Information & Security Volume 10, 2003

Command and Control in Civil Emergencies

Edited by Andrew Borden

Editorial
Command and Control in Civil Emergencies **Abstract**

National, State and City C2 Arrangements

Andrew Borden
Command and Control in Crisis Management **Abstract**

Michael Miller
Emergency Management Planning in San Antonio, Texas **Abstract**

H.T. Evans
Formulation of Crisis Plans and Strategies **Abstract**

Svetoslav Andonov, Katerina Kostadinova and Emil Simeonov
Modern Information Technologies and General Public Protection in the Republic of Bulgaria **Abstract**

Regional Cooperation in Crisis and Emergency Management

Petya Dimitrova
Networking South East Europe in Managing Non-traditional Challenges **Abstract**

Todor Tagarev

Developing South East European Cooperative Crisis Management Capacity **Abstract**

Implementing Advanced C2 Technologies

Stoyan Avramov
Integrating COTS Technologies into a Scalable Mobile Emergency Command Post **Abstract**

David Perme, Mark Whelan and William P. Loftus
Achieving Interoperability of Command and Control Systems Using Translation Gateways **Abstract**

Information & Security
Total Information Awareness (DARPA's Research Program) **Abstract**

I&S Monitor

I&S Library Update

Government against the Terrorist Threat of Twenty First Century

Police Action against the Threat of Special Weapons of Mass Destruction Chemical and Biological Weapons Terrorism: Forging a Response

Chemical and Biological Weapons Terrorism: Forging a Response

I&S Resources

Selected Internet Sources on Civil Emergency and Law Enforcement Issues

Author: **Editorial**
Title: **Command and Control in Civil Emergencies**
Year of issuance: **2003**
Issue: **Information & Security. Volume 10, 2003, pages 5-11**
Hard copy: **ISSN 1311-1493**

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 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.

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.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

Command and Control in Civil Emergencies

Editorial

Keywords: Emergency preparedness, Essential Elements of Information, civil emergency, crisis management, terrorism, bioterrorism, disaster, hazard, interagency, international, regional cooperation

Abstract: Command and Control (C2) is a military task that is pervasive. The Elements of Command and Control are to: assess the situation, plan, coordinate and direct. However, 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 formal and structured way. For the word "military" in the definition of C2, we can substitute the word "emergency." There is one important difference 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.

full text

Author: **Andrew Borden**
Title: **Command and Control In Crisis Management**
Year of issuance: **2003**
Issue: **Information & Security. Volume 10, 2003, pages 15-23**
Hard copy: **ISSN 1311-1493**

COMMAND AND CONTROL IN CRISIS MANAGEMENT

Andrew BORDEN

Table Of Contents:

Introduction
Elements of Command and Control (C2)
Changing Times (Plus Ca Change, C'est Plus La Meme Chose)
Adapting Command and Control to Current Needs
The Digital Soldier
A Note on Bio-Terrorism Preparedness
Conclusion
Notes

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.

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.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

Command and Control in Crisis Management

Andrew Borden

Keywords: Military command and control systems, civil-military cooperation, standard, homeland defense, C2 principles, bio-terrorism, chemical weapons.

Abstract: 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. 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.
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. The Global Command and Control System (GCCS) is an example of one command and control 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 provide a glimpse on the challenges of bio-terrorism. .

full text

Author: **Michael Miller**
Title: **Emergency Management Planning in San Antonio, Texas**
Year of issuance: **2003**
Issue: **Information & Security. Volume 10, 2003, pages 24-38**
Hard copy: **ISSN 1311-1493**

EMERGENCY MANAGEMENT PLANNING IN SAN ANTONIO, TEXAS

Mike MILLER

Table Of Contents:

Solamente San Antonio (nowhere else but San Antonio)
Outline of the basic plan
The current situation
Concept of operations
The incident command system
Interface between the ICS and the Emergency Operations Center (EOC)
Actions by phase of emergency management
Communications
Direction and control
Terrorist incident response
Readiness levels
General provisions for direction and control
Conclusions
Annex 1: Basic Plan - Table of Contents
Annex 2: Assessment Of Threats
Notes

Solamente San Antonio (nowhere else but San Antonio)

Residents of San Antonio are justified in regarding their city as unique and as uniquely interesting. This belief is supported by the large number of visitors to the city every year.

San Antonio, Texas, has a population of approximately one million. It is the tenth most populous city in the United States. The city is notable for its cultural diversity. Approximately half the citizens are Hispanic and the Spanish influence is evident everywhere – in music, dance, architecture and in the widespread use of the Spanish language. The Mexican border is only three driving hours away and it

is common to see Mexican nationals shopping in San Antonio or visiting relatives.

San Antonio has a medical school, five major universities and a large community college (two-year college) system with four campuses. These institutions contribute further to diversity by attracting students from all over the world. Two Mexican Universities have branches in the city as well.

The city is a major medical center for the South Central United States. In addition to the University hospital, there is a major Veterans Administration hospital and many private hospitals and clinics. The medical industry is a major part of the economic life of the city. The community colleges offer medical training in a number of sub-specialties such as medical imaging and local graduates are employed widely throughout the United States.

San Antonio has four major military bases and a large civilian depot where military aircraft receive periodic maintenance and refurbishment. One of the bases is the home of the Air Force's Education and Training Command. Pilot training is also conducted at this base and many foreign military officers attend this training. Another of the bases is the home of the USAF Air Intelligence Agency. Two of the bases have major medical facilities which provide training to US Air Force and US Army personnel, and serve as specialist hospitals for their respective services. The Brook Army Medical Center has a renowned burn treatment center and a deployable team which is an element of the city's emergency response plan.

The military bases also provide Basic training to Air Force recruits, Security Police training and language training to military members from many other nations. In some cases, the foreign military personnel go on to USAF flight training or other schools for advanced training.

There is little heavy industry in the city besides stone quarrying. There are many high-tech enterprises including biotechnology developers. One of the largest insurance companies in the world is located here [1] as well as other insurance providers. Oil company management and civilian aircraft modification are other significant elements of the economy.

San Antonio is a popular location for conventions all throughout the year. It is also a very popular tourist destination with many attractions. There are festivals of different types during every month of the year and large gatherings of people are common.

The diversity of San Antonio and the military presence mean that the potential for a variety of emergency situations exists. However, the military also offers resources that can be mobilized in emergency situations. It seems only natural that the Emergency Management Plan for the city and its Direction and Control Annex should closely resemble military contingency plans in format and in content. This plan was signed by the Mayor on August 26, 2001 and the Annex was approved in April of the same year. The responsibility for the maintenance and execution of the plan is with the City of San Antonio (COSA) Fire Department.

In this report some of the elements of the plan will be quoted and others will be summarized.

Outline of the basic plan

A city Executive Group consisting of the Mayor, City Manager(s), and the Emergency Management Coordinator provides guidance and direction for emergency management programs and for emergency response and recovery operations. The responsibilities of the members of the Executive Group are clearly specified in the Basic Plan.

The Table of Contents of the Basic Plan is presented in Annex 1 to this article. Its organization is consistent with the model of Command and Control described in the Introduction to this issue of the Journal. In fact, the plan closely resembles a military operations plan. Situation Assessment, Planning, Coordination and real-time Direction are explicitly addressed by the plan.

A particular strength of the plan is the comprehensive coverage of *coordination* with other agencies: the State of Texas, Federal, Local, private and non-governmental agencies, e.g., the Red Cross. Another strength of the plan is the explicit determination of responsibilities for reporting and Situation Assessment by the on-scene *Incident Command Post* (ICP) and the *Emergency Operations Center* (EOC).

The scope of the plan is necessarily broad, since the environment in the City is so diverse. The variety of possible hazards to be encountered is presented in a table from the plan – Hazard Summary – given as Annex 2 to this paper. Response guidelines are given for each type of hazard, but it is recognized that the Planning function continues on a real-time basis as information about the specific incident is received.

The current situation

In the ninety days following the World Trade Center attacks, bio-hazards have appeared in many places in the United States. Anthrax anxiety has proven to be challenging for local agencies in almost all cities, but there has been little impact on capital budgets in the City of San Antonio. The city had already made major capital investments to equip the Fire Department's *Hazardous Materials Response Team* which is responding to 10 times the normal volume of calls. These investments were to ensure logistics readiness consistent with the requirements in the Emergency Response plan.

Similar capital investments were made several years ago by the Metropolitan Health District which operates the disease surveillance laboratory for 46 South Texas counties, including the county in which San Antonio is located (Bexar County). The Bexar County Metropolital Health District is one of the agencies cooperating with the City of San Antonio in accordance with the Response Plan.

Although there has been no credible indication of anthrax in the State of Texas, there have been many reports of possible cases and many corresponding investigations. The Hazardous Material Response team has responded to calls 303 times, compared to 16 responses in the same period last year. More than 250 items have been tested by the city health department. None has tested positive for anthrax. Each basic laboratory culture costs about $30 to $35. In about 4 percent of the cases, additional tests are needed to confirm or deny false positive results.[2]

Concept of operations

In the Concept of Operations (CONOP), responsibilities are clearly defined and the elements of Command and Control as presented in the Introduction are explicitly called out. Initially, the authority for response to any emergency is the senior officer on the scene.

