Strategy Research Project

9/11 Ten Years After: Command, Control, Communications Remain an Issue

by

Lieutenant Colonel Brian A. Barthel
United States Air Force

United States Army War College
Class of 2012

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
09/02/2012	Strategy Research Project	

4. TITLE AND SUBTITLE
9/11 Ten Years After: Command, Control, Communications Remain an Issue

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Brian A. Barthel

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Colonel Charles W. Patnaude
Department of Defense Enterprise Management

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Approved for public release distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This research paper reviews current emergency management capability to respond to significant incidents, both natural and manmade. In such incidents, multiple agencies must respond, manage forces, and provide critical support as a cohesive team. These organizations span the gamut of local, tribal, state, and federal levels of government and of the private sector. They include the broad range of first responders, fire, medical, and police. The unity of effort needed to provide timely, efficient, and integrated responses can only be achieved through effective command, control, and communication within and among responding forces. A unified response requires interoperable communications among all agencies, at all levels. Responders need a mechanism to track all responding forces. All responders must share a common operating picture that fuses and displays disparate data. This paper reviews current national policies, procedures, and technologies for managing large-scale emergencies. It identifies challenges and opportunities for improvement. It concludes with recommendations for implementing a nationwide interoperable communications system which will facilitate formulation of a common operating picture for first responders.

15. SUBJECT TERMS
Interoperability, Common Operating Picture, Response Force Tracking, Homeland Security

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	32	

USAWC STRATEGY RESEARCH PROJECT

9/11 TEN YEARS AFTER: COMMAND, CONTROL, COMMUNICATIONS REMAIN AN ISSUE

by

Lieutenant Colonel Brian A. Barthel
United States Air Force

Colonel Charles W. Patnaude
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel Brian A. Barthel

TITLE: 9/11 Ten Years After: Command, Control, Communications Remain an Issue

FORMAT: Strategy Research Project

DATE: 9 February 2012 WORD COUNT: 5477 PAGES: 32

KEY TERMS: Interoperability, Common Operating Picture, Response Force Tracking, Homeland Security

CLASSIFICATION: Unclassified

This research paper reviews current emergency management capability to respond to significant incidents, both natural and manmade. In such incidents, multiple agencies must respond, manage forces, and provide critical support as a cohesive team. These organizations span the gamut of local, tribal, state, and federal levels of government and of the private sector. They include the broad range of first responders, fire, medical, and police. The unity of effort needed to provide timely, efficient, and integrated responses can only be achieved through effective command, control, and communication within and among responding forces. A unified response requires interoperable communications among all agencies, at all levels. Responders need a mechanism to track all responding forces. All responders must share a common operating picture that fuses and displays disparate data. This paper reviews current national policies, procedures, and technologies for managing large-scale emergencies. It identifies challenges and opportunities for improvement. It concludes with recommendations for implementing a nationwide interoperable communications system which will facilitate formulation of a common operating picture for first responders.

9/11 TEN YEARS AFTER: COMMAND, CONTROL, COMMUNICATIONS REMAIN AN ISSUE

> One of the most critical things in a major operation like this [response to 9/11 attacks on NYC's Twin Towers] is to have information. We didn't receive any reports of what was seen from the [NYPD] helicopters. It was impossible to know how much damage was done on the upper floors, whether the stairwells were intact or not.[1]
>
> — Fire Chief
> New York City Fire Department

The 9/11 terrorist attacks were a watershed event for the United States of America. They opened the nation's eyes, bringing the realization that this powerful nation is not immune to asymmetric attacks from non-state actors. They also painfully revealed the need to improve homeland security, specifically response efforts. The magnitude of these attacks required responses from all levels of government, local, state, and federal, as well as private and non-governmental support. The devastating problems arising in these responses brought to light significant command, control, and communication (C3) shortfalls, not only among responding organizations, but also within them and across all levels.

The 2010 National Security Strategy (NSS) cites the security of the United States and its citizens as an enduring national interest.[2] It further stipulates the requirement to strengthen security and resilience at home to counter the full range of threats, from natural disasters to terrorist attacks. The primary NSS goal is to prevent these dangers. However, if deterrence fails, national security requires effective rapid response and recovery operations.[3] To meet this challenge, the United States must integrate its all-hazard planning through collaboration at all levels of government and with the private

sector. To assure such collaboration the nation must invest in a reliable, interoperable, survivable communications system for first responders.[4]

This paper reviews the nation's current capabilities to respond to significant incidents, both natural and manmade. To respond effectively, multiple agencies (from local, state, federal government to the private sector) must manage their collective assets and provide critical support as a cohesive team. They include the broad range of first responders, fire, medical, and police. The unity of effort needed to provide timely, efficient, and integrated responses can only be achieved through effective C3 within and among responding forces. To effectively support the 2010 NSS, responders need interoperable communications among all agencies, a mechanism to track personnel, and share a common operating picture (COP). This paper reviews current national policies, procedures, and technologies for responding to national emergencies. It identifies challenges and opportunities for improvement. It concludes with recommendations for implementing a nationwide interoperable communications system that, along with an effective tracking system, will facilitate the formulation of a COP for first responders.

