COMMAND AND CONTROL IN CIVIL EMERGENCIES

Command and Control: The management of coordinated, purposeful (military) activities

The objective of this introductory paper is to present a view of Command and Control (C2) *concepts*. C2 can only be properly understood by an analysis of its elements. These elements are necessarily involved in any discussion of C2, specifically in the discussions contained in this issue. Therefore, the elements of C2 will be used as a framework within which to present the variety of articles that follow.

Command and Control (C2) is a military task which is pervasive. It is a part of virtually every military activity. When the third "C" (Communications) was added, C3 was no longer the description of a military task. Communications is a means for executing several C2 sub-tasks. Unfortunately, the tendency for the acronym to grow has been irresistible. The latest version is Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR). This is an amalgam of a military task, several supporting tasks and means to carry out these tasks. The editor of this volume prefers to stay with C2, a definable task, the elements of which can be identified and understood.

The Elements of Command and Control are to: assess the situation, plan, coordinate and direct. The objectives for the activity are assigned by an agency external to the process, the Command Authority. In addition, data about the situation as well as resources available are provided. The first step is to assess the situation, both the emergency or military situation itself and the status of usable resources to apply to the task. Situation Assessment may depend on the fulfillment of established Essential Elements of Information (EEI's) which are specific to the type of emergency being addressed. Reporting procedures and the responsibility for satisfying the EEI's are also a part of C2. A complete plan would address these issues, but for Operational Security reasons, might not contain the EEI's. Publication of specific information

needs is an invitation for perpetrators to disguise their activities and intentions by some form of deception.

The next step is Planning. Of course, a general plan almost surely exists. The general plan specifies the procedures to be followed in every aspect of the C2 process, including Situation Assessment. It probably contains a C2 Annex which outlines, among other things, communications procedures to be followed in support of C2. The second part of the Plan is an ad hoc plan, based on the situation specific assessment. In emergency response, this Plan could be very rudimentary, but it is always present. There may be an outline of the specific Plan in the overall Plan. Within the Planning block may be one or more approval cycles which must be followed before execution. Alternatively, an agent might be pre-authorized to execute the Plan without specific approval. The assigned objectives are a critical element of Planning. The objectives might be to prevent an incident, to apprehend the perpetrators, to contain the damage or to find possible survivors.

The general plan might contain information about support from external agencies which has already been negotiated and is available on demand. However, the specific plan might require approval for support from various agencies not under the direct control of the C2 agent. The requests for coordination go to the appropriate places and the *coordinated* support must be confirmed before the ad hoc Plan is approved and executed.

Of course, the C2 process is not a linear process. There might be an instant reaction, based on established policies, before the C2 process is even initiated. Support from other agencies will probably be assumed and there might be no need to wait for formal concurrence. Nevertheless, the elements almost always happen in a more (or perhaps) formal and structured way.

A Plan is useless unless it is transmitted to agents responsible for execution. Secure, reliable communications are essential for this purpose. If a Plan is to be published however, Operational Security might dictate that specific communications capabilities be kept out of the Plan and published in a confidential companion document.

For the word “military” in the definition, we can substitute the word “emergency”. The intent is that compliance with direction is not to be negotiated. The relationship between decision-makers and those who carry out the decisions is at least semi-authoritarian as it must be in emergency response. It follows that civilian C2 is virtually the same as the military version. The same elements are present.

In the papers that follow, the reader may look for the elements of C2 in the civilian setting. The articles in this volume of *Information & Security* are structured in three

sections. The first section covers emergency C2 arrangements in national and state setting. The second section contains two papers presenting initiatives, achievements and novel ideas for international cooperation in crisis and emergency management in the region of South East Europe (SEE). The third section provides examples of the use of advanced technology to achieve cost-effective command and control in civil emergencies. As usual, this volume of the journal also presents relevant books, initiatives, and Internet sites fur further study of command and control arrangements in civil emergencies.

