1998 article in US Naval Institute's *Proceedings*, Admiral Arthur K. Cebrowski and John J. Garstka posited the concept of NCW. Expounding upon developments in business models that have applied new information technology, and considered the next great "revolution in military affairs" (RMA), NCW has at its core the concept of linking networks of sensors, decision makers, and individual soldiers[1] with the purpose of achieving shared awareness, increased tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization.[2] Metcalfe's Law (the power of a network is the square of the number of nodes in that network) is a governing concept of NCW, as is the leveraging of information-intensive interactions between the nodes of the network.[3]

In theory, the small-unit soldier who can access information and intelligence from all collection sources will be able to employ combat assets such as air support, artillery, and electronic warfare (EW) with much more precision, timeliness, and effectiveness than with past capabilities. This superior situational awareness is often called "information superiority,"

which refers to a faster decision-making cycle compared to the enemy. In essence, NCW is intended to compress Boyd's "OODA loop" in order to gain an advantage of decision-making and operational tempo over any prospective enemy.[4]

EMERGENCY RESPONSE AND THE MILITARY PARADIGM

There are major differences between the emergency response community and the US military. Significant distinctions exist in culture, mission, training, and jurisdictional authority, and there is a uniqueness of skill sets and expertise in the emergency response community that is not resident in the armed forces. However, the tasks of exerting command and control and building situational awareness in a dynamic and potentially hostile environment have many common characteristics for both the military and emergency response fields. Additionally, the complexity and lethality of the modern terrorist threat requires more sophisticated and effective methods of command and control. It is, therefore, not surprising that a network-centric approach to emergency response similar to that of NCW has increasingly emerged.

The adopting by emergency responders of the NIMS/ICS command and control structure and the incorporation of new information management and collection technologies are heavily rooted in military models and requirements. The National Incident Management System/Incident Command System (NIMS/ICS), currently being implemented by the Department of Homeland Security (DHS), closely resembles a military C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance)[5] hierarchy. The function and organization of both NIMS/ICS and C4ISR are designed for efficient and effective command and control of large, complex, and dangerous events.

The myriad developments of sensors and collection assets are in many instances adaptations of military technology for use by emergency responders. These include environmental sensors, vehicle tracking, robots, unmanned aerial vehicles (UAVs), chemical, biological, and nuclear materials detection, and human and animal biological monitoring. All of these sensors provide information to responders in much the same way as a military headquarters receives battlefield information.[6]

NETWORK-CENTRIC CHALLENGES

Recent military operations in Afghanistan and Iraq have provided the first "live-fire" critiques of NCW. The challenges faced by the Department of Defense in putting the NCW concept into practice ought to prove highly instructive for the emergency response community.

It is the human dimension of a network-centric approach to emergency response that presents the most formidable set of challenges. Technical obstacles, the size and weight of communication devices, battery life, bandwidth, signal strength, encryption and security, commonality of architecture and software, etc.—all will be overcome by continued development and technical innovation. However, the impact of a network-centric emergency response paradigm on capabilities and procedures, on decision making, and on the behavior of individuals and organizations is difficult to predict.

Given the potentially massive volume of data available in a network-centric environment, the tasks of establishing a common understanding of events and conditions and sorting out facts and situations with the appropriate level of detail to support decision making, may prove exceedingly challenging.

Information inundation

Theoretically, the NCW approach to information sharing should result in pertinent and timely information being provided to the "shooter" when and where he needs it. But experience has proven that when such a massive amount of data is accessible, it becomes nearly impossible to extract what is pertinent from what is peripheral.[7] The result is "information overload," a cascade of data that exceeds the finite limits of information that can be processed and acted upon by a human being in a stressful and complex, multi-tasking environment.

> What is new is the potential for inundating all participants with an ever-increasing flow of data masquerading as information because it has been slickly packaged within the common operating picture . . . creating strong incentives for all to engage in information overload in an attempt to maintain their bearings in this overly ambitious big picture.[8]

In essence, just as a military "shooter" still needs time to shoot, a responder still needs time to do his job. Such an overload of information prevents him from making timely and effective decisions. This is true for the soldier and emergency responder alike.