Emergency responders from the City of San Antonio (COSA) are likely to be the first on the scene of an emergency situation. They will normally take charge and remain in charge of the incident until it is resolved or others who have legal authority to do so assume responsibility. The first responders will seek guidance and direction from COSA officials and seek technical assistance from State and Federal agencies and industry where appropriate.

The first local emergency responder to arrive at the scene of an emergency situation will implement the incident command system and serve as the *Incident Commander* until relieved by a more senior or more qualified individual. The Incident Commander will establish an Incident Command Post (ICP) and provide an assessment of the situation to local officials, identify response resources required, and direct the on-scene response from the ICP.

COSA will use its own resources to respond to emergency situations, purchasing supplies and equipment if necessary, and requesting assistance if COSA resources are insufficient or inappropriate. Bexar county will be the first channel through which the city will request assistance when its resources are exceeded. However, the presence of the military bases within a 25-kilometer radius of the center of the city means that non-civilian resources can be made available quickly and with only local coordination and approval. For example, The United States Army Fort Sam Houston is home to a major medical complex. Assigned to this complex is a renowned, deployable burn treatment team. In addition, Fort Sam has a Hazardous Materials Response Team that could supplement City resources on short notice. Lackland Air Force Base is home to Wilford Hall hospital, the largest in the US Air Force. Sufficient coordination with military resources has been done so that minimal approval would be needed in the event of an emergency requiring their assistance. Very specific direction for requesting military, County, State and/or Federal assistance is provided in the plan.

The incident command system

The Incident Command System (ICS) is both a strategy and a set of organizational arrangements for directing and controlling field operations. It is designed to effectively integrate resources from different agencies into a temporary emergency organization at an incident site that can expand and contract with the magnitude of the incident and resources on hand. A detailed description of the ICS is provided in one of the Attachments to the Basic Plan.

The Incident Commander is responsible for carrying out the ICS function of command – managing the incident. The four other major management activities that form the basis of ICS are operations, planning, logistics, and finance/administration. For small-scale incidents, the Incident Commander and one or two individuals may perform all of these functions. For larger incidents, a number of individuals from different departments or agencies may be assigned to separate staff sections charged with those functions.

An Incident Commander using response resources from one or two departments or agencies can handle the majority of emergency situations. Departments or agencies participating in this type of incident response will normally obtain support through their own department or agency.

In emergency situations where other jurisdictions or the state or federal government are providing significant response resources or technical assistance, it is generally desirable to shift from the normal ICS structure to a *Unified Command structure*. This arrangement helps ensure that all participating agencies are involved in developing objectives and strategies to deal with the emergency.

Interface between the ICS and the Emergency Operations Center (EOC)

For major emergencies and disasters, the Emergency Operations Center (EOC) will be activated. When the EOC is activated, it is essential to establish a division of responsibilities between the Incident Command Post and the EOC. A general division of responsibilities is outlined below. It is essential that a precise division of responsibilities be determined for specific emergency operations.

The Incident Commander is generally responsible for field operations, including:

- Isolating the scene;
- Directing and controlling the on-scene response to the emergency situation and managing the emergency resources committed there;
- Warning the population in the area of the incident and providing emergency instructions to them;
- Determining and implementing protective measures (including evacuation or in-place sheltering) for the population in the immediate area of the incident and for emergency responders at the scene;
- Implementing traffic control in and around the incident scene;
- Requesting additional resources from the EOC.

COSA has two mobile command and control vehicles operated respectively by the Police and Fire Departments which may be used as an Incident Command Post.

The EOC is generally responsible for:

- Providing resource support for the incident command operations;
- Issuing community-wide warning;
- Issuing instructions and providing information to the general public;

- Organizing and implementing large-scale evacuation;
- Organizing and implementing shelter and mass arrangements for evacuees;
- Coordinating traffic control for large-scale evacuations;
- Requesting assistance from the State and other external sources.

Actions by phase of emergency management

This section of the Plan addresses emergency actions that are conducted during all four phases of emergency management.

Mitigation

COSA will conduct mitigation activities as an integral part of the emergency management program. Mitigation is intended to eliminate hazards, reduce the probability of hazards causing an emergency situation, or lessen the consequences of unavoidable hazards. Mitigation should be a pre-disaster activity, although mitigation may also occur in the aftermath of an emergency situation with the intent of avoiding repetition of the situation. The COSA mitigation program is outlined in an annex to the Basic Plan – Annex P, Mitigation.

Preparedness

COSA will conduct preparedness activities to develop the response capabilities needed in the event of an emergency. Among the preparedness activities included in the emergency management program are:

- Providing emergency equipment and facilities;
- Emergency planning, including maintaining this plan, its annexes, and appropriate procedures;
- Conducting or arranging appropriate training for emergency responders, emergency management personnel, other local officials, and volunteer groups who assist COSA during emergencies;
- Conducting periodic drills and exercises to test COSA plans and training.

Response

COSA will respond to emergency situations effectively and efficiently. The focus of most of this plan and its annexes is on planning for the response to emergencies. Response operations are intended to

resolve an emergency situation while minimizing casualties and property damage. Response activities include warning, emergency medical services, fire fighting, law enforcement operations, evacuation, shelter and mass care, emergency public information, search and rescue, as well as other associated functions.

Recovery

If a disaster occurs, COSA will carry out a recovery program that involves both short-term and long-term efforts. Short-term operations seek to restore vital services to the community and provide for the basic needs of the public. Long-term recovery focuses on restoring the community to its normal state. The federal government, pursuant to the Stafford Act, provides the vast majority of disaster recovery assistance. The recovery process includes assistance to individuals, businesses, and to government and other public institutions. Examples of recovery programs include temporary housing, restoration of government services, debris removal, restoration of utilities, disaster mental health services, and reconstruction of damaged roads and bridges. The COSA Recovery program is outlined in an annex to the Basic Plan.

Communications

Primary responsibility for this function is assigned to the EOC Communications Officer who will prepare and maintain the Communications Annex to the Basic Plan and supporting procedures.

Emergency tasks to be performed include:

- Identify the communications systems available within the local area and determine the connectivity of those systems;
- Develop plans and procedures for coordinated use of the various communications systems available in this jurisdiction during emergencies;
- Determine and implement means of augmenting communications during emergencies, including support by volunteer organizations;

Direction and control

Primary responsibility for this function is assigned to the Emergency Management Coordinator who will prepare and maintain the Direction and Control to this plan and supporting procedures.

Emergency tasks to be performed include:

- Coordinate COSA operating forces;
- Maintain coordination with neighboring jurisdictions and the Disaster District 3B at Department of Public Safety Headquarters in San Antonio;

- Maintain the EOC in an operating mode or be able to convert the designated facility space into an operable EOC rapidly;
- Assign representatives, by title, to report to the EOC and develop procedures for crisis training;
- Develop and identify the duties of the staff, use of displays and message forms, and procedures for EOC activation;
- Coordinate the evacuation of areas at risk.

Terrorist incident response

Primary responsibility for this function is assigned jointly to the Police Chief and the COSA Emergency Management Coordinator who will prepare and maintain the Terrorist Incident Response Annex to the Basic Plan and supporting procedures.[3]

Emergency tasks to be performed include:

- Coordinate and carry out defensive anti-terrorist activities, including criminal intelligence, investigation, protection of facilities, [4] and public awareness activities;
- Coordinate and carry out offensive counter-terrorist operations to neutralize terrorist activities;
- Carry out terrorism consequence operations conducted in the aftermath of a terrorist incident to save lives and protect public and private property;
- Ensure that required notifications of terrorist incidents are made.

Readiness levels

The following Readiness Levels will be used as a means of increasing the COSA alert posture.

- Normal Conditions;
- Increases Readiness/Watch Conditions;
- High Readiness/Warning Conditions;
- Maximum Readiness/Emergency conditions.

For each of these alert levels, specific threat conditions are defined and required actions are specified. The types of threats are:

- Tropical weather threat (San Antonio is only 240 kilometers from the Gulf of Mexico. A number of tropical storms enter the Gulf every season);
- The Tornado threat;
- Flash floods (the soil in the San Antonio region is generally hard-packed clay and heavy runoff is encountered. Low water crossings are clearly identified, but explicit and timely warning is required);
- Wildfire threat;
- Winter storm warnings (although the San Antonio climate is mild, treacherous icing conditions sometimes occur and timely warning is needed);
- Mass gatherings.

Reports

Reporting is a critical element of the Situation Assessment. In some cases, Hazardous Materials incidents for example, reporting is a federal and state requirement. In all cases covered by the Plan, specific and formal reporting requirements are specified as the basis for Situation Assessment. Requirements for record-keeping and reporting are given in the annexes to the Basic Plan.

Review and critique

The Emergency Management Coordinator is responsible for organizing and conducting a critique following the conclusion of a significant emergency, incident, or exercise. The critique will entail both written and verbal input from all appropriate participants. Where deficiencies are identified, an individual, department, or agency will be assigned the responsibility for correcting the deficiency and a due date shall be established for that action.

General provisions for direction and control

Our direction and control structure for emergency operations includes an on-scene control system—the Incident Command System (ICS)—and a centralized direction and control system—the Emergency Operations Center (EOC). These two systems may be employed individually or in combination, depending on the situation.

Emergency situations classified as incidents will normally be handled by an Incident Commander using response resources from one or two departments or agencies. The EOC will generally not be activated.