Background

The events of 9/11 were surely eye-opening. But this was not the first event, manmade or natural, to reveal the need for better integration of first responders. The December 1993 terrorist bombing of the World Trade Center (WTC) revealed significant C3 issues. Responding forces were dispatched by different control centers and were not operating on the same radio frequencies, so they could not communicate with one another.[5] Even when leaders of different responders were collocated, they often used different terminology. For example, "fire" could mean a blaze or a gunshot. Lastly, as

experienced during 9/11, communication was lost with responding forces inside the WTC; radios could not penetrate the numerous steel and concrete floors; and too many units using the same point-to-point channel rendered communications ineffective.[6] These issues impeded emergency agencies from rapidly and comprehensively responding to the incident and from effectively performing their primary mission to protect the public.

As a result of the 1993 WTC bombing, NY/NJ Port Authority (responsible agency for the WTC) invested $100M to make physical, technological, and structural improvements, and to improve fire safety plans and procedures.[7] They upgraded the facilities emergency power, installed redundant alarms, posted a 24/7 alarm monitor, and established a fire warden program, among other upgrades.[8] Despite these improvements, the 9/11 attacks clearly reveal that much work still needed to be done regarding first responder C3 capabilities.

Since 9/11, a number of statutes, strategies and directives have been enacted to provide specific legal authority for both cross-sector and sector-specific protection and guidance. These directives have been crafted to the NSS mandate to protect the homeland of the United States. The 2002 Homeland Security Act established a cabinet level department headed by a cabinet Secretary of Homeland Security with the mandate and legal authority to protect the American people from terrorist threats.[9] Congress has assigned the Department of Homeland Security (DHS) the primary mission of minimizing damage and assisting in the recovery from terrorist attacks.[10] This Act further directs DHS to develop a comprehensive national plan for securing the nation's

critical infrastructure and key resources. One of these cited key resources is an emergency preparedness *communication* system.

Similarly, the Robert T. Stafford Disaster Relief and Emergency Assistance Act provides detailed authority for response to emergencies and major disasters.[11] The federal government is granted specific authority to provide assistance to state and local entities for disaster preparation and for emergency assistance to mitigate the damage of major disasters.[12] This assistance includes, among other things, resources and such services as emergency *communications*, emergency transport, and assistance in fighting fires.

Additionally, there are two Homeland Security Presidential Directives (HSPD) which address preparedness and response. HSPD 5, Management of Domestic Incidents, and HSPD eight, National Preparedness, establish a national approach to managing domestic incidents that ensures effective coordination among all levels of government and among government and non-government and private agencies.[13] They empower the Secretary of Homeland Security to coordinate federal resources used for prevention, preparedness, response, and recovery from terrorist attacks, major disasters, or other large-scale emergencies.[14] They further mandate development of emergency preparedness training, planning, equipment, and exercises.[15] Finally, they direct all involved parties to adhere to the same standards.

These legislative acts and presidential directives have led to the implementation of various DHS planning documents. Several seminal documents pertain to response planning and execution: the National Infrastructure Protection Plan (NIPP), the National Incident Management System (NIMS), the National Response Framework (NRF), the

National Emergency Communications Plan (NECP), and the Emergency Services Sector Specific Plan (SSP).

The NIPP provides a unified structure for integration and unity of effort at the national level. Its primary goal is to "build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating terrorists' attempts to destroy or incapacitate our nation's critical infrastructure and key resources (CIKR)."[16] Additionally, it aims to "strengthen national preparedness, timely responses, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency."[17] The DHS has designated emergency services as a key resource sector.

The NIMS is the national template designed to enable federal, state, local, tribal, private, and non-government agencies to work together efficiently to prevent, protect, respond, and recover from incidents.[18] It provides the doctrine for command, control, and incident management across all agencies, levels, and disciplines. It also provides the concepts, principles, terminology, and processes for collaborative incident management – *common operating picture*, *interoperable communications*, and information management.[19] The NRF builds on the NIMS and provides the "structure for implementing a nationwide response policy and for operational coordination of responses to all types of domestic incidents."[20]

The NECP is designed to "ensure operability, interoperability, and continuity of communications."[21] Its goal is to establish nationwide *interoperable* emergency communications.[22] Additionally, this plan seeks to develop a COP that will enhance responders' situational awareness and provide timely and consistent information during a crisis.[23]

Lastly, the Emergency Services SSP sets prioritized goals and objectives which support the overarching goal of the NIPP. It is designed to protect, among other things, personnel from both operational risk and risk from attackers, and to ensure timely, coordinated all-hazards emergency response.[24] This sector is comprised of law enforcement, fire and emergency services, emergency medical assistance, emergency management, and public works and constitutes the nation's first line of defense against a concerted terrorist attack.

Analysis

These policies, directives, and plans have substantially improved the nation's emergency response capabilities. Specifically, they provide the basic framework for agencies at all levels of government, for non-government assets, and for the private sector across all disciplines to share a common foundation for coordinating, planning, and responding to national emergencies. Collectively, they now share a common terminology for first responder communications; they clearly articulate goals; and they pursue specific objectives to meet those goals – interoperable communications, COP, etc. They also now have an incident command structure and know who is in charge based on the nature of the situation.

However, these documents, do not yet assure optimal and integrated responses. Federal policies and guidance are just that, guidance. As a result of our federalist system, the federal government lacks the authority to direct necessary measures to ensure effective response to major incidents. Response is an inherent function and responsibility of each state; effective responses require close coordination with private and non-profit entities to provide goods, services, and research and development.[25]

Improvements come only when local and state governments, in collaboration with the private sector, voluntarily comply with the federal guidance.

