"Network-Centric" Emergency Response: The Challenges of Training for a New Command and Control Paradigm

LtCol Mark Stanovich, USMCR
Emergency Readiness and Response Research Center
Institute for Security Technology Studies
Dartmouth College
45 Lyme Road, Hanover, NH 03755
mstanovich@ists.dartmouth.edu

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 leveraged in 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 technical 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 warfighting. Emergency Operations Centers, Incident Command Centers, 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 staffs and personnel in the assimilation of the new technology.

Introduction

The first real tests of the concept of Network Centric Warfare 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 USN, and John J. Garstka, posited the concept of Network Centric Warfare. Expounding upon developments in business models that have applied new information technology, and considered the next great "revolution in military affairs" (RMA), Network Centric Warfare 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

[1] Cateriniccia, Dan, & French, Matthew, (2003) Network Centric Warfare: Not There Yet, *Federal Computer Week Magazine Online*, 9 June 2003 Available at: www.fcw.com/fcw/articles/2003/0609 Retrieved on 11 August 2005

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

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 what was possible with past capabilities.
This superior situational awareness is referred to often as "information superiority", designed to achieve a faster decision-making cycle in relation to the enemy. NCW, essentially, 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 in culture, mission, training, and jurisdictional authority, and there is a uniqueness of skill sets and of 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 Network Centric Warfare 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 NIMS/ICS system, currently being implemented by DHS, closely resembles a military C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance)[5] hierarchy. Function and organization of both NIMS/ICS and C4ISR are designed to most efficiently and effectively allow for command and control of large, complex, and dangerous events and situations.

The myriad developments of sensors and collection assets are in many

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

[4] Cebrowski, Adm Arthur K.USN, and Gartska, John A., (1998), Network-Centric Warfare, Its Origin and Future,
USNI Proceedings, January 1998
Available at:
www.usni.org/proceedings/articles98/procebrowski.htm Accessed on 11 August 2005

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

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 operations in Afghanistan and Iraq provide the first "live-fire" critiques of Network-Centric Warfare. The challenges and difficulties faced by the Defense Department in putting the NCW concept into practice ought to prove highly instructive for the emergency responder 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, et cetera, 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 will be difficult to predict.

Given the potentially massive volume of data and information available, 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 in a "network-centric" environment.

- **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[6]. 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[7].

In essence, just as a military "shooter" still needs time to shoot, a responder

[6] Vego, Dr. Milan, (2003), Network-Centric is Not Decisive, *USNI Proceedings, January 2003*, Available at: www.usni.org/proceedings/articles03/provego.htm Accessed on 27 June 2005

[7] Barnett, Dr. Thomas P. (1999), 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 on 7 July 2005

still needs time to do his job. Such an overload of information prevents him from making timely and effective decisions. This is true for warfighter and emergency responder alike.

After-action feedback and Lessons Learned compiled from Iraq and Afghanistan highlight the problem of information overload and its effects upon operational and tactical command nodes in the conduct of operations.

The After-Action Report from the 1st 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.[8]

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", and that "Lower echelons can be quickly overwhelmed with information overflow"[9].

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

> …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"[10].

The above observations are equally applicable to an Incident Commander or EOC Commander who is being bombarded with information of varying quality and usefulness in an attempt to gain situational awareness as his/her command responds to an incident or disaster.

- **Unfiltered Information: Getting the Bad with the Good**

When every information source is treated as a collection asset of equal value, as Metcalfe's Theory would imply, the distinction between evaluated and processed intelligence, 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 significantly over-optimistic regarding the contribution of nodes to the value of the network.

[8] 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 on 9 July 2005

[9] Center For Army Lessons Learned (CALL) Newsletter, October 2003 Number 03-27, United States Army.

[10] Ibid.

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 adding of undesirable elements. Thus, in a "network-centric" concept, all sources of information are not of equal value, and do not contribute equally to overall situational awareness. Some may actually serve to hinder the accuracy of perceptions and the gaining of situational awareness[11].

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[12]. 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 massive influx of data[13].

- **"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 Incident Command System was developed in the late 1970s as a way of organizing the fight against wildfires in CA that involved thousands of people from hundreds of diverse organizations. The ICS is a structured, intentionally heirarchical command and control model for response to natural and manmade incidents of all sizes and severity, including terrorist attacks[14].