After-action feedback and lessons learned compiled from US personnel in Iraq and Afghanistan highlight the problem of information overload and its effects upon operational and tactical command nodes during operations. The after-action report from the First Marine Division in Operation Iraqi Freedom stated bluntly that:

> Intelligence sources at all levels were inundated with information and data that had little bearing on their mission and intelligence requirements . . . It seemed that all data, information, and products were being pushed through overburdened communications ports with little thought to who needed what and when they needed it . . . Too much time and bandwidth is wasted by employing the "information inundation" method.[9]

Similar observations and complaints from other units and services were common. The Center for Army Lessons Learned (CALL) noted that:

> At [higher echelons], without the ability to query, the operator had to search reams of information . . . Lower echelons can be quickly overwhelmed with information overflow.[10]

CALL also remarked that in the theater of operations, intelligence analysis personnel were overloaded with information from all sources:

> . . . conducted only minimal analysis on valuable tactical information provided by human intelligence teams because these personnel reported being so overwhelmed by input that they don't have enough time during the day to conduct an analysis.[11]

The above observations are equally applicable to an emergency operations center (EOC) commander who is being bombarded with information of varying quality and usefulness in an attempt to gain situational awareness of an emergency event.

Unfiltered information: Getting the bad with the good

When every information source is treated with equal value, as Metcalfe's Law would imply, the distinction between evaluated, processed information and raw, unverifiable information is lost. The latter can often assume the character of rumor and gossip, making it even more difficult for a commander to discern the actual situation. In practice, Metcalfe's Law has proven overly optimistic regarding the contribution of the individual nodes to the value of the network. Network nodes of similar type and usage history flatten the value equation, and some nodes may actually reduce the overall value of the network because of the addition of undesirable elements. Thus, in a network-centric model, all sources of information are not of equal value and do not contribute equally to overall situational awareness. Some may actually hinder the accuracy of perceptions and the gaining of situational awareness.[12]

This distraction created by peripheral and irrelevant information often has the effect of slowing the decision-making process, as commanders must process large amounts of obfuscating and sometimes contradictory information. There is a natural tendency in such circumstances to wait until additional, clarifying information is obtained before making a crucial and time-sensitive decision.[13] This "paralysis by analysis" is often made worse by the decision-maker's perception that a key item of information is sure to be included in the next influx of data.[14]

Network-centric: At odds with effective command and control

The infusion of information technology into hierarchical organizations typically reduces the traditional asymmetries of information that define superior-subordinate relationships.

Empirically, the "flattening" of command hierarchy regarding information availability and distribution may have some positive effects on overall situational

awareness. However, a paradigm where all entities potentially have access to all available information can create situations that can be counterproductive to the command and control necessary for coordinated management of resources and response to an incident.

The ICS was developed in the late 1970s as a way of organizing the effort to fight wildfires in California that involved thousands of people from hundreds of diverse organizations. The ICS is a highly structured, intentionally hierarchical command and control model for response to natural and manmade incidents of all sizes and severity, including terrorist attacks.[15]

NIMS/ICS acknowledges that, in dealing with a complex and dangerous situation, centralized planning and direction is essential for controlling and coordinating efforts, while decentralized execution is necessary to implement the guidance and tasks in the context of local conditions. No single commander can control the detailed actions of such a large number of people and agencies.[16] The ICS is heavily bureaucratic, formalized, and structured, reliant upon policies and plans, rules, and instructions.[17] But for all its bureaucracy, ICS is designed to allow subordinate organizations to adjust and adapt quickly and easily to deal with changing situations or unforeseen circumstances. The ICS retains the strengths (defined command relationships, efficiency, control) of a bureaucratic hierarchy, enabling preplanning in the more predictable aspects of disaster management, but permits the flexibility to foster and encourage a bias for action and provides leeway for local improvisation to adapt to unforeseen and often volatile conditions.[18]

Excessive control from above

The "flattening" of the hierarchical ICS command and control structure resulting from unregulated information infusion could erode the strength of the ICS's bureaucratic organization, negating advantages commanders have to leverage a wide range of expertise and experience in providing direction to his personnel.

