COMMAND AND CONTROL IN CRISIS MANAGEMENT

Andrew BORDEN

Introduction

This paper was started shortly before the events of 11 September 2001 and the subsequent actions that have been at the center of our daily news. Naturally, like all of us, I tried to put the terrible events and the even more terrible ramifications of those events into perspective. Every commentator seemed to repeat that we are entering a new phase of history and nothing will ever be the same. Nearly every aspect of American life, American politics, diplomacy, and yes American military life will be different alleged pundits from nearly all walks of public life. Thus, American Command and Control, and by extension Command and Control for crisis management, will be different. I believed it at first. I believe it less now and in the short length of this paper I hope to show you why. I also hope to show you that this lack of a radical change is both comforting and proper.

Elements of Command and Control (C2)

Classical Command and Control is based upon relatively simple principles: Know where the good guys, the bad guys, the lurk neutrals and unknowns are. Command and Control systems should enable visualization of the battle space, show the status of friendly (blue) forces and have an estimate of the effectiveness and capabilities of the enemy. Many C2 systems try to assist the commander in determining enemy intentions if possible, and if not, evaluate possible courses of action. Finally C2 systems allow the commander to communicate orders, observe results and do it all over again. This “decision cycle” is fed by information and sped by communications to forces capable of understanding the orders and taking prompt effective action. The elements of the above equations have been the subject of numerous ongoing technological improvements. These range from sensors, to systems which collect and display information, to communications systems.

Changing Times (Plus Ca Change, C’est Plus La Meme Chose)

As command and control systems evolve, the focus of those systems expands in both scope and depth. That is to say that command and control systems gather information from increasingly smaller sized units, and also from a wider variety of types of organizations and systems. This is reflected in new data elements which themselves reflect new types and capabilities of military and civilian units and equipment. But are these additional data elements used in new and different ways? The immediate answer is yes, because of improvements in sensor to shooter cycles, increased accuracy and efficiency in the application of weapons.

Naturally this allows a correspondingly wider array of options to the military. Nevertheless, little of this is a radical change. Most of it is the natural evolutionary response to the "revolution in military affairs," and fueled by the pace of technological change in the commercial world. All of this change, at least in the military realm, is focused on the changing nature of the military threat to our nation. It is not a new idea that nature and other ancient enemies, like major accidents, civil unrest and domestic and foreign terrorism, should also have a military component. What is new is the greater attention to integration of civil and military responses. From an information perspective, are military incidents involving light infantry significantly different than shootings between elements of rival gangs in an urban setting? Even if the urban setting is in Bosnia or California? The size of force, mobility and sustainability all differ but our systems can now display the data critical to the assessment of those factors and more. Hiding in hospitals or in caves or bunkered up in a ravine should make little difference other than a challenge to our sensors, weapons and ultimately targeteers. Taking this one step further, the “stuff” we track can be virtually anything. The forward edge of battle can be the leading edge of a forest fire, the boundaries of an ethnic Serbian neighborhood or a line of demarcation between the street gangs in an inner city. Blue force heavy equipment can be as easily tanks or fire engines, and air planners can bomb with fire retardant instead of 2000 pound general purpose weapons.

In each of the foregoing, we can imagine a mixture of civil and military forces, traditional battle spaces and neighborhoods, free fire zones and residential communities where the rules of engagement come in a three ring binder with a lawyer attached. All of the variances in actual application of resources are driven by data. In this light, data structures and data handling become critical for interoperability. If we think back to the integration efforts among elements of our own military establishment, we will remember the efforts (some still on-going) at data standardization. Thanks to the horrible impetus provided by terrorists, we now stand on the threshold of extending this process across all of the sectors of public safety and national defense.

Starting as far back as the mid-seventies we had plans for the military to take over postal delivery in the event of a postal strike. A strange twist of history and some vile terrorist actions have today brought that possibility back to mind as the postal union reacts to anthrax threats and absenteeism rises in the light of two tragic deaths in the ranks of mail handlers. The military forces that took over the command center of the United States Commander In Chief Atlantic during a hurricane to coordinate air and sea supplies to Florida, our forces in Guantanamo Bay Cuba, Puerto Rico, and other Caribbean islands used the facility to plot and track relief flights and shipping. Early after the storm struck, a mobile WorldWide Military Command and Control System (WWMCCS) terminal was dispatched to Puerto Rico and for a time it served as the *only link* to the government there. There are many other examples: the reinforcement of police in the riots in Los Angeles, the support to flood relief efforts in the mid-western United States, the Three Mile Island nuclear power plant accident, and so on. Each of these examples involves a relatively unique sequence of events leading to coordinated action at the most common technical denominator, people sitting together, linked by telephones and a few radios.