DHS has taken further measures to improve communication capabilities. For example, the National Communications System provides a number of communication services for qualifying federal, state, local, and non-profit agencies that provide emergency services. The Government Emergency Telecommunications Service (GETS) provides emergency priority and access to segments of the public switch wireline network, using a special dialing plan and unique personal identification number.[26] GETS is designed to make maximum use of available communication lines. Similarly, Wireless Priority Service (WPS) provides access and priority to cellular networks over non WPS subscribers.[27] To improve the probability of successfully completing a call during an emergency, DHS recommends using WPS in conjunction with GETS. But this is not an ideal situation: Telecommunication providers are not required to offer this service and do not guarantee call completion.[28] Additionally, access to the service requires WPS-enabled cell phones, and users are charged a fee on a pay-as-you-go basis.[29]

Statewide Communications Interoperability Plans (SCIP) represent significant progress. With the assistance of the DHS Office of Emergency Communications, all states and territories have drafted department-approved plans.[30] These plans specify how states will communicate within the state across agencies, disciplines, and jurisdictions, as well as with other states and federal agencies. They provide a mechanism and process for communicating with disparate agencies, but not the means. So they do not assure genuine interoperability.

Lastly, federal grant programs have helped improve communications capabilities across the emergency services sector. The Federal Emergency Management Agency (FEMA) administers the interoperable emergency communications grant program. This program provides states, territories, and local governments with funds for governance, planning, training, and exercises to achieve interoperable communications.[31] In fiscal year 2009 and again in 2010, the federal government distributed $48M each year in support of SCIP.[32]

Despite the great strides made in policy and funding to improve communications and increase situational awareness among and across state and federal jurisdictions, more needs to be done. America still does not have, but needs, a nationwide interoperable communications system, an effective way to track responding personnel and assets, and a coherent mechanism to capture all relevant data into a shared COP.

Interoperable Communications

First and foremost, an effective C3 system begins with interoperable communications. This is the backbone for the other elements, enabling a response force tracking capability and a COP. The NIMS defines interoperable communications as the ability of emergency response personnel to communicate within and across agencies and jurisdictions by voice, data, and video.[33] Today, in most locales, communications rely on a number of archaic methods; swapping radios, radio/phone patches, use of liaisons, information relayed by dispatchers/control centers, shared channels, or trunked systems.[34] All of these methods fall short of providing effective interoperable communications.

As previously stated, many cornerstone homeland security documents, and real world events have revealed the need and requirement for interoperable

communications. For example, the NECP purports that emergency response agencies require interoperable and seamless communications to manage response, to control response partners, and to maintain a common operating picture.[35] But the lack of interoperable wireless communication among first responders diminishes this capability. The 9/11 Commission recommended dedicating a portion of radio spectrum to create a coast-to-coast, interoperable digital emergency communications network.[36] Accordingly, Homeland Security Act 2002 and Homeland Security Appropriation Act 2007 legislates the creation of a nationwide emergency communications capability.

This legislation is being implemented by means of the NECP, the NIMS, and various emergency management working groups. However, Congress has yet to resolve issues of frequency spectrum allocation and licensing. Nor has it appropriated sufficient funds to build a Public Safety Broadband Network (PSBN). Finally, Congress has not addressed governance concerns of both the public safety and commercial sectors, nor have they granted PSBN the D Block radio frequency spectrum.[37] This frequency band is contiguous to existing PSBN spectrum and is needed to meet emergency responders' day-to-day communications needs.[38] The 2005 Deficit Reduction Act stipulates that this frequency band will be auctioned to the highest bidder.[39] Congress must amend this Act to assure that PSBN has an adequate radio frequency spectrum. Likewise, Congress must allocate sufficient funds for construction of this system, which is estimated in the tens of billions of dollars.[40]

Currently three primary options are being discussed. The first option is to continue to advocate for local stakeholders to find their own solutions within the construct established by the DHS. This option assumes that stakeholders have the

greatest understanding of their particular issues and concerns, so they are in the best position to decide what is needed. Under this option, the system will develop incrementally along a continuum established by an agency designated in the NECP.[41] While this approach offers benefits to the local community, history reveals two significant drawbacks in this bottom-up approach. First, these systems are generally proprietary, tailored to the local market; therefore, they are not interoperable across jurisdictions or regions. Second, it is costly to purchase, install, operate and maintain them. In the past nine years, the federal government has expended $13B on emergency communications, and the estimated cost to upgrade existing equipment is another $18B.[42] But these upgrades do not guarantee interoperability. This option exposes both the general public and first responders to increased and unnecessary risk.

The second option is to build a dedicated, nationwide, interoperable wireless network for public safety. To fully reach this goal, 10MHz of spectrum from the D Block must be reallocated to the PSBN to assure public safety.[43] This will provide first responders with twice the current spectrum and twice the capability for current and evolving communications requirements; data, voice, and video.[44] Additionally, the system will provide 4G technology, which is 10 times faster than the current high-speed wireless services. It will also provide wider service to 98% of the population.[45] Lastly, it provides priority access to a self-governed dedicated system to meet both day-to-day operational needs and to respond to large-scale contingencies. There are, however, two major concerns with this proposal: First, Congress must amend current legislation that requires auctioning off the D Block frequency spectrum. Second, the Federal Communications Commission (FCC) estimates this network's initial cost to be

approximately $15.7B.[46] Finally, to build and operate this system over the next 10 years will cost approximately $34-47B.[47]