The first article by the editor of this volume looks at how military command and control concepts may be adapted to the management of civil emergencies. In the light of the recent terrorist attacks and the beginnings of what is likely be a long war on terrorism, it is time to think of C2 systems that are capable of being extended to the civilian components which will ultimately be working with and alongside military forces. C2 systems gather information from increasingly smaller sized units and from a wider variety 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.

All that is required is the will to extend and unify command and control. Perhaps the new US 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. The Global Command and Control System is an example of one C2 system that could be of value. 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.

The paper also provides a glimpse on the challenges of bio-terrorism. Referring to survey results, the author questions the preparedness of medical facilities in the United States to deal with bio-terrorist attacks such as the recent anthrax attack. Only after the attacks began, The Senate of the United States was briefed on these same issues… but with considerably more urgency. The response of the lawmakers was necessary and predictable – spend large amounts of money to increase readiness and protect the American people.

The article by Mike Miller presents the Basic Plan for emergency management of the City of San Antonio that has approximately one million inhabitants. This city faces variety of hazards and threats. Chief Miller points out that the plan has all necessary requisites of an organization consistent with the military model of Command and

Control. There is one important difference, however, between military C2 and civilian emergency response. Military forces can *actively* take the initiative. Civilian agencies are necessarily *reactive*. However, civilian agencies can *proact* by preparing relatively detailed ad hoc plans for a wide range of contingencies and by coordinating with other agencies in advance to minimize approval times when incidents occur. The City of San Antonio (COSA) has certainly done this in its emergency response plan that is most like a military plan. The elements of C2 are explicitly called out as they must be if emergency response is to be timely and effective. The Plan clearly explains the responsibility of the Emergency Operations Center and the on-scene Commander for Situation Assessment. Generally, the on-scene Commander is autonomous in Planning and in the Direction of execution as long as established guidelines are followed.

The city has done extensive coordination with all agencies that could support emergency response. For example, the support of the renowned burn center at the nearby Brook Army Medical Center is pre-coordinated so that no time is wasted in requesting approval from higher authority. The activities of voluntary agencies like the American Red Cross are specified in advance so that their response can be almost automatic. Interagency arrangements and the terrorist threat are addressed in detail. In an annex the article provides assessment of all major hazards faced by the City of San Antonio.

The article by Bud Evans presents a framework for corporate emergency response planning. It describes how a crisis management team should be organized and what the specific responsibilities of team members should be, with a special attention paid to companies with international presence. The requirements for situation assessment and decision-making are clearly identified. The framework is intended for use by multi-national corporations which might have to respond to crises across continents. This framework has been used, for example, by international insurance companies which offer protection not only against natural disasters, but also against terrorism in the form of product tampering.

A team of senior executives from the State Agency for Civil Protection of the Republic of Bulgaria contributes the last article in the first section of the volume. It presents the information systems used by the Agency to collect, process and distribute up-to-date analyses, assessments and information on chemical, biological and hydro-meteorological emergencies, as well as emergencies related to radiation, traffic or fire, including natural disasters, technological incidents and traffic accidents. The agreement for developing a framework for regional cooperation—the Civil-Military Emergency Planning Council for Southeastern Europe—is presented in an annex. This article is an example of successful multi-national cooperation among nations with a common interest. In this case, it is the protection of the Danube River basin.

The principles of Command and Control apply as well here as in any emergency response situation.

The Civil Protection Agency article also makes the transition from national to international arrangements in emergency management, discussed in the second section of the volume. In the first paper on SEE cooperation in crisis and emergency management Petya Dimitrova assesses key regional developments. The political will of the states in the region to consider security challenges and address common national concerns together has been vested in a number of initiatives promoting joint decision-making and practical cooperation, i.e. the creation of the Civil Military Emergency Planning Council, the Disaster Preparedness and Prevention Initiative, etc. Adding efficiency, these initiatives already transform traditionally negative perceptions and attitudes among SEE countries and people.