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[15]. The ICS is heavily beaurocratic, formalized and structured, reliant upon policies and plans, rules and instructions.[16] But for all its beaurocracy, ICS is designed to allow subordinate organizations to adjust and

[11] Odlyzko, Andrew, & Tilly, Benjamin, (2005)

[12] Vego, (2003)

[13] Ferris, John, (2003), 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*

[14] Biegley & Roberts, (2001)

[15] Department of Defense, (2001) *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

[16] Mendonca, Sandro, Pina e Cunha, Miguel, Kavo-Oja, Kari, and Ruff, Frank; (2003) *Wild Cards, Weak Signals, and Organizational Improvisation*
Available at:
www.portal.fe.unl.pt/FEUNL/bibliotecas/BAN/WP-2003.htm Accessed on 15 August 2005

adapt quickly and easily to deal with changing situations or unforeseen events and circumstances. The ICS retains the strengths (defined command relationships, efficiency, control) of a beaurocratic hierarchy, enabling pre-planning 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[17].

- **Excessive Control From Above**

The "flattening" of the hierarchical ICS command and control structure resulting from unregulated information infusion could erode the strengths of the Incident Command System's beaurocratic organization, negating advantages that allow for commanders to leverage a wide range of expertise and experience to provide direction to the efforts of the responders.

The availability of such a plethora of near-real time information often creates the false impression among commanders that they have as solid and accurate a grasp of conditions and situational awareness as the local responders dealing with an incident at the scene. The result of such an illusion often leads a commander to be over-controlling with his subordinates, imposing significant restrictions on the initiative of subordinate commanders[18]. Instead of issuing guidance and allowing his subordinates to leverage their expertise to accomplish their tasks and adapt to changing conditions within that guidance, such a commander is prone to issue overly-detailed directives that are irrelevant or inappropriate for the rapidly-evolving local situation. The infamous Vietnam War parable 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 communications are possible, that does not mean they are 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 the efforts of subordinate agencies[19].

- **Renegade "Freelancers" From Below**

An illusory impression of situational awareness can work to the opposite direction, as well. Subordinate commanders, viewing what they perceive as virtually the same information as higher-level commands are seeing, 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 handle changing situations and conditions, this adjusting must be done within the context of the overall guidance and objectives of the senior Emergency Operations Center (EOC) or Incident Command Center (ICC)[20]. If the lower entity's interpretation of events is at odds with that of the higher command, then the risk is of "freelancing" by people acting on their own interpretation (and consequently ignoring the guidance from higher). "Freelancing" is generally defined as illegitimate improvisation that is not working toward the goals of senior

[17] Ibid.
[18] Vego, (2003)
[19] Barnett, (1999)
[20] Biegley & Roberts, (2001)

Incident Commanders[21]. It is deviation from higher intent that is both unpredictable and unexpected, and such activity presents serious problems to a unified response effort. At its least damaging, freelancing results in a squandering of effort and resources best used differently, while at its worst, it may create dangers for those who are freelancing and for others involved in the response effort whose actions and safety will be impacted.

- **Networking for Networking's Sake**

The value of an extensively-networked ICC or EOC as a means of 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 an information conduit rather than for its intended purpose of command and control of response efforts[22].

Interestingly, some NCW advocates in the US Military already have proposed a restructuring of command elements into something radically different from their traditional organization and functional responsibilities. This reorganization to correspond to the major "network centric" tasks that contribute to the commander's "image" (read: situational awareness); tasks such as "image maintenance", "image validation", and "image communication"[23] will mean such a command staff will be functioning more as an information conduit rather than in the more traditional command and control responsibilities[24].

In emergency response, with a host of people such as elected officials, media outlets, and higher-level emergency commands clamoring for the latest information, the temptation is great to think of an EOC or ICC as a super-communications node. Establishing network connectivity may become an end unto itself, rather than a means to the end for enhancing command and control capabilities. However, 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 supporting task to the overall purpose of command and control of the resources and people in the field who are dealing with the consequences of critical incidents[25].