The third option is to develop a public-private partnership between public safety agencies and wireless carriers; these partners will share joint responsibility for decision-making. This partnership will build a nationwide network that meets the express needs of first responders for robust interoperable communications. Theoretically, this shared infrastructure and capability will provide economies of scale, new sources of funding, continuous technological improvements, and access to additional spectrum during large scale incidents.[48] There are significant concerns about this option. Public safety proponents fear they will have insufficient influence over access and operations of the system. Specifically, they would have to compete with the private sector during incidents for more bandwidth (an issue during 9/11 and Hurricane Katrina). They fear that commercial carriers will not be willing to push paying customers off the network at critical times. Additionally, during major crises like 9/11, public networks were overwhelmed and rendered virtually ineffective. Furthermore, the proposed network would provide only video and data capabilities. It does not address the requirement for voice, which is the first responders' most needed capability. Lastly, the FCC estimates this system will cost approximately $12-16B, while the public estimate is $18-40B.[49]

First responders must be able to effectively communicate across disciplines and jurisdictional lines and to swiftly respond to and resolve issues. Without this capability, the public's safety and the lives of first responders and of all U.S. citizens remain at risk. No matter which of the above options is chosen, our national leaders must commit to

providing an effective system of interoperable communications for our responders to national emergencies.

Response Force Tracking

The second area requiring attention is a means to track personnel and resources. The ability to effectively communicate during a crisis is crucial; however, the ability to track the location of first responders is equally important. The NIMS identifies accountability of resources as essential during incident response operations.[50] Furthermore it cites the need for unity of command, for personnel accountability, and tracking resources. The lack of effective tracking of equipment and especially personnel, during 9/11 impaired C3 response capabilities. During the initial 9/11 response, the Fire Chief lost radio communications with fire fighters inside each tower.[51] This greatly inhibited his ability to command the situation and his ability to effectively allocate additional resources. If tracking devices had been available, the fire chief would have known what floor his personnel were on. And he would have had a fairly good idea how the evacuation was proceeding. Tragically, many fire fighters died on 9/11 because they never got the word, via radio or mouth, to evacuate the building. Armed with tracking technology, runners could have pinpointed first responders' locations and verbally ordered units to evacuate. Unfortunately, the methods for tracking personnel have not changed much since 9/11. Agencies still rely on listening to land mobile radio communication, radio status checks, and plotting boards.

But effective and proven tracking technology now exists. Over the past 10 years, the U.S. military has conducted extensive research, development, and tests on tracking devices, and has fielded "Blue Force Tracking" (BFT). This system uses a global positioning system (GPS) beaconing instrument that provides point-to-point, peer-to-

peer and/or point-to-command center tracking.[52] The system provides position location, an identification function, a transceiver, a communications network, and a user interface.[53] It provides near real-time information that transmits the exact location of personnel, vehicles, and assets.[54] This information is displayed on a portable or fixed monitor that depicts friendly forces on an easy-to-read digitized geospatial map. The number of assets being tracked directly determines how much bandwidth is required. This is why emergency management needs a dedicated nationwide wireless network that includes the additional 10 MHz of spectrum.

BFT has been used extensively in Iraq and Afghanistan; it has proven effective in both rural and urban terrain. When BFT is properly integrated with other data feeds, it provides enhanced situational awareness and a COP that optimizes command and control (C2). This system can be adapted for civilian use to track critical equipment, key assets, and responding forces.

This technology has proliferated to the private sector. Wireless providers, Verizon, AT&T, and Sprint, offer applications that can track the precise location of individual cell phones. Additionally, New York City emergency management agencies are acutely aware of the benefits of this technology and have begun outfitting all their fire trucks and ambulances with GPS tracking devices.[55] It enables them to instantly dispatch the nearest unit to an incident scene: reducing response time means more lives saved.

To track their personnel, the New York City Fire Department (FDNY) is in the process of fielding the Electronic Fireground Accountability System (EFAS). This system, like BFT, uses GPS technology and geographic information system mapping to

graphically display firefighters in flaming structures; it can track personnel in high-rise buildings or in the subways.[56] Handheld radios carried by FDNY personnel transmit GPS locations on both mobile and fixed platforms; this system tracks personnel individually by fire company and position.[57] Moreover, it transmits distress signals and conducts electronic roll calls. Armed with this information, Incident Commanders (IC) can better deploy, employ, command, and control responding forces. Then they can effectively send search teams to locate dead, missing, or injured comrades.

EFAS has already been tested in four units across the boroughs with positive results.[58] Consequently, FDNY leaders are expanding the program to other units citywide. This system will provide better situational awareness for the ICs, improve their ability to effectively C2 responding forces, and quickly deliver aid to distressed first responders.

Common Operating Picture

The third C3 element, COP, builds on or is the culmination of the other two. It can be fully realized only after a dedicated nationwide communication system has been established, along with an effective means to track responding personnel, vehicles, equipment, and assets. As with interoperable communications, there are many definitions of COP. For purposes of this paper, the following NIMS definition will be used: "COP provides an overview of an incident created by collating and gathering information, such as traffic, weather, actual damage, and resource availability, of any type (voice, data, etc.) from agencies and organizations in order to support decision-making."[59]

The need for a COP for the first responders was born out of 9/11. All national-level policies identify COP, at a minimum, as a desired end state to be achieved through

procedures, agreements, and eventual integration of systems. For example, the NIPP advocates a networked approach for information-sharing, and the NRF contends that in order to have an effective, unified effort, response agencies (governmental and NGOs) must gain and maintain situational awareness by continually monitoring relevant information.[60] Likewise, the Emergency Services SSP cites COP as the primary national strategic goal for the national critical infrastructure sector.[61] Fundamentally, the COP provides the right information, at the right time, in a user-friendly format to support effective decision-making.