Today the ubiquity of the telephone is matched by that of the Internet and significant improvements in telecommunications in both the civil and military communities. VPN can allow for government use of the Internet to interoperate with civil agencies without undue risk to their own network security.

What we need to do is formally recognize this in the structure of our command and control systems. Huge modifications are not needed. To engineers, this means modifications to the current MIL-STD 2525B. Some commercial products already have these graphics included. Without much effort that standard can be updated in a manner to include civil police, fire, rescue, and public health units. Since the mid 1980’s, under direction of the Secretary of Defense, command and control has increasingly become based on commercial off-the-shelf products which are available to civil organizations at all levels. For the most part, there is little barrier to the extension of technology, even policy and procedure to the civil authority that would result in an improved civil-military coordination.

In the United States, there are Posse Comitatus laws which present legal barriers to civil-military cooperation. Changes to these laws have been proposed. The impact could be, not only that civilian-military interoperability would become critical, but also that the military Command and Control model would have to be adopted by civilian emergency response agents. The generic military command and control functions to support the typical organizations found in a military headquarters, manpower, intelligence, operations, logistics, plans, and communications are, after all, not so different from the functions required for state and local police, fire and rescue services. The civilian agencies used in disaster relief, disaster mitigation, and crisis management have similar needs differing perhaps in the immediate requirements to recognize and control the financial aspects of their decisions. Further, civilian organizations (and to a much smaller extent military organizations) must contend with liability issues in a litigious society. In this light, the retention of decision data becomes important. A company in California, Alert Technologies, recognizes these needs in their web based product, OpCenter, which merges the military C2 model with civilian financial accountability.[1]

Adapting Command and Control to Current Needs

In the light of the recent terrorism and the beginnings of what will likely be a long war involving many attacks on this country, it is time that we think of command and control systems that are capable of being extended to the civilian components which will ultimately be working with and alongside military forces. While the degree of interoperability may be new, the concepts are founded on ideas that have been around for quite some time. As I mentioned at the outset of this paper, perhaps other things may have been permanently changed by the attack on 11 September, but proven and fielded technologies and the concepts behind them can well serve our nation without a radical change. All that is required is the will to extend and unify command and control. Perhaps the new office of Homeland Defense can define the framework in which military command and control can be extended to civil agencies and organizations and help define the nature and extent of data standardization that will allow for independent yet coordinated development.

Collectively command and control programs have over the years followed the waves of technological change, expanding when technology brings new approaches, contracting when cost and interoperability considerations dominate. The American military establishment is really a collection of establishments, service elements, Joint Commands, assorted agencies, civilian positions of oversight, political positions in the legislative and executive branches, and all supported by competing commercial entities. Every part of this cacophony has some degree of funding, of manpower, of willpower, and is capable of affecting what passes for command and control within the United States. This is well known. That it produces systems that work as well as they do is a miracle and not the subject of this paper. Nevertheless, emerging from the tangle is a breed of Command and Control systems that accomplish their mission with increasing effectiveness. The architectural underpinnings of the great command and control systems currently within the military purview are flexible enough to undertake extension to the civilian world in the broad context of support to civil authority, as we have described above. Whether that support is in the form of disaster mitigation, crisis management, or augmentation of police and law enforcement agencies is irrelevant if the architectural framework for data exchange is in place.

The Global Command and Control System (GCCS) is an example of one command and control system that could be of value. Its common operational picture and ability to bring together vast amounts of planning and intelligence information could make it an ideal adjunct for civil planners. An unclassified version of this system could be set up with special attention to unclassified data exchange which would allow senior military commanders to view civil response units and, at the same time, release similar information to appropriate civil authority thereby aiding in planning. Already, in New York, there is evidence that a joint command center has materially helped coordination of the numerous organizations and vast resources required for mitigation after the September 11th terrorist attack. Automated systems, appropriate training and support could further increase the effectiveness of this kind of coordination.