During major emergencies and disasters, both an ICP and the EOC will generally be activated. The Incident Commander will manage and direct the on-scene response from the ICP. The EOC will

mobilize and deploy resources for use by the Incident Commander, coordinate external resource and technical support, research problems, provide information to senior managers, disseminate emergency public information, and perform other tasks to support on-scene operations.

For some types of emergency situations, the EOC may be activated without activating an incident command operation. Such situations may occur:

- When a threat of hazardous conditions exists, but those conditions have not yet impacted the local area. The EOC may accomplish initial response actions, such as mobilizing personnel and equipment and issuing precautionary warning to the public. When the hazard impacts, an ICP may be established, and direction and control of the response transitioned to the Incident Commander.

- When the emergency situation does not have a specific impact site, but rather affects a wide portion of the local area, such as an ice storm. For operational flexibility, both ICS and EOC operations may be sized according to the anticipated needs of the situation. The structure of ICS is specifically intended to provide a capability to expand and contract with the magnitude of the emergency situation and the resources committed to it. The EOC will also be activated on a graduated basis.

The first local emergency responder to arrive at the scene of an emergency situation will serve as the Incident Commander until relieved by a more senior or more qualified individual. The Incident Commander will establish an ICP, provide an assessment of the situation to local officials, identify response resources required, and direct the on-scene response from the ICP.

The Incident Commander is responsible for carrying out the ICS function of command – making operational decisions to manage the incident. For small-scale incidents, the Incident Commander and one or two individuals perform all major management activities. For more serious emergency situations, representatives of various local departments or agencies or external response organizations may be assigned to the respective ICS staff sections. If the EOC has been activated, the Incident Commander shall provide periodic situation updates to the EOC.

Conclusions

The Emergency Response Plan for the COSA closely resembles a typical military Operations Plan. All the elements of Command and Control are addressed and responsibilities are clearly identified. Provisions are made in the plan for review and update and these might be needed as a consequence of the events of September 11, but the essential elements for emergency response are there. The Plan is specific and comprehensive and is the basis for long-term preparedness.

BASIC PLAN

Table of Contents

I. Authority

A. Federal

B. State

C. Local

II. Purpose

III. Situation and Assumptions

A. Situation

B. Assumptions

IV. Concept of Operations

A. Objectives

B. General

C. Operational Guidance

D. Incident Command System (ICS)

E. ICS - EOC Interface

F. State, Federal, Other Assistance

G. Emergency Authorities

H. Actions by Phases of Emergency Management

V. Organization and Assignment of Responsibilities

A. Organization

B. Assignment of Responsibilities

VI. Direction and Control

A. General

B. Emergency Facilities

C. Lines of Succession

VII. Readiness Levels

VIII. Administration and Support

A. Agreements and Contracts

B. Reports

C. Records

D. Consumer Protection

E. Post-Incident and Exercise Review

IX. Plan Development and Maintenance

A. Plan Development

B. Distribution of Documents

C. Review

D. Update

X. Attachments

Attachment 1: Distribution List

Attachment 2: References

Attachment 3: Organization for Emergency Management

Attachment 4: Emergency Management Functional Responsibilities

Attachment 5: Annex Assignments

Attachment 6: Agreements and Contracts

Attachment 7: Incident Command System (ICS) Summary

Attachment 8: Acronyms and Definitions

XI. Annexes (distributed under separate cover)

Annex A – Warning

Annex B – Communications

Annex C – Shelter and Mass Care

Annex D – Radiological Protection

Annex E – Evacuation

Annex F – Fire Fighting

Annex G – Law Enforcement

Annex H – Health and Medical

Annex I – Public Information

Annex J – Recovery

Annex K – Public Works and Engineering

Annex L – Energy and Utilities

Annex M – Resource Management

Annex N – Direction and Control

Annex O – Human Services

Annex P – Hazard Mitigation

Annex Q – Hazardous Materials and Oil Spill Response

Annex R – Search and Rescue

Annex S – Transportation

Annex T – Donations Management

Annex U – Legal

Annex V – Terrorist Incident Response

Annex 2

ASSESSMENT OF THREATS

	Likelihood of Occurrence*	**Estimated Impact on Public Health & Safety**	**Estimated Impact on Property**
Hazard Type:	**(See below)**	**Limited, Moderate, Major**	**Limited, Moderate, Major**
Natural			
Drought/Heat Wave	Highly Likely	Limited to Moderate	Moderate
Earthquake	Unlikely	Limited	Limited
Flash Flooding	Highly Likely	Moderate to Major	Moderate to Major
Flooding (River Or Tidal)	Likely	Moderate to Major	Moderate to Major
Hurricane	Occasional	Moderate	Moderate
Tornado	Occasional	Moderate to Major	Moderate to Major

Wildfire	Unlikely	Limited	Limited to Moderate
Winter Storm/Ice	Occasional	Major	Major to Moderate
Technological			
Dam Failure	Unlikely	Major	Major
Energy/Fuel Shortage	Occasional	Limited	Limited
Hazmat/Oil Spill (Fixed Site)	Highly Likely	Limited to Major	Limited to Major
Hazmat/Oil Spill (Transport)	Highly Likely	Limited to Major	Limited to Major
Major Structural Fire	Occasional	Limited	Limited
Water System Failure	Occasional	Limited to Major	Limited to Major
Security			
Civil Disorder	Occasional	Limited to Major	Limited to Major
Enemy Military Attack	Unlikely	Major	Major
Terrorism/Domestic	Occasional	Major	Limited to Major

***** Likelihood of Occurrence: Unlikely, Occasional, Likely, or Highly Likely

---

Notes:

1. United Services Automobile Association.
2. Additional details were provided at the session on “Bioterrorism: An Overview of Medical Aspects and Community Preparedness”, organized by the Texas A&M International University and The University of

Texas Health Science Center at San Antonio (UTHSCSA) Mini-Medical School, October 22, 2001.

3. Requirements based on Post-September 11 analyses were quickly reflected in emergency arrangements. See for example Governor's Task Force on Homeland Security Releases Report, Press Release (Austin, Texas, Texas General Land Office, January 31, 2002).

4. Preparedness to address the relatively novel issue of cyber-terrorism was tested in a recent multi-agency exercise. For details see Dan Caterinicchia, "Cyberterrorism drill set: Operation Dark Screen to help government, industry prepare for attacks," *Federal Computer Week* (July 22, 2002).

MICHAEL R. MILLER is Assistant Fire Chief for the City of San Antonio Fire Department. Chief Mike Miller is also the City of San Antonio's emergency management coordinator. Address: Assistant Fire Chief / EMC, 115 Auditorium Circle, San Antonio, Texas 78205. E-mail: mmiller@sanantonio.gov; mmiller@ci.sat.tx.us.

BACK TO TOP

Emergency Management Planning in San Antonio, Texas

Michael Miller

Keywords: emergency preparedness, incident commander, incident command post, emergency operation center, terrorist incident response, hazard assessment

Abstract: The article presents the Basic Plan for emergency management of a US city with approximately one million inhabitants that faces variety of hazards and threats. The author points out that the plan has all necessary requisites of an organization consistent with the military model of Command and Control. 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.

full text

Author: **H.T. Evans**
Title: **Formulation of Crisis Plans and Strategies**
Year of issuance: **2003**
Issue: **Information & Security. Volume 10, 2003, pages 38-42**
Hard copy: **ISSN 1311-1493**

FORMULATION OF CRISIS PLANS AND STRATEGIES

Harry Thomas EVANS
(CEO, H.T. Evans Inc)

Table Of Contents:

Objectives
Purpose of a Crisis Management Plan (CMP)
Corporate Crisis Management Team Organization
International Organization
Crisis Management Team Initial Crisis Briefings

Objectives

A company or corporation's paramount corporate objectives in cases requiring crisis management are to ensure, to the greatest extent possible, the safety and security of its employees and their families, customers, the public at large, as well as the safety of the company's physical assets.

Purpose of a Crisis Management Plan (CMP)

The purpose of these plans is to assist a company or corporation Crisis Management Team in responding and focusing corporate, regional and international resources to resolve a crisis situation ensuring safety to all personnel and minimum disruption to business operations. This plan should provide an organization and assign responsibilities to crisis management team members. It should outline and clarify specific guidelines and procedures for response, management and resolutions to various types of crisis incidents.

Corporate Crisis Management Team Organization

The Crisis Management Team organization will reflect 2 (two) key principles:

1. Crisis Management Team structure

2. Strategic decision-making

Initially, corporate, regional and international personnel, in charge of specific functional areas, administrate and coordinate those specific areas. When a crisis occurs, it affects every aspect of a corporation. Therefore, it is imperative that every cell or section be notified of potential problems. If necessary, the team may assemble to identify and assess a crisis situation, identifying short and long-term objectives, select options, develop responses, and ensure the implementation of measures that have been agreed upon. This team approach offers the benefit of bringing together diverse perspectives and collective experience in a situational briefing format to address crisis issues at hand.

International Organization

When a crisis occurs in a venue or country away from the corporate headquarters, it will be more efficient to decentralize decision-making, delegating management, if necessary, to a corporation authority at the location of the crisis situation. A point of contact for each facility will be the operations manager. The International Crisis Management Team will be structured in a way, similar to the corporate model, and will operate under the same functional crisis management guidelines. Corporate Headquarters will be kept duly informed of all relevant crisis intelligence data and will be extensively involved in the decision-making process regarding any and all crises.