The availability of such a plethora of near real-time information often creates the false impression among commanders that they have as accurate a grasp of current conditions as the responders do at the scene. Such an illusion often leads a commander to micromanage his subordinates, imposing significant restrictions on the initiative of subordinate commanders.[19] Instead of offering guidance and allowing subordinates to use their expertise to adapt to changing conditions, such a commander is prone to issue overly detailed directives often irrelevant or inappropriate to the rapidly evolving situation. The infamous Vietnam War story of President Johnson personally communicating from the White House with army small-unit leaders in the field while they were in contact with the enemy reminds us that simply because a certain type of communication is possible does not mean it's always a good idea. Such a command and control situation in emergency response is sure to stifle initiative and will greatly reduce the effectiveness of subordinate agencies.[20]

Renegade "freelancers" from below

The illusory impression of complete situational awareness can work in the opposite direction as well. Subordinate commanders, viewing what they perceive as virtually the same information as higher-level commanders, might come to radically different conclusions about courses of action. This can result in a lower-level entity ignoring guidance from higher commands. While ICS allows for and encourages improvisation and adaptation to changing conditions, this adjusting must be done within the context of the overall guidance and objectives of the senior EOC or incident command center (ICC).[21] If the lower entity's interpretation of events is at odds with the higher command, there is the risk of "freelancing" by this individual who may ignore the guidance of his superior. "Freelancing" is generally defined as illegitimate improvisation that is not working toward the goals of senior Incident Commanders (ICs).[22] It is deviation from higher intent that is both unpredictable and unexpected, an activity that undermines a unified response effort. At its least damaging, "freelancing" results in a squandering of effort and resources, while at its worst, it can create real dangers to unsuspecting personnel.

Networking for networking's sake

The value of a highly networked ICC or EOC gathering real-time information is immense. So great

is that value that there is a danger that such a command structure will be employed as simply an information conduit rather than for its intended purpose of command and control of response efforts.[23]

Interestingly, some NCW advocates in the US military have already proposed a restructuring of command elements into something radically different from their traditional organizational responsibilities. This reorganization corresponds with the major network-centric tasks that contribute to the commander's "image" (i.e., situational awareness); tasks such as "image maintenance," "image validation," and "image communication"[24] will mean such a command staff will be functioning more as an information conduit rather than in the more traditional command and control function.[25]

In emergency response, when there is often a host of people such as elected officials, media, and higher-level emergency personnel clamoring for the latest information, the temptation is great to think of an EOC or ICC as a super-communications node. It is important to remember that the building of situational awareness, albeit important, is but one task of many for commanders and their staffs and is a secondary task to the overall purpose of command and control of the resources and people in the field.[26]

ADDRESSING CHALLENGES AND LEVERAGING ADVANTAGES OF NETWORK-CENTRIC EMERGENCY RESPONSE

There is much to be gained by taking advantage of the technological developments of the last twenty years regarding data collection and dissemination. Whether a network-centric approach for emergency response will be successful is difficult to say, but current and future technology has the potential to be a significant "force multiplier" for emergency responders, making for a more rapid and efficient decision cycle and a more effective deployment of people and resources to an incident.

The potential pitfalls of network-centric operations, the lessons from Iraq and Afghanistan, and the lessons learned in training exercises should all serve as the starting point for exploring the efficacy of the network-centric model in an emergency response organization.