Taken on a national scale, customs and immigration functions and numerous other federal, state and local agencies must share operational and tactical information thereby improving homeland defense. Regional coordination centers must track resources, follow developing situations, orchestrate multi-agency responses, disseminate critical time sensitive information, and alert the public using a common command and control system. None of the federal, state or local organizations would need to give up authority over resources to make this kind of system work. In fact, the technology required would facilitate cooperation while minimizing jurisdictional disputes since planners would have the time to address issues requiring common response and operators would have the ability to manage in accordance with such plans.

The Digital Soldier

Imagine a soldier, equipped with a “Windows CE” based Personal Digital Assistant (PDA), laser range finding binoculars, and a data radio. This soldier could be stationed forward in battle to observe possible enemy movement. Using his binoculars, with a press of the button, he could know the range and bearing to any target from his own position which itself is known through Global Positioning System (GPS) to the PDA he is wearing. The PDA with its pre-formatted messages could then pass through the data radio contact information that is instantly entered into the command and control system. Variations on this already exist and artillery fire or other responses can be coordinated in a matter of seconds. Now image the same equipment but the preformatted messages would be those that coordinate medical responses, rescue requests, reports of building or forest fires, or damaged infrastructure. The same command and control system that takes the request for artillery support can also display the civil data. Civil organizations reporting refugees or disaster victims could ensure that both civil and military authority had such information. Further, the shared information does not need to be tabular or textual in nature. Imagery from still or video cameras can be sent in this manner as well.

Mobile command and control centers based upon scalable and modular systems could be deployed forward to the scene of a disaster, perhaps first by helicopter, later augmented by vehicle mounted systems. Linked via landline, data radio, or satellite to city, county or state command centers this data can form the basis of an initial response. Military command centers already in existence could be sent the situational picture as it develops so that commanders can anticipate the military consequences and, when necessary, intelligently augment civil authority.

A Note on Bio-Terrorism Preparedness

An issue of profound current interest is the preparedness against biological and chemical warfare attacks. In an article published in May 2001, three authors from the School of Public Health and Community Medicine, University of Washington, Seattle, Washington, published an article on the subject in the American Journal of Public Health. The article was based on a survey of hospitals located in the Northwestern United States. The survey identified a general lack of awareness of the chemical/ biological threat and a complacent attitude toward readiness.[2]

The survey found that there is no systematic effort to integrate hospitals into response plans and that a large proportion of hospitals are probably poorly prepared to handle victims of chemical or biological terrorism.[3] In fact, the researchers concluded that hospitals in the survey are not fully prepared to respond to massive casualty disasters of any kind.

The study was a cross sectional questionnaire/survey of all hospital Emergency Departments in the states of Alaska, Idaho, Oregon and Washington. The questionnaire requested information about:

1. Hospital and Emergency Department demographics;
2. Awareness and Opinions;
3. Planning, training and drills within the past 24 months;
4. Patient isolation and decontamination resources;
5. Personal protective equipment, and
6. Inventory of selected antidotes.

The analysis examined the preparedness of individual hospitals to initiate treatment in two hypothetical incidents involving 50 individuals exposed either to a chemical weapon (sarin, a deadly nerve toxin) or a biological weapon containing anthrax. For the anthrax incident, medication preparedness was defined by the reported availability of ciprofloxacin or doxycycline sufficient to provide prophylaxis for two days, with the assumption that replacement stocks would become available thereafter. The risks of secondary aerosolization and person-to-person transmission of anthrax were regarded as negligible, so scenario preparedness was defined only by having a biological weapons plan and the necessary antibiotic supply without any requirement for specific physical resources.