Decision-Making

The Chairman of the Crisis Management Team, or someone acting on his / her behalf, will make final decisions on major issues. The team will report to the Chairman and make recommendations with regard to options and courses of action available. The Chairman will take all recommendations into consideration, but will act unilaterally, should the circumstances so require.

The Crisis Management Decision-Making Process encompasses actions targeted to:

1. Identify the problem.
2. Specify objectives and criteria for choosing a solution.
3. Develop alternatives or strategies.
4. Analyze and compare alternatives / strategies.
5. Select the best course of action.
6. Implement the selected plan.
7. Monitor and register results.

It is based on presumptions, such as:

- Decision-making is a process of selecting one course of action from an array of alternatives to achieve an objective.
- Decision-making is an indispensable part of the management process.
- Effective decisions are made to eliminate the cause(s) of the problem.
- Ineffective decisions attack symptoms and not causes.
- The decision-maker should examine the impact of the decision on the problem, the soundness of the solution and its workability after implementation.
- An effective decision has the following characteristics:

    - It deals with underlying factors rather than superficial symptoms.
    - It provides solutions which can be readily applied.
    - It identifies short- and long-term contingencies and impacts on the problem.
    - It is practical within human, financial and other constraints.

Other characteristics of the decision-making process can be summarized as follows:

- The process is contained in a capsule.
- There are time constraints / little time to review.
- The collective approach is best, but not always available.
- Verification of all information is needed.
- The actions of the CMT are scrutinized.
- Post-crisis decisions will be reviewed by everyone.
- Stakeholders want to be a part of the resolution process.
- Decisions have short-term effects.

- Decisions have long-term effects.

Crisis Management Team Initial Crisis Briefings

Should a crisis occur, the first person receiving notification of it should confer it to the Intelligence Coordinator. Then team *assignments* are made to confirm, clarify and verify current intelligence data. In the *immediate action phase* that follows, we need to determine:

- what must be done immediately to preserve lives and contain the situation;
- who should be deployed to the scene of the crisis;
- the *Essential Elements of Information* – who, what, where, when, why, how much, how little, how often;
- whether an off-site operational venue should be designated;
- should anyone from corporate headquarters be deployed to the crisis site;
- if specialized operational / support groups should be formed, briefed, or activated.

The *deliberate planning phase* designates the actions required to isolate and contain the incident. It involves strategic and continuing briefings for senior-level management and other corporate personnel who are aware of the situation, and developing documentation to capture all pertinent data related to this particular incident.

The *essential elements of information* comprise a threat assessment (what is known, what has happened, what are the damages or injuries and the imminent risk for further damages or injury, what are the cause(s) and alternative strategies), policy decisions (aimed to confirm the appropriate limits of what may be done and what will not be done) and strategy formulation (an overall strategy that should be pursued and separate strategies for media response, damage limitation, security, financial response, human resources).

At the *resolution phase* all components to resolve the crisis situation at the corporate, regional and international levels are coordinated. Eventually, the *post-critical phase* includes critiques/debriefings (oral and written) and psychological post-critical incident debriefings, as well as assigning personnel to secure all crisis incident documentation. A Post-Crisis Report is then elaborated that should emphasize the problems encountered, how those problems were addressed and how these problems will be addressed in future operations.

HARRY THOMAS "Bud" EVANS, a former Supervisory Special Agent with the Federal Bureau of Investigation, is the founder and President of H.T. Evans, Inc., a Crisis Management based organization affiliated with security

missions for law enforcement, military and business personnel. A Managing Director for Kroll Associates from July 1999 through December 2001, Evans directed and coordinated the development of Crisis Management and Disaster Recovery Plans for domestic and international corporations. A former member of the FBI Critical Incident Response Group (CIRG), he coordinated the establishment of FBI Crisis Response Plans and Crisis Management Teams as well as assisted in the development of the position of Crisis Management Coordinator for all FBI field divisions. Mr. Evans, a twenty-seven year veteran of the FBI, is a Crisis / Hostage Negotiator, Bomb Technician, Firearms and Defensive Tactics Instructor and is well versed in the areas of fraud, extortion/kidnapping, domestic and international terrorism. He has been assigned as well as testified in numerous Crisis Management and international terrorist operations to include the World Trade Center bombing, 1993; the Oklahoma City bombing, 1995; the 81-day Freeman compound siege in Jordan, Montana, 1996; the Atlanta Olympic Park bombing, 1996; the U.S. Embassy bombings in Kenya and Tanzania, 1998; and was assigned to coordinating duties at a Crisis Command Center for FBI operations in Kosovo, the Republic of Yugoslavia. Mr. Evans has instructed in the areas of Crisis Management, Crisis/Hostage Negotiations and Tactical Operations throughout the United States, Europe, Africa, and the former Soviet Union. Address for correspondence: H.T. Evans, Inc. 11915 Kingswood Blvd., Fredericksburg, Virginia 22408, Fax: + 1 540 891-9321.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

Formulation of Crisis Plans and Strategies

H.T. Evans

Keywords: Crisis management, critique, decision-making, deliberate planning, immediate action, crisis plans, crisis management strategy

Abstract: This paper 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.

full text

Authors: **Svetoslav Andonov, Katerina Kostadinova and Emil Simeonov**
Title: **Modern Information Technologies and General Public Protection in the Republic of Bulgaria**
Year of issuance: **2003**
Issue: **Information & Security. Volume 10, 2003, pages 43-55**
Hard copy: **ISSN 1311-1493**

MODERN INFORMATION TECHNOLOGIES AND GENERAL PUBLIC PROTECTION IN THE REPUBLIC OF BULGARIA

Svetoslav ANDONOV, Katerina KOSTADINOVA and Emil SIMEONOV

Table Of Contents:

Roles of the Civil Protection Agency of the Republic of Bulgaria
Advanced IT in support of Emergency management
Annex A
Notes

Bulgaria is in the process of adapting its system for crisis and emergency management to the requirements of democratic governance, market economy and membership in NATO and the European Union. With the start of the comprehensive defense reform in 1999, the Civil Protection Agency, until that time part of the Ministry of Defense, received the status of a State Agency as a first-level budget holder directly subordinated to the Council of Ministers. Dealing with a variety of natural and man-made disasters, the Agency cooperates with numerous organizations, including the Ministry of Defense, the Ministry of the Interior, local authorities, etc. The Agency has a range of capabilities allowing it to serve as the central national authority in dealing with civil emergencies. With a history of timely and efficient contribution to mitigating the consequences of natural disasters in neighboring countries, it further plays a very active role in promoting emergency management cooperation in South East Europe.[1] After describing the roles of the Agency, this paper presents major developments in implementing advanced information and communications technologies both in national and international setting. The recently signed Agreement on the establishment of the Civil-Military Emergency Planning Council for Southeastern Europe is given in the appendix.

Roles of the Civil Protection Agency of the Republic of Bulgaria [2]

The State Agency for Civil Protection of the Republic of Bulgaria (CPRB) is part of the Bulgarian national system of governmental, organizational, economic, scientific and social activities aimed to protect the population and the national economy in disasters, accidents and catastrophes. CPRB drafts laws and regulations regarding the protection of population and the national economy. It is responsible

for establishing, recruiting, training and using civil protection units and their readiness for rescue and protective activities. CPRB supervises the development of plans for the protection of the population and national economy; organizes the protection of the population; directs and carries out training of the members of the public for protection, assistance and mutual aid in disasters, accidents and catastrophes.

The Agency cooperates with the Armed Forces during rescue and emergency operations in disaster struck areas. CPRB is responsible for prevention and mitigation of harmful consequences when emergencies arise, as well as for application of international experience in civil protection in disasters and accidents in line with the principles and standards of International Humanitarian Law. It notifies the population and governmental authorities when disasters, accidents and catastrophes arise.

The Civil Protection Agency maintains the National Crisis Management Center that collects, processes, analyses and classifies the complete information on the occurrence of an emergency situation and informs the government authorities; organizes the interaction between state agencies and regional structures during liquidation of consequences from disasters, accidents and catastrophes.

The CPRB activities cover the whole territory of the country, interacting with the state and local administration, industrial and other organizations. Locally, CPRB's Directorates in the Regional Administrations and specialists in Municipality Administrations provide assistance to regional governors and mayors in execution of their tasks in preparation, organization, execution and control of the protection of population and national economy in disasters, accidents and catastrophes.

Table 1 provides statistical information on registered accidents and disasters in the year 2002 in comparison with 2001.[3]

The Civil Protection Agency maintains the National Plan for carrying out rescue and urgent emergency restoration activities. The Plan considers the following issues: general forecast of the potential disasters and accidents, of their consequences and final outcome, emergency preparedness, alerting and getting the authorities and forces ready, management, organization and carrying out of the rescue and urgent emergency restoration activities, types of insurance, order of implementation of the plan and the responsibilities, order of informing of the country, the population, etc.

On the territory of the country CPRB maintains 18 rescue teams with professional staff and one chemical protection unit. The rescue teams maintain a permanent day and night shifts. In emergency they cooperate with the National Fire Service and the National Police forces, emergency medical help centers and teams for rendering of specialized medical help; units of the Bulgarian Red Cross, units/ teams of the Mountain Rescue Service and the Water Rescue Service, support points, sanitary teams and posts. If necessary, units of the armed forces can take part in emergency activities.