In order to understand how a network-centric operation can be a boon rather than a bane, it is critical for ICs and other personnel to have a clear idea of their information requirements. They must understand what information is pertinent, what is peripheral, and what is extraneous. They also must determine what agencies are the most reliable sources and how those agencies can provide that information, when it is needed, and in the format required.[27] Though a seemingly simple and commonsense step, identifying those requirements is a highly complex and challenging task.

Determining information requirements

Each type of incident or event has its own characteristics and its own set of critical information requirements. The type of information required by ICs depends on the specific decisions they must make. To this end, information must be presented in a form that caters to decision-making and situational needs.[28] Emergency responders have trained for many years to understand the characteristics of chemical spills, fires, floods, weather events, accidents, etc., and the likely information commanders will need to know about each. Add the complexities of a modern terrorist attack such as an intentional chemical or biological release, radiological contamination, or devastating explosives, and it is obvious that the potential information requirements across a full threat spectrum are voluminous.

In recent years, emergency responders have worked through these likely terrorist scenarios, through a thorough examination of real-world events and training exercises, to study the common characteristics of such events. From this examination, they have defined the basic information an IC needs to begin building situational awareness and validated as much as possible the assumptions about decision making and resource allocation during such incidents. These basic information requirements should be incorporated into standard operating procedures (SOPs) and response plans in which agencies are made well aware of their specific roles and responsibilities.

When developing specific response plans, emergency responders consider the particulars such as terrain,

weather, road networks, population, infrastructure, vulnerable entities (e.g., hospitals, schools), proximity to other potential dangers (fuel or chemical storage, for instance), training level, equipment possessed by local responders, and availability of resources from neighboring communities. These specific conditions and factors weigh heavily in the decision-making process, generating information requirements over and above the basic requirements for that type of incident or event. These additional requirements must also be outlined in the appropriate response plan.

In responding to an event, an IC needs to be disciplined in his information requests, both to keep lower echelons from having to needlessly spend time gathering and reporting information of questionable value and to avoid an inundation of peripheral information to be processed and assimilated.

The use of technology in such complex and dynamic events that allows unfettered communications between any persons or agencies at any time can create a bewildering jumble of information, facts, and rumors that are impossible to digest or sort out. Such a situation is almost certain to obscure rather than enhance an IC's ability to gain situational awareness and exert direction and control over the resources in his jurisdiction.

Training the decision makers and command staffs

The training of decision makers, commanders, and command staffs to operate effectively in environments of urgency and uncertainty, where imperfect information must be evaluated and acted upon, is vital to developing strong leaders who can perform in a crisis. Last year's hurricanes in Louisiana and Mississippi and the subsequent response highlight the need to involve key decision makers in such training.

The concept of realistic and immersive staff drills is hardly a novel one. Wargaming and mission rehearsal have long been a part of the training of the military, public safety agencies, and emergency responders. Not surprisingly, a network-centric approach to emergency response will require extensive rehearsal by IC and EOC staffs. Training, exercises, and experimentation is a must, providing a forum during which new information technology and data management capabilities can be incorporated and tested in realistic and immersive environments. A large amount of training is needed to iron out questions of doctrine, technique, procedures, and best practices for a network-centric approach. What is needed is an innovative and cost-effective method of creating an immersive and powerful training experience for IC staffs and first responders.

User-friendly, realistic, low-cost training

Simulation-based training exercises furnish a low-risk, medium-fidelity environment for both individual and organizational learning. Simulation is critical for the introduction and orientation of new information technology in command and control processes.[29] In various forms, simulation has been a part of training for a variety of disciplines for much of the last century including the military, nuclear power, business, and public safety.

However, few communities have the manpower, financial resources, or exercise design expertise to frequently conduct in-depth and meaningful staff training exercises. Large-scale, high-dollar simulations that require a great degree of technical skill or high-end computer hardware are often beyond the reach of most communities.

The type of simulation required for training local first responders will have a different focus from the first-person, task-oriented pedagogical learning simulation, such as can be found in a virtual classroom.