Currently, responders rely on a number of disjointed methods to get a COP. At the national level a 24/7 National Operation Center (NOC) acts as a hub for fusing law enforcement, intelligence, emergency response, and private sector reporting.[62] Its primary function is to maintain situational awareness and provide operational coordination across the federal government for incident management.[63] This is largely accomplished through standardized reporting procedures, delivered telephonically or electronically, set forth in the previously mentioned national policy documents. Additionally, the NOC seeks to sustain situational awareness by means of the Homeland Security Information Network, a web-based communications platform that enables federal, state, local, and partner agencies to obtain, analyze, and share information.[64] The NOC thereby facilitates collaboration among members and assists with providing real-time connectivity between states and the NOC.

At the state and local levels, COP is generally achieved through emergency operation centers, which may or may not be operated 24/7. A COP can also be derived from coordinating information from first-responder control centers.[65] These centers

serve as the nerve system for multiagency coordination. During an incident, these centers provide inter- and intra-agency coordination, communication, resource allocation, and information collection, analysis, and dissemination.

While common language and command structure protocols have been established via NIMS and the Incident Command System, there is no single standard COP in use across all levels of emergency response, jurisdiction, and disciplines. There are however, a number of government and commercial programs available and in use throughout the country. However, these systems are usually not networked. Once again, because of the very nature and complexity of war, the military has long recognized the benefits of having an integrated C2 suite. Accordingly, it has developed and implemented the Global Command and Control System (GCCS). This system-of-systems provides a foundation for dominant battlespace awareness by providing an integrated, near real-time picture that facilitates conduct of combined, ground, air, and naval operations.[66] GCCS fuses selected C2 capabilities (satellite imagery, BFT, radar, camera feeds, etc.) into a comprehensive, interoperable system through exchange of operational and planning information.[67] This architecture shows promise for wider use, both within the military and the civilian sector, but its current utility is limited by the fact that the system only operates at the “secret” classification level. Its users must access the Secure Internet Protocol Router Network, which many emergency management agencies do not have access to.

In the public sector, NYC developed a systematic approach to incident management called CIMS (Citywide Incident Management System). It is very similar to and complies with the NIMS construct; it establishes roles and responsibilities, directs

how incidents will be managed, and offers a means for integrating regional, state, and federal agencies into a NYC response.[68] Under the CIMS umbrella are a variety of systems designed to improve situational awareness. Overall they provide a COP. These systems rely on geographic information to link maps with databases; they enable users to visualize, manipulate, analyze, and display spatial data.[69] One of these incident management systems is E-Team, which enables responders to collaborate and manage efforts across multiple organizations sharing a single identical display.[70] Another CIMS tool, CALMS (Citywide Asset and Logistics Management System), integrates multiple resource management systems. This web-based system captures information on resources commonly used during disaster response (personnel, vehicles, equipment, and supplies) from local, state, federal, and private partners.[71] It graphically depicts the location of evacuation centers, special use equipment, and facility blueprints.[72] Also it provides rosters of skilled craftsmen. FDNY is currently testing and fielding a number of systems to improve situational awareness and incident management, most notably EFAS.

Recommendation

Many changes have been made in the past 10 years to improve interoperable communications and to create a COP for our nation's first responders. However, more work is needed to truly meet the spirit and intent of published guidance and, more importantly, to meet the needs of our nation. To fully achieve viable interoperable communications, tracking, and a meaningful COP, the nation needs enabling legislation, improved compliance with established policies, clearly articulated technical standards, and a coherent funding strategy.

As a critical first step, the federal government must commit to fund and build a dedicated, nationwide, interoperable wireless network. The other options are too risky and too limited. Local stakeholders can only provide ad hoc communications and public-private partnerships leave many questions unanswered regarding dedicated bandwidth and overall governance of the system.

A dedicated public safety system will assure effective emergency communications. This system is affordable over time. It will benefit from economy-of-scale and provide better service through access to and competition from the commercial sector for cutting-edge technology. Benefitting from the upgrade of 4G technologies, the public safety community will benefit from a quantum leap in access to state-of-the-art capabilities, which will enable them to better protect themselves, and the homeland.[73]

To build this system, Congress must amend legislation and dedicate the D Block to the existing public safety frequency spectrum. This new legislation will provide the domestic security community with twice the current bandwidth and much greater capacity for current and future needs.[74] This additional bandwidth is required, as proven during a recent test in San Francisco, to take full advantage of video, data, and eventually voice capabilities. Based on the results of this public safety broadband network test, at least 20 MHz of continuous spectrum is needed to fulfill emergency responder's day-to-day voice, data, and video needs.[75]

To pay for this upgrade, the federal government should use proceeds from the upcoming auction of frequency spectrum already identified by the FCC. The initial sales

are projected to generate approximately $24B in revenue, which more than covers the estimated $15.7B cost to implement this network.[76]

Once there is a dedicated nationwide network, then work can begin on effectively integrating the disparate systems. The DHS needs to establish a bonafide communications roadmap. The DHS Science and Technology (S&T) Division is a logical choice to lead this effort. S&T must develop a consolidated list of approved technologies (radios, software, and COP systems) predicated on robust research and development followed by extensive testing and evaluation. This menu of items should be sufficiently varied to meet the diverse needs of emergency management agencies both large and small, both urban and rural, all disciplines, and at all organizational levels. These systems should operate intuitively, perform to standards, be dependable, and be fully interoperable. Additionally, well-defined requirements must be established for data, imagery, voice, video, back-up capabilities, display functions/icons, etc.