An annex to the paper presents the multinational *Crisis Information Network* (CIN) intended to provide SEE nations with an information technology support to help coordinate regional civil-military assistance and emergency relief projects. Initially, this will be a PIMS-based capability [1] primarily oriented toward support of the SEE Engineer Task Force. In the longer term, the initiative could be oriented towards improving interoperability between existing national information systems. The initial CIN capability might be used to develop a mechanism for coordinating assistance and intervention from all sources in regional emergencies and civil-military assistance situations.

Building on critical assessment of the achievements of security cooperation in South East Europe, Todor Tagarev reasons for launching SEE Cooperative Crisis Management Initiative aimed at developing sustainable regional *Cooperative Crisis Management Capacity*. The author defines this capacity as a set of Cooperative Crisis Management Capabilities to deal with the most probable crises in SEE, not least natural disasters such as earthquakes, floods, avalanches, volcanic eruptions, massive forest fires and landslides, severe storms and draught, and extreme temperatures, as well as technological disasters, industrial accidents and pollution, i.e., nuclear reactor incident, hazardous material spill, etc.

To this purpose SEE countries need to achieve commonality of terminology and procedures, standardization of reporting methods, and overall interoperability of crisis management assets, to agree on procedures for crisis management and to procure, jointly or in a coordinated manner, equipment, systems for command and control, and infrastructure. Essential is the establishment of a *Regional Crisis Management Center*, i.e., on the premises of the SEE Brigade HQ in Plovdiv, Bulgaria, once the HQ transfers to Romania (the fall of 2003).

The final section of the volume looks at some technological aspects of C2 and interoperation. Stoyan Avramov describes an ongoing effort in developing and demonstrating the capabilities of commercial-off-the-shelf technologies, integrated to provide cost-effective on-site command and control of various emergencies. The author briefly presents major operational, system, and technical architecture issues, as well as the approach chosen to deal with the problem of information assurance. The proposed C2 architecture may be easily scaled to better fit requirements of a particular customer. A scalable *Mobile Emergency Command Post* has been tested in laboratory environment and highly acclaimed at technical exhibitions. The concept will be further tested during an international disaster relief exercise, to be conducted in the summer of 2003 in Bulgaria under the coordination of the State Agency for Civil Protection of the Republic of Bulgaria.

In the next article a team of Gestalt LLC presents an approach to achieving interoperability among variety of C2 systems. Over the last several decades, C2 benefits from the increased knowledge and capabilities by using expanding number of computerized systems. The cost of establishing collaboration between these systems, however, is typically high and is complicated by differing organizational readiness levels, willingness, and technical ability to affect collaboration. The authors' approach is based on the use of a translation gateway. Translation is the conversion of one data format or protocol to another while retaining the meaning and context of the original. The key factors in translation include the data itself, the format of the data, the medium of transmission, and the context of the data that turns it into useful information. A successful architectural approach utilizes the layered methodology. Gestalt has identified four key layers that contribute to a successful translation gateway. They are: a system-neutral data interchange format, an external systems interface layer, a translation layer and an intelligence layer.

The final paper presents the Total Information Awareness research program of DARPA - the US Defense Advanced Research Projects Agency. In response to September 11, 2001, DARPA created the Information Awareness Office to research, develop, and demonstrate innovative information technologies to detect terrorist groups planning attacks against American citizens, anywhere in the world. The objective of this particular program is to create a counter-terrorism information system that increases information coverage, provides focused warnings, supports collaboration, analytical reasoning and information sharing so that analysts can hypothesize, test and propose theories, and mitigating strategies about possible futures, so decision-makers can effectively evaluate the impact of current or future policies and prospective courses of action. The articles also provides brief description of a dozen of related DARPA programs.

We believe that this volume will provide students of emergency management and law enforcement with a framework for debating variety of organizational and command and control issues, with ideas how to increase international cooperation and how technology may contribute cost-effectively.

Information & Security

Notes:

[1] PIMS is the Partnership Information Management System evolving in the framework of the NATO Partnership for Peace Program. For details refer to the PIMS Website at http://www.pims.org.