Addressing Challenges and Leveraging Advantages of "Network Centric" Emergency Response

It is certain that there is much to be gained by taking advantage of the technological developments of the last twenty years regarding the collection

[21] Mendonca, et al, (2003)

[22] Barnett, (1999)

[23] Erb, LCDR Stephen B. USN, (2004) *Network-Centric Warfare: An Operational Perspective.* Joint Military Operations Department, Naval War College

[24] Alberts, David S. & Hayes, Richard E., (2003) *Power to the Edge: Command and Control in the Information Age*, Department of Defense Command and Control Research Program (CCRP)
Available at:
www.dodccrp.org/events/2005/10th/cd/track02.htm
Accessed on 2 August 2005

[25] Borgu, Aldo, (2003), *The Challenges and Limitations of Network Centric Warfare; The Initial Views of an NCW Skeptic*. Presented at the Network-Centric Warfare Conference, 17 September 2003.
Available at:
www.aspi.org.au/pdf/ncw_ab.pdf
Retrieved on 7 July 2005

and dissemination of large amounts of information. Whether this truly evolves into a successful "network-centric" approach to emergency response is difficult to say, but the technology now available and being developed 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 employment of the people and resources available to respond to any incident.

The potential pitfalls of network-centric operations, and the lessons from Iraq and Afghanistan, as well as those learned in training and exercises, should be the starting point for exploring the impact and consequences of applying information technology to command and control of emergency response organizations.

In order to understand how the availability of such massive quantities of information can be a boon rather than a bane, it is critical for Incident Commanders and other emergency responders 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[26]. Though a seemingly simple and common-sense 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 incident commanders depends on the specific decision they must make. To this end, information must be presented in a form that fits decision-making and situational needs[27]. 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 apparent that the potential information requirements across a full threat spectrum are voluminous.

In recent years, emergency responders have worked through these likely terrorist scenarios, using thorough examination of real-world events and training exercises, to study the common characteristics of such events. From this examination, they define the "basic" information that an Incident Commander needs to begin building situational awareness, and validate 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 should be well aware of their roles and responsibilities.

[26] Kirsch, Dr David, MD, & Peterson, Dr Nicole, MD, & Lenert, Dr Leslie, MD, (2005) *An Ontology of Geo-Reasoning to Aid in Medical Response to Attacks With Weapons of Mass Destruction*

[27] Ibid.

When developing specific response plans, emergency responders consider the particulars of such things as terrain, weather, road networks, population, infrastructure, vulnerable entities (such as hospitals or 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 decision-making processes, generating information requirements in addition to the "basic" requirements for an incident or event. These additional requirements also must be outlined in the appropriate response plan.

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

The injecting into such complex and dynamic events of technology 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 even sort out. Such a situation is almost certain to obscure rather than enhance an Incident Commander or EOC Commander'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 in environments of urgency and uncertainty, where imperfect information must be evaluated and acted upon, is vital to building experience and competence and developing effective leaders who can perform in a crisis. Recent events involving the Gulf Region hurricanes 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 Incident Commanders and EOC staffs. Training, exercise 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 substantially 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 valuable training experience for Incident Command 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 Incident Command staffs in the development of a network-centric approach to emergency response, a simulation must be able to represent accurately the inputs from the various entities that would provide information in a real-world situation[28]. The representations need the amount of fidelity required to be effective stimuli for valuable 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 understanding the effects of new information technology on the internal function of staffs and between staff organizations. This highly complex interaction makes discovery and invention a complicated and iterative process. Knowledge discovered in training and educational exercises is invaluable to 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 (C2) decision system[29].

Organizations must develop basic rules and assumptions for the employment of new technology and capabilities, based on experience and expertise. New technology must be tested and assumptions validated, procedures created or modified to most effectively employ that technology. These results must be used to develop and adapt procedures. These procedures need to be practiced and rehearsed using real-world response plans and situations, and the results analyzed so that

[28] Pizzo, Christian, & Powell, Gerald, PhD, & Brown III, Chester F., & May, Jaqueline; (2005) *Modeling and Simulation Support for Answering Commanders' Priority Information Requirements*. US Army Research and Development Command, CERDEC I2WD, Ft Monmouth, NJ.
Available at:
www.dodccrp.org/events/2005/10th/cd/track02.htm
Accessed on 11 August 2005

[29] Erhart & Bigbee, (1999)

procedures can be further refined and validated.