Approved systems must be able to fuse data from the myriad of sources and systems. An effective COP should depict the geographical locations of responding elements, available assets, specialized equipment and vehicles, key facilities, critical infrastructure, and specialized teams. The military's GCCS or NYC's CIMS are examples of systems that integrate alarms, videos, CALMs, and EFAS. Whenever it is practical, these new systems should accommodate legacy equipment.[77] The goal is to create a suite of systems that are compatible in a plug-and-play fashion, regardless of their hardware and/or software manufacturers.

While our federalist system cannot mandate compliance with existing and emerging standards, state and local agencies can be encouraged to comply with shared

standards through funding. For example, when federal funds pay for radios, they should be purchased off the S&T approved list and be loaded with the appropriate national emergency frequency.[78] Despite the fact that emergency response efforts and funding are state and local responsibilities, DHS must work with all levels of governmental and non-governmental agencies to develop a comprehensive funding strategy. The nation needs an objective, standardized framework to identify and assess nationwide emergency management communications capabilities in order to prioritize where limited funds are most needed.[79] Emergency management leaders should identify funding sources (federal, state, local, and private) and develop a prioritized funding strategy predicated on compliance with established guidance (NECP), risk (number of people impacted), and need (current capability and financial). For example, a small rural town that needs 3 or 4G technology and lacks the financial means to acquire this capability should be able to consult DHS to determine what funding sources are available and whether they can pay for the needed technology. In addition to the established grant programs, Homeland Security Grant Program, Public Safety Interoperable Grant Program, etc., the federal government should provide incentives for commercial carriers to share the costs of building a nationwide network. For example, the frequency bandwidth currently slated for sale could be offered at a reduced cost with the caveat that the private carrier expands 3 or 4G capability to rural areas and allows the public sector to use existing infrastructure, that is, communication towers.[80]

Finally, there is no reason to reinvent the wheel. Available technology can facilitate interoperable communications, can track assets, and can produce a shared COP. Through the various working groups like Regional Emergency Communications

Coordination Working Group, DHS can do a better job of improving communications among the various agencies within the emergency management sector. DHS should capture best practices from the field, evaluate the process, develop procedures, and identify proven technology and make all of these available to the emergency response community.[81] For example, DHS could test and evaluate NYC's solutions, determine which pieces have utility across the sector, and add the specific hardware and/or software to the approved technology list for other agencies to use.

Conclusion

To meet the national security objective of protecting the homeland and people, first responders need new and better tools. Watershed events like 9/11 have exposed vulnerabilities in first responders' communication capabilities. Effective and efficient emergency response C3 requires such capabilities in order to mitigate the damages of catastrophic terrorist attacks and to respond to major natural disasters or other emergencies.

To improve their capability to protect our great nation, first and foremost responders need a dedicated, interoperable, nationwide wireless network. Such a network will facilitate integration, synchronization, and unity of effort from all levels of government; non-government agencies; and all disciplines. After this network is created, further enhancements can be realized to track and provide a "true" COP that is shared, viewed, and used by all echelons of emergency response leadership. This capability will provide incident command teams with the ability to pinpoint equipment, locate key facilities and infrastructure, and effectively track emergency response personnel. All of this will expedite, improve, and synchronize critical response and

recovery efforts. Most of all, it will save lives and assure the best use of critical national resources.

Despite improvements made in first responder communications, there is still a great deal of work left to be done. For example, Congress needs to act quickly to dedicate spectrum to public safety and fund a nationwide wireless network. The time to act is now, before the next major catastrophic event, natural or man-made, takes more innocent lives. Our nation, our people, and our emergency responders deserve and demand protection. Our elected leadership must act decisively to ensure homeland security through better policy and appropriate funding.

Endnotes

[1] Thomas H. Kean and Lee H. Hamilton, *The 9/11Commission Report* (2004), 298.

[2] Barack H. Obama, *A National Security Strategy* (Washington, DC: The White House, May 2010), 17.

[3] Barack H. Obama, *A National Security Strategy* (Washington, DC: The White House, May 2010), 18.

[4] Barack H. Obama, *A National Security Strategy* (Washington, DC: The White House, May 2010), 19.

[5] Thomas H. Kean and Lee H. Hamilton, *The 9/11Commission Report* (2004), 283.

[6] Willam a. Manning, *World Trade Center Bombing: Report and Analysis* (February 1993), 52.

[7] Thomas H. Kean and Lee H. Hamilton, *The 9/11Commission Report* (2004), 280.

[8] Thomas H. Kean and Lee H. Hamilton, *The 9/11Commission Report* (2004), 280.

[9] *Homeland Security Act of 2002*, Public Law 107-296, 107th Cong. (November 25, 2002), 8

[10] *Homeland Security Act of 2002*, Public Law 107-296, 107th Cong. (November 25, 2002), 8

[11] *Robert T. Stafford Disaster Relief and Emergency Assistance Act*, Public Law 93-288, as amended, codified at 42 U.S.C. 68. (June, 2007), 1.

[12] *Robert T. Stafford Disaster Relief and Emergency Assistance Act*, Public Law 93-288, as amended, codified at 42 U.S.C. 68. (June, 2007), 1.

[13] George W. Bush, *Homeland Security Presidential Directive-5, Management of Domestic Incidents* (Washington DC: The White House, February 28, 2003), 1.