Table 1. Registered disasters in Bulgaria in 2001 and 2002

•	Type of disaster	Number of accidents		Change in percents
		2001	2002	
1.	Fires	30 948	18 451	*-40*
2.	Incidents involving radioactive sources	27	38	*+414*
3.	Industrial accidents	24	17	*-29*
4.	Incidents involving industrial poisonous chemical substances	64	119	*+86*
5.	Incidents involving mercury	33	52	*+58*
6.	Incidents involving bombs and unexploded charges	108	132	*+22*
7.	Earthquakes	50	110	*+120*
8.	Snowstorms and Icing	164	243	*+48*
9.	Floods	29	1 667	*+5648*
10.	Heavy highway and railway accidents	6 675	6 683	*+0.1*
11.	Landslides	36	210	*+483*
12.	Hailstorms	32	68	*+113*
13.	Wind Storms and Heavy Rains	148	388	*+162*
14.	Avalanches		1	*+100*
15.	Zones of contagious diseases	11	84	*+664*
16.	Recovery of drowned people	57	64	*+12*
17.	Others	629	1 698	*+170*
	Total	**39 035**	**30 025**	**-23%**

The data in the Table obviously shows that the total decreasing of the arising accidents on the country territory in 2002 are due to of significant smaller number of registered fires and industrial accidents. All rest values of indexes are higher than these for 2001.

Advanced IT in support of Emergency management

The extensive development of information technologies (IT) gave rise to various applications in the last few decades. In spite of resource constraints, through coordination of own, national and international programs the State Agency for Civil Protection implements advanced information and communications technologies across its activities.

General public protection and emergency management in the event of natural and man-made disasters are functions directly related to the process of risk assessment and potential hazard evaluation, which presupposes the employment of high-tech methods for analysis and modeling. The introduction of up-to-date techniques for collecting, processing and handling data in support of the decision-making and emergency management system plays a major role for the success of the preventive activities and prompt response to natural and technological disasters.

The objectives for the setting up and functioning of the Civil Protection Information System include collecting, processing and distributing data, analysis and assessment of chemical, biological, hydro meteorological crisis situations, as well as situations related to traffic, fire or radiation including natural disasters, technological incidents and traffic accidents. The Information System is structured at four levels [4]:

- First level – national government (Permanent Commission for Protection of the Population in the Event of Major Natural and Man-Made Disasters /PCPP/ under the Council of Ministers; National Situation Center – Civil Protection Agency, ministries and agencies);
- Second level – district administrations;
- Third level – municipalities;
- Fourth level – peripheral (high-risk industrial or business facilities, power stations, sensitive points, research sites, observatories, warning and alert systems, etc.)

Through the existing *Matra 6501* digital communication system the establishment of 30B+D (2 Mbps) high-speed primary access to *Integrated Services Digital Network* (ISdN) of the Bulgarian Telecommunications Company PLC is possible. The integration of our information system to the National Administration network is also feasible. In that way, speedy and reliable exchange of voice, data, textual messages, geographic information and images among the ministries, central agencies and local administrations can be supported.

In compliance with the *Rules on the Organization of Emergency Response and Elimination of the Consequences of Natural and Man-Made Disasters* radio communication systems for mobile, operative and emergency communication have been built in the districts of Stara Zagora, Bourgas, Plovdiv, Kardzhali, Haskovo, Varna and Dobrich. These systems are designed for the needs of the Civil Protection and Permanent Commissions for Protecting the Population and Managing Search and Rescue (SAR) operations in the event of disasters or other emergencies.

Improving the organization and coordination of SAR and recovery activities in emergency situations demands the creation of radio communication systems in the remaining districts as well as the connection to the newly built local systems of other ministries and organizations. This problem will be finally solved by setting up a system based on modern technologies and radio communication standards (TETRA) and the appointment of an authorized operator of that system. The operator should have competence related to national security. Thus, compatibility and interoperability among the specialized professional forces and the teams of the different jurisdictions would be achieved in the process of information exchange – voice messages, data, geographic information and images from the disaster-stricken site.

The tendency for extending the IT applications to cover a larger number of human activities (research as well as management and planning) corresponds to the increased need for developing and implementing specific projects and systems supporting the overall processes of prevention and population protection.

The EDRIM—Electronic Discussion Group for Risk Management—program has been designed and is currently being set up by a leading communications and IT company by order of the Council of Europe. This IT system is intended to be the backbone of the European states' information system used for emergency management. The system is tailored to the current needs providing for services as follows:

- Non-delay, round-the-clock, all the year through communications;
- Exchange of views among all correspondents;
- Private (service) informing of the customers;
- Cooperation for efficient decision-making;
- Distribution of experience and new information.

The services above are supported during emergencies as well as in the course of planned computer-assisted workshops (meetings), exercises and training practices with the use of:

- Internet-based applications;
- Video teleconferencing;
- Electronic forums;
- Distribution of software applications and products – GIS, Word, Draw, etc.

ISDN systems, generally available in most European states, will be employed as transfer media.

The expected result is the achievement of real-time transfer (exchange) capabilities and coordinated work on:

- Plain text messages, images, video films, sound and other multimedia applications;
- Research and technical data (data bases).

The network architecture will be designed at three levels – international, national and local (regional).

The Geographic Information Systems (GIS), being an integral component of the IT systems above, possess great potential as a powerful tool for area measurements and registration of events in disaster locations, inhabited places management, statistics, search and rescue operations, environmental protection, communications, etc.

In compliance with the International Danube River Convention signed in 1994,[5] a Program on the Protection of the Danube River Environment was adopted in 1999 [6] setting up a common Emergency Notification and Alert System for the Danube River Basin. The Danube River disaster and incident warning system provides for:

- On-time receiving, processing and transferring information on an incidental pollution of the Danube River water with potential trans-boundary effects;
- Timely notification of the Danube states with the purpose of danger reduction, identification of the source of pollution, damage handling and elimination of further losses and general public information.

By a decision of the Danube Secretariat in Vienna already thirteen Principal International Alert Centers (PIAC) have been installed, respectively in Germany, the Czech Republic, Hungary, Slovakia, Slovenia, Romania, Moldova, Austria, Ukraine (2 centers), Bulgaria and Bosnia. The International Alert Center is the basic operational unit of the system. It is responsible for collecting and processing information, decision-making and coordinating the response of international cooperation. The technical equipment of the International Alert Center includes computer hardware and software, as well as INMARSAT-c satellite transceivers.

Since 1997, the Ministry of Environment, Civil Protection State Agency and the Nuclear Regulatory Agency have been using the *National Automated Radiation Monitoring System* (*RAMO*).[7] The system includes the following facilities:

- Central Monitoring Station at the Executive Agency on Environment and Waters;
- Mobile Monitoring Station;
- Regional Monitoring Stations;

- Response Cell at the Civil Protection Situation Center;
- Local Monitoring Stations;
- Control Monitoring Points at the CPRB and the Nuclear Regulatory Agency.

Information exchange between the different elements of the system is performed via modem on phone and radio channels. The software allows the reception of up-to-date visual operational information, the evolution of the radiation levels and signal indication of change in the background radiation. Usually, 10 minutes is the shortest time interval for updating the information coming from monitoring stations to the server in the Central Monitoring Station. The measurement and report interval should be shortened to 2 minutes if the radiation background is increased. The integration of the RAMO system with the *Kozloduy* Nuclear Power Plant Off-Site Radiation Control System has been realized since 2002. The projected extension of the system would include:

- Additional local monitoring stations to complement the system in the southeastern part of the country. Local monitoring shall provide for registering potential tritium pollution in case of release as a result of the operation of *Cherna Voda* Nuclear Power Plant in Romania;
- Using the full capacities of the available doze rate meters—RIT display boards installed at the municipalities—by connecting them to the radiation control system, full automation and avoidance of human factor.

In conclusion, there is no doubt that the modern information technologies play a significant role for the success of crisis management and post disaster recovery missions. The extended range of IT applications will facilitate the decision-making process and the efficient coordination and cooperation on both national and international levels.

Annex A

AGREEMENT

ON THE ESTABLISHMENT OF THE CIVIL-MILITARY EMERGENCY PLANNING COUNCIL FOR SOUTHEASTERN EUROPE

Preamble

The States-Parties to this Agreement, hereinafter referred to as the Parties;

Reaffirming their dedication to the purposes and principles provided by the United Nations Charter;

Cognizant of the fact, that civil military cooperation has become a very important element for enhancing mutual assistance among nations in the field of disaster relief;

Believing that close cooperation and coordination among the nations of Southeastern Europe must be further developed;

Stressing the importance of International Organizations and Non-Governmental Organizations in the disaster relief and response field;

Supporting the United Nations', North Atlantic Treaty Organization's, and Euro-Atlantic Partnership Council's efforts in disaster relief.

We have agreed as follows:

Article I. PURPOSE

The purpose of the present Agreement is to create the legal framework necessary for the immediate and efficient planning and coordination of the available resources, according to the decision of each Party, for disaster relief and intervention. For this purpose the Parties hereby establish a Civil Military Emergency Planning Council for Southeastern Europe, hereinafter referred to as the Council.

Article II. DEFINITIONS

For the purpose of the present Agreement, the following definitions shall apply:

"Civil defense institutions" or "Civil protection institutions" means the national emergency management authorities or bodies, which take preventive measures and action in the event of a disaster, hereinafter referred to as the Institutions.