In order to be a valuable training tool for IC staffs in the development of a network-centric approach to emergency response, a simulation must be able to represent accurately the variety of inputs from the different entities that would provide information in a real-world situation.[30] Unless there is a high degree of real-world fidelity, the simulation exercise will have limited value for decision-making practice and post-event analysis.

Practice, practice, practice

The overarching question of incorporating information technology into a network-centric emergency response is: how can organizations train to integrate technology into process, determine requirements for

that technology, and train individually and collectively in the new processes that encompass the new technology?

Since decision-support systems interact with cognitive and decision-making processes, it is vital to understand the effects of new information technology on the internal function of an organization as well as between different organizations. This highly complex interaction makes discovery and invention a complicated and iterative process. Knowledge discovered in training exercises is invaluable for the development and maturation of systems, the evolution of operational processes and, ultimately, to the successful integration of new technology into the larger command and control decision system.[31]

Organizations must develop basic rules and assumptions for the employment of new technology based on experience and expertise. New technology must be tested and assumptions validated. These results must be used to develop and adapt procedures, and these procedures need to be practiced and rehearsed using real-world response situations and the results analyzed so that these procedures can be further refined and validated.

CONCLUSION

Cutting edge information technology is making its way into the domain of emergency response by virtue of its usefulness and adaptability. A network-centric approach is quickly coming to emergency response and is, to some degree, already present. Its impact upon command and control will be considerable. Emergency responders must be ready for it, understand it to the maximum extent possible, and account for it with mature concepts of employment and best practices developed and validated through realistic training and analysis.

Despite major differences between the US military and the emergency response community, there is considerable common ground regarding methods of command and control in highly complex and dangerous events. The lessons being learned in the use of NCW by our armed forces in Afghanistan and Iraq provide a highly instructive set of lessons for emergency responders as they incorporate the technology and philosophies of a network-centric approach to emergency response.

The challenges of integrating new information technology into an established discipline are significant. Information overload that chokes analysts and decision makers, the flattening of command hierarchies, the subordination of command and control responsibilities to information gathering and connectivity concerns—all are real and serious issues that must be resolved.

Yet, in spite of the negative effects this new technology can have upon command and control if misapplied, the vast potential such technology has for improving capabilities, awareness, and responsiveness make its implementation a virtual certainty.

It will be through extensive training, experimentation, practice, and repetition, with lessons learned properly applied, that assumptions will be validated or found faulty, concepts proven or rejected, and the theoretical molded into the practical—that process alone will yield the best practices, policies, and procedures required for the effective employment of new technology.

If history is a guide, the best practices and procedures that emerge from a true network-centric emergency response paradigm are likely as not to bear little resemblance to what was initially envisioned when the technology that drove that paradigm was developed.

Lt. Col. Mark Stanovich, USMCR, Emergency Readiness and Response Research Center, Institute for Security Technology Studies, Dartmouth College, Hanover, New Hampshire.

REFERENCES

1. Caterinicia D, French M: Network Centric Warfare: Not There Yet. *Federal Computer Week Magazine Online*, 9 June 2003. Available at: *www.fcw.com/fcw/articles/2003/0609*. Accessed August 11, 2005.

2. Gartska JA: Implementation of Network-Centric Warfare. (2004) Available at: *www.oft.osd.mil/library/library_files/trends_338_transformation_trends_28_january_2004_issue.pdf*. Accessed July 27, 2005.

3. Odlyzko A, Tilly B: A Refutation of Metcalfe's Law and a Better Estimate for the Value of Networks and Network Interconnection. (2005) Available at: *www.dtc.umn.edu/~odlyzko/doc/metcalfe/htm*. Accessed July 26, 2005.

4. Cebrowski AK (Adm., USN), Gartska JA: Network-Centric Warfare, Its Origin and Future, USNI Proceedings, January 1998. Available at: *www.usni.org/proceedings/articles98/procebrowski.htm*. Accessed August 11, 2005.