[14] George W. Bush, *Homeland Security Presidential Directive-5, Management of Domestic Incidents* (Washington DC: The White House, February 28, 2003), 1.

[15] George W. Bush, *Homeland Security Presidential Directive-8, National Preparedness* (Washington DC: The White House, February 28, 2003), 4.

[16] U.S. Department of Homeland Security, *National Infrastructure Protection Plan* (Washington DC: Department of Homeland Security, 2009), 9.

[17] U.S. Department of Homeland Security, *National Infrastructure Protection Plan* (Washington DC: Department of Homeland Security, 2009), 9.

[18] Michael Chertoff, *National Incident Management System* (Washington DC: Department of Homeland Security, December 2008), 1.

[19] Michael Chertoff, *National Incident Management System* (Washington DC: Department of Homeland Security, December 2008), 23.

[20] U.S. Department of Homeland Security, *National Response Framework* (Washington DC: Department of Homeland Security, January 2008), 7.

[21] Michael Chertoff, *National Emergency Communications Plan* (Washington DC: Department of Homeland Security, July 2008), 6.

[22] Michael Chertoff, *National Emergency Communications Plan* (Washington DC: Department of Homeland Security, July 2008), 2.

[23] Michael Chertoff, *National Emergency Communications Plan* (Washington DC: Department of Homeland Security, July 2008), 2.

[24] Todd M. Keil and W. Craig Conklin, *Emergency Services Sector-Specific Plan* (Washington DC: Department of Homeland Security, 2010), 27.

[25] George W. Bush, *A National Security Strategy for Homeland Security* (Washington, DC: The White House, October 2007), 4.

[26] U.S. Government Accounting Office, *Emergency Communications: National Communications Systems Provides Programs for Priority Calling, but Planning for New Initiatives and Performance Measurement Could be Strengthened* (Washington, DC: Government Accounting Office, August, 2009), 13.

[27] U.S. Government Accounting Office, *Emergency Communications: National Communications Systems Provides Programs for Priority Calling, but Planning for New Initiatives and Performance Measurement Could be Strengthened* (Washington, DC: Government Accounting Office, August, 2009), 16.

[28] "Wireless Priority Service," linked from *National Communications System Page* at "Wireless Priority Service," http://wps.ncs.gov/program_info.html (accessed January 26, 2012).

[29] U.S. Government Accounting Office, *Emergency Communications: National Communications Systems Provides Programs for Priority Calling, but Planning for New Initiatives and Performance Measurement Could be Strengthened* (Washington, DC: Government Accounting Office, August, 2009), 17.

[30] "Statewide Communication Interoperability Plans," October 13, 2010, linked from *The Department of Homeland Security Page* at "Statewide Communication Interoperability Plans," http://www.dhs.gov/files/programs/gc_1225902750156.shtm (accessed December, 15, 2011).

[31] FY 2010 Interoperable Emergency Communications Grant Program, linked from *Federal Emergency Management Agency* at "FY 2010 Interoperable Emergency Communications Grant Program," http://www.fema.gov/government/grant/iecgp/index.shtm (accessed December, 15, 2011).

[32] FY 2010 Interoperable Emergency Communications Grant Program, linked from *Federal Emergency Management Agency* at "FY 2010 Interoperable Emergency Communications Grant Program," http://www.fema.gov/government/grant/iecgp/index.shtm (accessed December, 15, 2011).

[33] Michael Chertoff, *National Incident Management System* (Washington DC: Department of Homeland Security, December 2008), 141.

[34] U.S. Government Accounting Office, *First Responders: Much Work Remains to Improve Communications Interoperability* (Washington, DC: Government Accounting Office, 2007), 9.

[35] Michael Chertoff, *National Emergency Communications Plan* (Washington DC: Department of Homeland Security, July 2008), 2.

[36] Thomas H. Kean and Lee H. Hamilton, *The 9/11Commission Report* (2004), 397.

[37] Thomas H. Kean and Lee H. Hamilton, *Tenth Anniversary Report Card: The Status of the 9/11 Commission Recommendations* (September, 2011), 14.

[38] Andrew M. Seybold, "The Value of the D Block," October 11, 2011, http://andrewseybold.com/2674-the-value-of-the-d-block (accessed November 14, 2011).

[39] Linda K. Moore, *Funding Emergency Communications: Technology and Policy Considerations* (Washington, DC: U.S. Library of Congress, Congressional Research Service, October 4, 2011), 35.

[40] Linda K. Moore, *Funding Emergency Communications: Technology and Policy Considerations* (Washington, DC: U.S. Library of Congress, Congressional Research Service, October 4, 2011), 11.

[41] Linda K. Moore, *Funding Emergency Communications: Technology and Policy Considerations* (Washington, DC: U.S. Library of Congress, Congressional Research Service, October 4, 2011), 3.

[42] Linda K. Moore, *Funding Emergency Communications: Technology and Policy Considerations* (Washington, DC: U.S. Library of Congress, Congressional Research Service, October 4, 2011), 5.

[43] Andrew M. Seybold, "The Value of the D Block," October 11, 2011, http://andrewseybold.com/2674-the-value-of-the-d-block (accessed November 14, 2011).

[44] President Obama Details Plan to Win the Future through Expanded Wireless Access (Washington DC: The White House, Office of the Press Secretary February 10, 2011), 2.

[45] The Benefits of Transitioning to a Nationwide Wireless Broadband Network for Public Safety (Washington DC: The White House, November 14, 2011), 5.