"Disaster" means a natural or technological event, which causes or threatens destruction or damage to life or property of such magnitude as to seriously endanger the public health, safety and welfare of populations. Natural or technological disasters include, *inter alia*, earthquakes, volcanic eruptions, landslides, floods, droughts, environmental pollution, pest infestations, forest fire, dam failures, epidemics, nuclear power plant accidents, chemical and industrial accidents, air-crashes, railway accidents, and ship wrecks.

"Disaster relief" means any action taken for saving life, protecting property and returning life as soon as possible to normal activity.

"Other States" means any State not a Party to this Agreement.

Article III. ROLE OF THE COUNCIL

The role of the Council shall be to consult each other as necessary about the Parties' methods, practices, and circumstances in order to enhance practical cooperation in disaster management. It is recognized that this consultation shall help alleviate the magnitude of damages from disasters.

The Council shall coordinate efforts in all phases of the disaster management cycle: mitigation, prevention, planning, response, and reconstruction.

Article IV. COUNCIL'S AREAS OF COORERATION AND ACTIVITIES

The Council's areas of cooperation and activities shall include the following:

- Develop processes and means for practical regional cooperation in disaster management;
- Develop improved coordination methods for all phases of the disaster management cycle: mitigation, prevention, planning, response, and reconstruction;
- Develop a regional risk assessment;
- Develop recommended response plans for the greatest risks;
- Develop standard operating procedures for additional Council activities and interoperability; and
- Plan, organize, and conduct exercises and training.

The Council's fora shall include:

Annual gatherings, or as necessary, to consult on plans and procedures and the exchange of information, including inventories of any personnel, response organizations, materials, and equipment available for disaster relief;

Other fora as may be necessary for additional consultation between the Parties and Other States, International Organizations, and Non-Governmental Organizations.

Article V. STRUCTURE

The consultation and decision making of the Council shall be done with civilian and military personnel. The Council shall be composed of the heads or their representatives of the Institution(s).

The Council shall form working groups as necessary to explore and develop the Council's areas of cooperation and activities. The Council shall approve the terms of reference for the working groups.

The Council shall form a Provisional Secretariat. The Provisional Secretariat shall meet as needed to coordinate the Council's areas and activities and to plan the annual meeting.

If a Permanent Secretariat is needed, it shall be agreed to in a supplementary agreement.

Each Council gathering shall be chaired and hosted by a Party. The position of the Chairman and Vice-Chairman shall be rotational according to the agreed order and hold office for a designated time period. The Chairman and Vice-Chairman shall be chosen at the first formal meeting of the Council. The position of Chairman and Vice-Chairman shall last for one year beginning on the first of January. The Party that chairs the Council shall organize and host the annual meetings.

Article VI. DECISION MAKING

All decisions of the Council shall be made by a consensus of the Parties.

Article VII. FUNDING

Each Party shall be responsible for funding its national participation in the Council meetings and activities. Other possible sources may be asked to contribute and the Council can accept contributions to support the Council's efforts to the accomplishment of this agreement.

Article VIII. EXTERNAL RELATIONSHIPS AND OTHER INTERNATIONAL OBLIGATIONS

Decisions of the Council shall be submitted to Parties' national authorities for implementation and for approval if necessary. The non-acceptance of one Party does not preclude the execution of the decision by the other Parties.

Inasmuch as it is probable that the pattern for mutual aid among two or more Parties may differ from that appropriate among other Parties, nothing contained in this agreement shall preclude any Parties from entering into agreements with other Parties, Other States or International Organizations.

The Council may invite disaster relief agencies of Other States, International Organizations and Non-Governmental Organizations to act as a consultative body under this agreement. The Council may also invite other states or representatives of their agencies, International Organizations or Non-Governmental Organizations to attend the respective meetings of the Council in a non-decision making capacity, as observers.

The Council shall promote an active policy in order to attract other resources.

Noting of this agreement will prejudice rights and obligations of the Parties deriving from international law, international agreements and arrangements to which they are parties.

Article IX. ACCESSIONS

The present agreement shall remain open for accession by other states, able and willing to contribute to its purpose by invitation or request. Accession shall be subject to Approval by consensus of Parties.

Article X. AMENDMENTS

Any Party may suggest amendments to this agreement at any time. The Parties suggesting the amendments should provide the other Parties copies of the amendment at least thirty (30) days before the Council meetings on the amendment. Amendments shall enter into force according to provisions of Article XII.

Article XI. DISPUTES

All disputes arising from the interpretation or application of this agreement shall be settled by consultation between the Parties without recourse to outside jurisdiction.

Article XII. RATIFICATION – ENTRY INTO FORCE

This agreement shall be subject to ratification. All instruments of ratification shall be deposited in the country where this agreement is signed. The Depository shall notify the Parties of each deposit. Thirty (30) days after four signatory Parties have deposited their instruments of ratification, this agreement shall enter into force among them. For the remaining signatory Parties the agreement shall enter into force thirty (30) days after the deposit of their instruments of ratification.

For Other States acceding to this Agreement, it shall enter into force thirty (30) days after the deposit of its instrument of accession.

Article XIII. DURATION AND TERMINATION

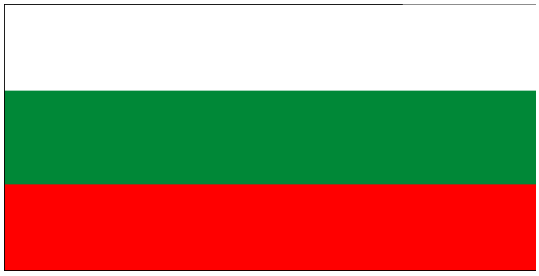
This Agreement is valid for a ten-year period and subject to automatic renewal for additional ten-year period, unless the Parties decide otherwise.

Article XIV. DENUNCIATION

Any Party may denounce the present Agreement at any time. This denunciation shall be effected by a written notification addressed by this Party to the depositary. The denunciation shall take effect one month after the receipt of the notification. After the expiration of this period, the Agreement shall cease to be in force as regards the Party which denounced it, but it shall continue to be in force for the remaining Parties.

This Agreement signed at Sofia, Bulgaria, on 03 April 2001 in one original in the English language, shall remain deposited in the Archives of the Depository. Duly certified copies shall be transmitted to the Parties.

Signed by:



……

Nikola Nikolov

Chairman of the State Agency for Civil Protection

……

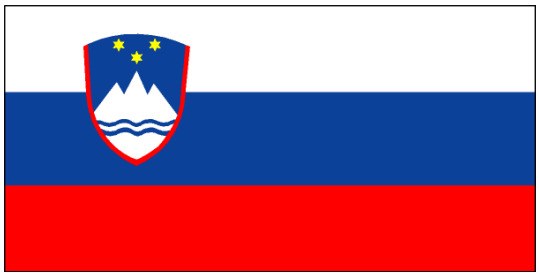
Zarko Katic

Assistant Minister of Interior

……

Dusan Gorgievski

Assistant to the Minister of Defense for Civil Protection



……

Damjan Lah

Deputy Director of the Administration for Civil Protection and Disaster Relief

---

Notes:

1. For details on Southeast European cooperation in crisis and emergency management the reader may refer to the articles by Petya Dimitrova and Todor Tagarev in the current volume.
2. "Organic Regulations for the State Agency 'Civil Protection'," Decree # 53 of the Council of Ministers of the Republic of Bulgaria, *State Gazette* 22 (9 March 2001), Amendments, *State Gazette* # 87 (15 October 2001) and # 108 (14 December 2001). Details and regular updates are available through the Website of the Civil Protection Agency at http://www.cp.government.bg/.
3. The original source is the database of the National Situation Center of the State Agency for Civil Protection.

4. Regulations for the organization and activities on prevention and mitigation of consequences of natural and technological disasters, accidents, and catastrophes, Decree # 18 of the Council of Ministers of the Republic of Bulgaria, *State Gazette* 13 (2 February 1998), Amendments, *State Gazette* # 3 (11 January 2000) and # 22 (9 March 2001), <http://www.cp.government.bg/normativna-18.html> /in Bulgarian/.

5. *Convention on Cooperation for the Protection and Sustainable Use of the Danube River* (Danube River Protection Convention), <http://www.defyu.org.yu/E-catchment/catchment2-2-1.htm>; <http://ksh.fgg.uni-lj.si/danube/envconv/>.

6. Program on preservation of the environment in the basin of Danube River. See also *Danube Pollution Reduction Program* (DPRP), Danube Program Coordination Unit, <http://www.defyu.org.yu/E-catchment/catchment2-2-2.htm>; <http://www.oieau.fr/ciedd/contributions/atriob/contribution/danube.htm>

7. Regulation on the development and exploitation of the national automated system for continuous monitoring of the radiation background in the Republic of Bulgaria, *State Gazette* 112 (1997).

SVETOSLAV ANDONOV is Deputy Chairman of the State Agency for Civil Protection since April 2001. He holds a degree in chemical engineering form the Army Academy, 1968, and M.Sc. degree in organic synthesis from the Chemical Technology University in Sofia, 1978. Mr. Andonov is 1984 graduate of the "G.S. Rakovsky" Defense College in Sofia. He specializes in radiation protection and emergency preparedness and manages the emergency activities in case of pollution of Danube River with toxic chemicals. Mr. Andonov is trained under the Convention on the Prohibition of Chemical Weapons and is Supernumerary Inspector for the Republic of Bulgaria under this Convention. He underwent extensive training at the Environmental Agency of the USA, related to toxic industrial substances, dangerous waste and response to chemical accidents. Mr. Andonov is national coordinator for the exercises on radiation response activities in case of nuclear accidents.