5. Biegley GA, Roberts KH: The Incident Command System: High-Reliability Organizing for Complex and Volatile Task Environments. (2001) *Academy of Management Journal*. January 2001. Available at: *www.apps.aomonline.org/articleretrieval*. Accessed August 2, 2005.

6. Hammes TX (USMC, retired): War Isn't a Rational Business; USNI Proceedings, July 1998. Available at: *www.d-n-i.net/fcs/hammes-netwar.htm*. Accessed August 22, 2005.
7. Vego M: Network-Centric is Not Decisive, USNI Proceedings, January 2003. Available at: *www.usni.org/proceedings/articles03/provego.htm*. Accessed June 27, 2005.
8. Barnett TP: Seven Deadly Sins of Network-Centric Warfare (originally published in *USNI Proceedings*, January 1999, reprinted by Naval War College with author's permission). Available at: *www.nwc.mil/wardept/7deadl~1.htm*. Accessed July 7, 2005.
9. 1st Marine Division Lessons Learned, Operation Iraqi Freedom, United States Marine Corps, August 2003. Available at: *www.globalsecurity.org/military/library/report/2003/imardiv_oif_lessons_learned.doc*. Accessed July 9, 2005.
10. Center For Army Lessons Learned (CALL) Newsletter, October 2003, Number 03-27, United States Army.
11. Ibid.
12. Odlyzko, Tilly, 2005.
13. Vego, 2003.
14. Ferris J: A New American Way of War? C4ISR, Intelligence, and Information Operations in Operation Iraqi Freedom: A Provisional Assessment. *Intelligence and National Security*. Winter 2003, Volume 18, Number 4.
15. Biegley, Roberts, 2001.
16. Department of Defense: Joint Publication 0-2, United Action Armed Forces (UNAAF), Rev July 2001, (DOD Publication No. JP-02) Washington, DC: US Government Printing Office, 2001: V-3.
17. Mendonca S, Pina e Cunha M, Kavo-Oja K, et al.: Wild Cards, Weak Signals, and Organizational Improvisation. (2003) Available at: *www.portal.fe.unl.pt/FEUNL/bibliotecas/BAN/WP-2003.htm*. Accessed August 15, 2005.
18. Ibid.
19. Vego, 2003.
20. Barnett, 1999.
21. Biegley, Roberts, 2001.
22. Mendonca, et al, 2003.
23. Barnett, 1999.
24. Erb SB (LCDR, USN): Network-Centric Warfare: An Operational Perspective. (2004) Joint Military Operations Department, Naval War College.
25. Alberts DS, Hayes RE: Power to the Edge: Command and Control in the Information Age. (2003) Department of Defense Command and Control Research Program (CCRP). Available at: *www.dodccrp.org/events/2005/10th/cd/track02.htm*. Accessed August 2, 2005.
26. Borgu A: The Challenges and Limitations of Network Centric Warfare; The Initial Views of an NCW Skeptic. (2003) Presented at the Network-Centric Warfare Conference, 17 September 2003. Available at: *www.aspi.org.au/pdf/ncw_ab.pdf*. Accessed on 7 July 2005.
27. Kirsch D, Peterson N, Lenert L: An Ontology of Geo-Reasoning to Aid in Medical Response to Attacks With Weapons of Mass Destruction. (2005)
28. Ibid.
29. Ehrhart LS, Bigbee A: *Discovering How to Fight as You Train: Evolving C2 Organizations and Information Technology Through Training*. (1999) MITRE Publications, March 99, Vol. 3 No. 1. Available at: *www.mitre.org/news/the_edge/march_99*. Accessed August 6, 2005.
30. Pizzo C, Powell G, Brown III CF: *Modeling and Simulation Support for Answering Commanders' Priority Information Requirements*. (2005) US Army Research and Development Command, CERDEC I2WD, Ft Monmouth, NJ. Available at: *www.dodccrp.org/events/2005/10th/cd/track02.htm*. Accessed August 11, 2005.
31. Erhart, Bigbee, 1999.