[46] Linda K. Moore, *Funding Emergency Communications: Technology and Policy Considerations* (Washington, DC: U.S. Library of Congress, Congressional Research Service, October 4, 2011), 12.

[47] Linda K. Moore, *Funding Emergency Communications: Technology and Policy Considerations* (Washington, DC: U.S. Library of Congress, Congressional Research Service, October 4, 2011), 12.

[48] The Benefits of Transitioning to a Nationwide Wireless…The White House 14 Nov 11 page 11.

[49] Linda K. Moore, *Funding Emergency Communications: Technology and Policy Considerations* (Washington, DC: U.S. Library of Congress, Congressional Research Service, October 4, 2011), 11.

[50] Michael Chertoff, *National Incident Management System* (Washington DC: Department of Homeland Security, December 2008), 49.

[51] Thomas H. Kean and Lee H. Hamilton, *The 9/11Commission Report* (2004), 298.

[52] Otto J. Guenther, "Blue Force Tracking," *Army*, April 1, 2004, 13.

[53] Michael M. Sweeney, *Blue Force Tracking: Building a Joint Capability*, Strategic Research Project (Carlisle Barracks, PA: U.S. Army War College, March 15, 2008), 5.

[54] Otto J. Guenther, "Blue Force Tracking," *Army*, April 1, 2004, 13.

[55] David M. Halbfinger, "GPS Units so Faulty, they Showed Fire Trucks in New York Harbor," *New York Times*, November 9, 2011.

[56] Fire Department of New York, *FDNY Strategic Plan 2011-2013* (New York, NY: Fire Department, City of New York, 2011), 9.

[57] Fire Department of New York, *FDNY Strategic Plan 2011-2013* (New York, NY: Fire Department, City of New York, 2011), 9.

[58] Fire Department of New York, *FDNY Strategic Plan 2011-2013* (New York, NY: Fire Department, City of New York, 2011), 9.

[59] Michael Chertoff, *National Incident Management System* (Washington DC: Department of Homeland Security, December 2008), 23.

[60] U.S. Department of Homeland Security, *National Response Framework* (Washington DC: Department of Homeland Security, January 2008), 32.

[61] Todd M. Keil and W. Craig Conklin, *Emergency Services Sector-Specific Plan* (Washington DC: Department of Homeland Security, 2010), 61.

[62] U.S. Department of Homeland Security, *National infrastructure Protection Plan* (Washington DC: Department of Homeland Security, 2009), 63.

[63] U.S. Department of Homeland Security, *National Response Framework* (Washington DC: Department of Homeland Security, January 2008), 55.

[64] "Homeland Security Information Network," linked from *The Department of Homeland Security Page* at "Homeland Security Information Network," http://www.dhs.gov/files/programs/gc_1156888108137.shtm (accessed January 26, 2012).

[65] U.S. Department of Homeland Security, *National Response Framework* (Washington DC: Department of Homeland Security, January 2008), 51.

[66] Michael M. Sweeney, *Blue Force Tracking: Building a Joint Capability*, Strategic Research Project, (Carlisle Barracks, PA: U.S. Army War College, March 15, 2008), 14.

[67] Michael M. Sweeney, *Blue Force Tracking: Building a Joint Capability*, Strategic Research Project, (Carlisle Barracks, PA: U.S. Army War College, March 15, 2008), 14.

[68] New York City Office of Emergency Management, New York City Community Emergency Response Team, Standard Operating Procedure (New York, NY: New York City Office of Emergency Management, August, 2009), Appendix D, 1.

[69] "Emergency Response: Geographic Information Systems," linked from *New York City Office of Emergency Management* at "Emergency Response: Geographic Information Systems," http://home2.nyc.gov/html/oem/html/about/about_gis.shtml (accessed January 26, 2012).

[70] "NYC OEM Incident Management & Coordination in NYC," briefing slides, Queens Hospital Center, September 18, 2008.

[71] "NYC OEM Incident Management & Coordination in NYC," briefing slides, Queens Hospital Center, September 18, 2008.

[72] "NYC OEM Incident Management & Coordination in NYC," briefing slides, Queens Hospital Center, September 18, 2008.

[73] The Benefits of Transitioning to a Nationwide Wireless Broadband Network for Public Safety (Washington DC: The White House, November 14, 2011), 11.

[74] President Obama Details Plan to Win the Future through Expanded Wireless Access (Washington DC: The White House, Office of the Press Secretary February 10, 2011), 2.

[75] Andrew M. Seybold, "Public Safety Broadband: Real-World Test Results," September 18, 2011, http://andrewseybold.com/2637-public-safety-broadband-real-world-testing-results (accessed November 14, 2011).

[76] Andrew M. Seybold, "The Value of the D Block," October 11, 2011, http://andrewseybold.com/2674-the-value-of-the-d-block (accessed November 14, 2011).

[77] Todd M. Keil and W. Craig Conklin, *Emergency Services Sector-Specific Plan* (Washington DC: Department of Homeland Security, 2010), 62.

[78] Michael Chertoff, *National Emergency Communications Plan* (Washington DC: Department of Homeland Security, July 2008), 22.

[79] Michael Chertoff, *National Emergency Communications Plan* (Washington DC: Department of Homeland Security, July 2008), 12.

[80] President Obama Details Plan to Win the Future through Expanded Wireless Access (Washington DC: The White House, Office of the Press Secretary February 10, 2011), 2.

[81] Michael Chertoff, *National Emergency Communications Plan* (Washington DC: Department of Homeland Security, July 2008), 17.