KATERINA KOSTADINOVA is Chief of the NBC & Ecology Department of the State Agency for Civil Protection since 2000. She holds a M.Sc. in physics from the "St. Kliment Okrhridski" Sofia University, 1988, with specialization in nuclear physics. Ms Kostadinova is with Civil Protection Agency since 1996. She is in charge of control and data processing on potentially dangerous sites in Bulgaria; chemical and radiation accidents emergency planning and response; inspection of chemical plants, sites using radioactive sources, and the nuclear power plant; control on pesticides stockpiles; data processing and inspection on individual protective equipment in Republic of Bulgaria.

EMIL SIMEONOV is Chief of Section "Telecommunications Systems" of the Crisis Management Department in the State Agency for Civil Protection. He is graduate of a technical college (Radio and Telecommunications) and holds a M.Sc. degree in Automation from the Technical University of Sofia (1972). Mr. Simeonov has worked as researcher in the area of telecommunications. His professional interests are in application of advanced communications technologies, geographic information systems and Web services in the area of crisis warning and emergency management. Mr. Simeonov is fluent in English and Russian. *E-mail*: simeonov@cp.government.bg.

***Address for correspondence*:** 30, "Nikola Gabrovski" Str., State Agency for Civil Protection, Sofia 1172, Bulgaria. *E-mail*:sacp@cp.government.bg; cprb@mb.bia-bg.com. Fax: +359 2 688 115.

BACK TO TOP

---

e-mail: infosec@mbox.digsys.bg

Modern Information Technologies and General Public Protection in the Republic of Bulgaria

Svetoslav Andonov, Katerina Kostadinova and Emil Simeonov

Keywords: National Situation Center, Risk Assessment, ISDN, GIS, INMARSAT-C, SAR, EDRIM, Emergency Notification and Alert System for the Danube River Basin, National Automated Radiation Monitoring System

Abstract: This article presents the Information System used by the State Agency for Civil Protection of the Republic of Bulgaria (IS-CPRB). The IS-CPRB is designed for collecting, processing and distributing 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. EDRIM (Electronic Discussion Group for Risk Management), the National Automated Radiation Monitoring System (RAMO) and the International Alert System for the Danube River are reviewed as useful support tools for the IS-CPRB. The agreement for developing another framework for regional cooperation-the Civil-Military Emergency Planning Council for Southeastern Europe-is presented in the annex.

full text

Author: **Petya Dimitrova**
Title: **Networking South East Europe in Managing Non-traditional Challenges**
Year of issuance: **2003**
Issue: **Information & Security. Volume 10, 2003, pages 59-72**
Hard copy: **ISSN 1311-1493**

NETWORKING SOUTH EAST EUROPE IN MANAGING NON-TRADITIONAL CHALLENGES

Petya DIMITROVA

Table Of Contents:

The Assessment
The Response
The Mechanisms
The Tools
Annex
Notes

South Eastern Europe's delicate security environment has been a challenge itself for over a decade now. However, the need to foster positive trends region wide and build communities of interest in managing problems together and not against one another has been quite prominent. Typical regional scepticism has started giving way to a more practical approach that builds on positive experiences and inclusive postures. This paper is an attempt to demonstrate how the willingness of South East European states to evolve their vision and attitudes is translated into doable ventures that try to answer the abundance of expectations and make prosperity and progress permanent features of the region.

There are various tools for addressing cooperatively current and prospective security challenges. They range from common security and risk assessment based on identical, or at least aligning, values, perceptions and considerations; common approaches delivered through respective networking and, if and when possible, a joint action.

This holds true for the region of South Eastern Europe as well. The recent redefinition of missions, re-estimation of values, reconsidering of visions, and revision of strategies has been related to certain changes in attitudes and behaviour. In addition, the external changes and internal transition have affected the way problems have been approached and treated. As a result, in the last decade or so the countries in South Eastern Europe have come up with various kinds of documents that present their assessment of the strategic environment and their respective security needs, missions and tasks – be it a national security/defence concept, strategy or something else. They offer new approaches to old

problems or treat new problems in a different fashion, and outline the principles of managing capacities and managing activities.

Lately national perspectives as to key security issues have been laid out on a new setting. 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 openness and transparency, as well as joint decision-making and practical cooperation.

Some of those initiatives have been inspired and "nursed" by outside actors – international organisations or single states, others have been launched within the region, but it is up to the will of South East European countries that implementation is put forward and progress achieved. It is also well understood by the international community. In a resolution adopted 20 December 2000 by the United Nations General Assembly, *inter alia*, it is confirmed that there is an urgency of consolidating South Eastern Europe as a region of peace, security, stability, democracy, cooperation and economic development and of strengthening relations among the states in the region. The resolution stresses the importance of regional efforts aimed at preventing conflicts, arms control, disarmament and confidence-building measures, as well as closer cooperation in crime prevention, combating illicit trade of people, drug trafficking and money laundering and closer engagement of the South East European states in furthering cooperation on the European continent that will favourably influence the security, political and economic situation in the region.[1]

This corresponds to South East European states' assumptions and understanding too. The region well makes geostrategy, geopolitics and geo-economics matter with various dimensions and emphases. Thus the particular attention paid to security cooperation in South Eastern Europe that is also demonstrated by the Organisation for Security and Cooperation in Europe (OSCE), the European Union (EU), NATO and their member states, can be attributed to the specific regional environment, its challenges and risks as well as to special interests that meet here.

South Eastern Europe is also a region where history matters. And yet, it is more and more the present and the future that have been on the agenda lately. The forward looking approach has been an incentive of an unprecedented sharing and discussing of security concerns. As a result, a headlong dynamics in relations and a considerable abundance in attempts have generated a sometimes still embryonic but rather comprehensive security network in meeting contemporary challenges. The progress therein will be very much subject to the willingness of the states to pursue what has been agreed upon on the strategic (political) level and to implement it effectively in practice. Thus it is very important for South East European states to come to terms by defining their mission and vision clearly, by holding to the same values and developing a common strategy since in most cases a single state's efforts are insufficient and inadequate to the challenges.

It is widely understood that the existence of a certain information environment is the initial crucial step in any attempt for a joint management. It is related to the overall openness and transparency that is gradually becoming a feature of security interaction. In the case of South Eastern Europe the actual networking starts on the political level where the security environment and its implications on states is assessed by means of the South East Europe Common Assessment Paper on Regional Security Challenges and Opportunities (SEECAP) – a project within NATO's South East European Initiative

(SEEI). There are also other attempts for a joint consideration of security challenges but not as comprehensive in scope and involvement and not really variant in conclusions. For the purpose of this endeavour, it will be the SEECAP that will be inspected in details.

Having a common security assessment it is rather easy to understand and channel the measures taken to address common regional challenges – be it an international formation such as the South East European Brigade (SEEBRIG) and the Operational Group for Naval Cooperation in the Black Sea area (BLACKSEAFOR) for instance, be it a council/group as is the case with the Civil-Military Emergency Planning (CMEP) one, or be it another form of affiliation.

The Assessment

The *South East Europe Common Assessment Paper on Regional Security Challenges and Opportunities (SEECAP)* is a real shift from traditional risk and threat assessment. The very aim of the Paper [2] can be summarised as a contribution to regional cooperation processes vested in various instruments; to dialogue and good-neighbourly relations, promoting better understanding of challenges and facilitating actions to address these challenges. It is a document that sets out perceptions, expectations and agendas shared by South East European countries in their effort to establish practical contacts among national security related bodies and take concerted action.

Since it is still transformation that characterises the strategic environment in South Eastern Europe and diversity that particularises the states in the region, the common resolve to promote peace, security and prosperity in a comprehensive manner is an achievement in itself. However, South East European countries have come to the conclusion that it is necessary to go further than words and take coordinated and even joint action. This effective joint ness of action is viewed as a key element promoting peace, security and stability in the region.

The resolve to respond together is declared and duly pursued though it is widely understood that South East European countries are unequally susceptible to the particular challenges. The SEECAP recognises no direct threat of military aggression between states of South Eastern Europe and it streamlines basic challenges into several categories: political, defence-military, economic, social and environmental. It iterates the need to fight real problems such as political and ethnic tensions, organised crime, economic and social failure, civil emergencies, etc., as well as psychological stereotypes and prejudice such as the international perception of the region as a source of insecurity and instability for example. The SEECAP puts a special emphasis on issues like terrorism, weapons and proliferation, early warning, conflict prevention and crisis management capabilities, considering them from both a political and military perspective. It reaffirms the fundamental roles of armed forces as “deterrence, protection, participation in collective and other security arrangements and contribution to international military operations” and stresses the importance of a proper management of change by a respective military and security strategies and doctrines’ adaptation as well as a well-reasoned psychological and technical adaptation of military personnel adequate to the new requirements and needs. It also refers to the democratic development challenges as well as the insufficient national and regional mechanisms in meeting problems such as refugee flows, natural disasters, industrial accidents and pollution.