Most of the hospitals (61 percent) were in rural locations. Slightly more than half of the respondents to the study were even aware of local or state preparedness. Only about a third of respondents were aware of plans of resources at the national level. Only 14 percent reported any familiarity with applicable federal legislation. Nearly half of the respondents answered "yes" to a question asking whether or not "biological and/or chemical weapons are a real enough threat to your community that your hospital should make specific plans in preparation to treat victims of such weapons."[4]

About 80 percent of the hospitals reported having a plan for response to hazardous materials incidents, whereas fewer than 20 percent had response plans for incidents involving biological or chemical weapons. Only 21 percent of hospitals reported having an Emergency Department area with isolated ventilation, shower and water decontamination systems. About a third of these same hospitals additionally had outdoor portable decontamination units and 24 percent had an outdoor decontamination unit, but less than a fully integral indoor unit.

Most hospitals reported having no respiratory protective equipment that would be appropriate against chemical agents. Twenty nine percent of respondents reported having enough atropine to treat 50 patients of more in response to the hypothetical sarin incident. Sixty four percent of respondents reported having antibiotic stocks for two days of prophylaxis for the 50 hypothetical anthrax-exposed individuals. Four of the five hospitals located within 35 miles of a chemical weapons depot at Umatilla, Idaho, reported that they had conducted chemical weapons response training, but they had only slightly more atropine available and no better than average preparedness for biological incidents. The authors conclude that the findings of this survey are disturbing, although not surprising. The overall assessment was that the state of preparedness in the four states studied is not adequate to support the stated strategy of the United States Domestic Preparedness Program.

According to the Associated Press,[5] Dr. Mohammed Akhter, Executive Director of the American Public Health Administration, agrees with this assessment. He briefed a United States Senate panel on this subject on October 9. According to Dr. Akhter, only 24 states have Epidemic Intelligence Service officers from the federal Centers for Disease Control. Only 32 states employ public health veterinarians, very important for identifying diseases that can be transmitted from animals to humans or are usually found in animals such as anthrax.[6]

Dr. Akhter is especially concerned about the Situation Assessment capabilities of the fifty states. He claims that 10 percent of the state health department do not even have email capabilities. The lawmakers apparently agreed with Dr. Akhter. There is a current proposal to add $1.4 billion to the $350 million that the federal government plans to spend to detect, prevent and fight deadly diseases that could potentially be spread by terrorists. The funding package also has provisions for a government medicine stockpile and food safety inspections. Among other vaccines, smallpox vaccine is also being cultured and stored in increased quantities.

This particular examination may be helpful in understanding how theory and practice of military command and control may be useful in analyzing civil emergency organization and recommending its adaptation.

Conclusion

There has been a natural convergence of technologies in command and control for the military and for civil authority which, I believe, has been ongoing, as a result both of new technological developments and converging mission areas. The events of 11 September 2001 have probably accelerated this convergence but have not changed the fundamental principles which make it inevitable. We should be assured that despite the changes forced upon us by terrible deeds, the factors that will improve our responses and help with our continuing defense have long been recognized and are already producing some results. As the military aims of our enemies increasingly fall upon our civilian population, the defense of the nation becomes an exercise in unity and commonality of purpose across all institutions. This is not a radical change. It is an inevitable change and change that has already benefited from trends in existing command and control development. Ultimately, the successful defense of any Command and Control community has been the leader.

Notes:

[1] See The company's Website <www.alerttech.com> for details.

[2] D.C. Wetter, W.E. Daniell, and C.D. Treser, "Hospital Preparedness for Victims of Chemical or Biological Terrorism," Study supported by the United States Public Health Service, Office of Emergency Preparedness, *American Journal of Public Health*, 91, 5 (May 2001), 710-715.

[3] A review of the emergency response plan of the City of San Antonio suggests that this city is an exception to this unfortunate trend.

[4] This percentage would probably be much different today.

[5] *Express News*, Associated Press Release (San Antonio, Texas, October 10, 2001).

[6] For updates the reader may refer to the official Website of the American Public Health Administration at http://www.apha.org/.

ANDREW BORDEN is a mathematician with long experience in Electronic Warfare. He has published many papers on the subject of decision-making systems. Mr. Borden is a retired Air Force Officer. His last active duty assignment was as Deputy Chief of Staff for Intelligence in what is now the USAF Air Intelligence Agency. He has advanced degrees in mathematics from the Kansas State and Ohio State Universities. Currently, he is associated with DRH Consulting, San Antonio, TX. The address for correspondence is: 1210 Scenic Knoll, San Antonio, TX 78258. *Email:* borden@wireweb.net.