Conclusion

Revolutionary information technology is making its way into the domain of emergency response, by virtue of its usefulness and adaptability. A "network-centric" approach to emergency response is coming to a greater or lesser degree, and in fact is already here. Its impact upon command and control will be considerable. Emergency responders must be ready for that impact, understand it to the maximum extent possible, and account for it with mature concepts of employment and best practices that were developed and validated during realistic training and analysis.

Despite major differences between the US Military and emergency responders, there is considerable common ground regarding methods of command and control in highly complex and dangerous events. The lessons being learned in the adaptation of Network Centric Warfare by our Armed Forces in Afghanistan and Iraq provide a highly instructive set of lessons to emergency responders as they incorporate the technology and philosophies of a "network-centric" approach to emergency response.

The challenges of integrating new information technology and its unforeseen consequences 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.

References

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

2. Cebrowski, Adm Arthur K.USN, and Gartska, John A., (1998), Network-Centric Warfare, Its Origin and Future,
   USNI Proceedings, January 1998
   Available at:
   www.usni.org/proceedings/articles98/procebrowski.htm
   Accessed on 11 August 2005

3. Mendonca, Sandro, Pina e Cunha, Miguel, Kavo-Oja, Kari, and Ruff, Frank; (2003) *Wild Cards, Weak Signals, and Organizational Improvisation*
   Available at:
   www.portal.fe.unl.pt/FEUNL/bibliotecas/BAN/WP-2003.htm
   Accessed on 15 August 2005

4. Vego, Dr. Milan, (2003), Network-Centric is Not Decisive,
   USNI Proceedings, January 2003,
   Available at:
   www.usni.org/proceedings/articles03/provego.htm
   Accessed on 27 June 2005

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

6. Alberts, David S. & Hayes, Richard E., (2003) *Power to the Edge: Command and Control in the Information Age*, Department of Defense Command and Control Research Program (CCRP)
   Available at:
   www.dodccrp.org/events/2005/10th/cd/track02.htm
   Accessed on 2 August 2005

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

8. 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 on 9 July 2005

9. Center For Army Lessons Learned (CALL) Newsletter, October 2003 Number 03-27, United States Army.

10. Ferris, John, (2003), 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*

11. Barnett, Dr. Thomas P. (1999), 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 on 7 July 2005

12. Department of Defense, (2001) *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

13. Borgu, Aldo, (2003), *The Challenges and Limitations of Network Centric Warfare; The Initial Views of an NCW Skeptic*. Presented at the Network-Centric Warfare Conference, 17 September 2003.
Available at:
www.aspi.org.au/pdf/ncw_ab.pdf
Retrieved on 7 July 2005

14. Erb, LCDR Stephen B. USN, (2004) *Network-Centric Warfare: An Operational Perspective.* Joint Military Operations Department, Naval War College

15. Ehrhart, Lee Scott, & Bigbee, Anthony, (1999) *Discovering How to Fight as You Train: Evolving C2 Organizations and Information Technology Through Training*, MITRE Publications, March 1999, Vol. 3 No. 1
Available at:
www.mitre.org/news/the_edge/march_99
Accessed on 6 August 2005

16. Kirsch, Dr David, MD, & Peterson, Dr Nicole, MD, & Lenert, Dr Leslie, MD, (2005) *An Ontology of Geo-Reasoning to Aid in Medical Response to Attacks With Weapons of Mass Destruction*

17. Pizzo, Christian, & Powell, Gerald, PhD, & Brown III, Chester F., & May, Jaqueline; (2005) *Modeling and Simulation Support for Answering Commanders' Priority Information Requirements*. US Army Research and Development Command, CERDEC I2WD, Ft Monmouth, NJ.
    Available at:
    www.dodccrp.org/events/2005/10th/cd/track02.htm
    Accessed on 11 August 2005

18. Cateriniccia, Dan, & French, Matthew, (2003) Network Centric Warfare: Not There Yet, *Federal Computer Week Magazine Online*, 9 June 2003
    Available at:
    www.fcw.com/fcw/articles/2003/0609
    Retrieved on 11 August 2005

19. Hammes, Col T. X.,USMC (Ret'd) (1998) War Isn't a Rational Business; *USNI Proceedings*, July 1998
    Available at:
    www.d-n-i.net/fcs/hammes-netwar.htm
    Accessed on 22 August 2005