Some of these challenges are met by reinforcing national political and social-economic systems; others can only be successfully addressed by a joint effort. The SEECAP welcomes the principle of multinationality in shaping regional response capabilities and mechanisms and is considered to be an initial step on the way to prospective security strategies and planning based on common perceptions. It sets out priorities and venues, making way for complementarity and added value. Its provisions and recommendations support the European and Euro Atlantic course followed by South East European states and fit within the broader security framework provided by the OSCE and the UN. [3]

The SEECAP is a steady consolidating effort and an ever-learning process. It reflects the regional risk environment and offers a multi-faceted security perspective that confirms the most immediate items on the regional agenda: international organised crime and terrorism, drug and arms trafficking and proliferation, economy-related challenges, ecological issues, corruption, information infrastructure threats, natural disasters and industrial accidents, etc. The options for dealing with them therefore range from informing others what is being done on a national scale in conformity with the principles of openness and transparency, to coordinating national efforts, joint decision-making and synchronised implementation by national bodies and employment of joint formations. They present various levels of commitment that reflect the evolution of relations among international actors.

The SEECAP's concept is also vested in a number of initiatives, stemming there from, such as:

- the comparative study of national security strategies in South East Europe (SEESTUDY);
- the project on the exchange of political-military and other early warning, conflict prevention and crisis management information (SEECHANGE), that envisages the voluntary exchange of classified and non-classified information on the strategic environment, political, defence-military, economic, social and democratic development challenges, as well as environmental challenges and civil emergencies;
- the exchanges of border security personnel (SEESTAFF);
- the promotion of civil-military interaction in security management (SEEMAG);
- the Compendium of Anti-Terrorism Measures in South East Europe.

The Response

The political will and effort embodied by the SEECAP and other similar endeavours have been translated into various mechanisms and tools for sharing responsibilities and enjoying benefits. Whether it is NATO's SEEI, the South Eastern Europe Cooperation Process (SECP), the Stability Pact or something else, there is always the need for a synergy and coherence among different efforts. They run parallel to the efforts undertaken by South East European states in their capacity as members of the UN, the OSCE, the Council of Europe or derive from various arrangements related to their aspiration or membership in the EU, NATO and other international organisations.

The Mechanisms

Correspondingly, it is two processes, the Southeast European Defence Ministerial and the Stability Pact for South Eastern Europe, that mostly focus the attention.

It is envisaged, within the political framework of the *Southeast European Defence Ministerial (SEDM)* process, to gradually develop a system of consultations and dialogue, cooperation and joint planning in conformity with the declared will to enhance regional interaction in meeting non-conventional and non-military challenges by sharing respective responsibilities. Bearing in mind that the institutionalisation of cooperation processes is crucial for the promotion of stability and security, the leaders of South East European states have launched a number of SEDM mechanisms and tools to address challenges and exploit opportunities.

Being an instrument for regional cooperation fostering stability, security and prosperity in South Eastern Europe and intending to streamline various security related efforts, the *Stability Pact for South Eastern Europe* provides tools for addressing most nontraditional challenges mentioned hitherto. It also supports state and institution building as well as social and economic consolidation within states of the region. It is a mechanism for focusing and channelling efforts and resources and by means of its working tables it develops a system of projects that target comprehensively security matters reinforcing the security network by "hardening" its soft dimension.

The Tools

Both the SEDM and the Stability Pact provide flexible frameworks within which various initiatives and projects are generated. For the reason of complementarity, a few of them have been selected to illustrate the extending and expanding networking of willing and able states in South Eastern Europe.

The Multinational Peace Force South Eastern Europe and its component, the SEEBRIG, gives countries a unique chance. It brings together units from NATO and Partnership for Peace countries that can be assigned to carry out peace support operations under UN or OSCE mandate based on the UN Charter. Following the combined joint task force (CJTF) principle, the Brigade's international composition allows for military from different countries with different background and tradition to work together on aligning practices and increasing interoperability, both in terms of techniques and attitudes. It constitutes a precedent in South Eastern Europe as smaller units come together under a joint command and staff and presents a challenge to both resolve and capabilities.

The Brigade became operational in May 2001 and its establishment has been accompanied by a number of staff and field exercises as well as computer-assisted ones. The intent to enhance the potential range of its activities in the future is related to a great extent to the South East European states' desire to produce security through regional sources and minimise the external support to regional stability. Ideas have also been voiced that the Brigade could be involved in missions in South Eastern Europe especially in the light of a possible US withdrawal from certain military engagements in this part of the world.

The fundamental notion of the Agreement on the establishment of the MPFSEE is that it is not aimed

at allying against any country or group of countries. The decision to deploy the Multinational Brigade will be preceded by political and military consultations and will be subject to approval by participating states in conformity with their national legislation arrangements. Particular participation, tasks and rules of engagement as well as withdrawal from an operation will also be decided together though any country can withdraw its forces following due notification and consultations. [4]

The Brigade's components come together for exercises and training. In such cases the MPFSEE headquarters, currently located in Plovdiv, is fully activated. It is also connected to the South East European Crisis Information Network (Concept sheet is provided in the appendix). In 1999 the SEDM also originated the *Engineer Task Force* within the MPFSEE to take part in rescue operations in the region and carry out small projects as an aid to Kosovo post-conflict reconstruction.

Another part of the network similar in concept to the MPFSEE though irrelevant to the SEDM process is the recently established *Operational Group for Naval Cooperation in the Black Sea area (BLACKSEAFOR)* bringing together countries selected by another regional criteria, willing to cooperate in search-and-rescue operations, humanitarian operations, mine-protection activities, environmental protection and other maritime operations. It comprises 4-6 ships from the Black Sea countries, including one for command and control.

The SEDM states have extended their cooperation to include other initiatives such as the SEESIM and SIMIHO. The *South Eastern Europe Simulation Network (SEESIM)* has been designed to facilitate SEDM countries in establishing integrated operational capabilities and reaching an average level of interoperability with NATO member states in terms of communications systems. It is a tool for integrating several related SEDM initiatives through a series of computer modelling and simulation-based exercises. The project for *Satellite Interconnection of Military Hospitals (SIMIHO)* is intended to cover a particular area of certain importance, with details regarding computer network, software, technical and communications equipment requirements still under discussion.

The SEDM was also the framework within which the *Civil Military Emergency Planning Council (CMEP)* was established to support and intensify regional cooperation, to study the possibilities for immediate effective planning and coordination of resources available for management of natural disasters, industrial accidents, etc.

A similar instrument exists within the Stability Pact for South Eastern Europe. The *Disaster Preparedness and Prevention Initiative (DPPI)* has been intended to promote regional cooperation and coordination in disaster prevention and preparedness, to reduce the impact of natural and technological disasters and to develop synergies and cooperation with existing or planned initiatives in the region with the close involvement of specialised agencies (UNDP, NATO, IFRC) and single countries (US, Italy, Sweden, Switzerland, etc.) without any excessive institutionalisation. [5]

Based on a "Regional Assessment Report" drafted by a joint team led by Croatia and Bulgaria, an attempt to develop a regional strategy for disaster prevention, preparedness and response was put forward that, if implemented successfully, will require respective programmes and projects to sustain necessary resources and capabilities. It is facilitated by the initial identification of areas of action that include:

- information sharing and networking;
- “lessons learned” from disasters and exercises;
- standardisation and harmonisation;
- preparedness planning and exercises;
- cooperation in preparedness for seasonal and common risks, including joint contingency planning, preparedness exercises and measures and early warning systems;
- joint disaster management training with a special emphasis on technical, operational and other skills, exchange of plans, techniques and materials;
- public awareness and media relations;
- strengthening local structures and involving communities in the DPPI dialogue;
- border crossing procedures.[6]

These areas of action are referred to by means of certain mechanisms that include information/expertise exchange, working groups, joint reports, exercises, conferences and seminars, establishing data base of focal points, 24-hour contacts in national emergency centres and international organisations; communicating reports and information on national organisations and structures, and on emergency management procedures. Progress has been made on the consolidation of the Disaster Management Training (DMT) Programme for South Eastern Europe as well as particular projects, such as the Joint Fire Fighting Unit Croatia/Bosnia and Herzegovina/the Federal Republic of Yugoslavia – Montenegro, etc.

The Stability Pact has been the background for a number of other initiatives as well. The *Anti-Corruption Initiative (SPAI)* is intended to give a decisive impetus to the fight against corruption in the region through a comprehensive set of actions under five pillars:

- adoption and implementation of European and other international instruments;
- promotion of good governance and reliable public administrations;
- strengthening of legislation and promotion of the rule of law;
- promotion of transparency and integrity in business operations;
- promotion of an active civil society.[7]

As organised crime has been considered as one of the gravest problems in South Eastern Europe with specific political, economic, social and psychological implications and references, related to the region's geographic location and historic legacy, an *Initiative to Fighting Organised Crime (SPOC)* [8] has been launched to help South East European states counter actions of criminal groupings that are often irregularly structured and transnationally supported. Weak institutions, failure of coordination, and insufficient resources to withstand make the organised crime a threat to fragile democracies in the region. Thus SPOC is a tool that helps identify problems and objectives and mobilise regional and international resources to achieve these objectives, provide targeted assistance for policies, institutions and capacities and ensure political commitment.

The fight against organised crime is a national effort that by means of SPOC is placed within the institutional and legal framework of the UN, the OSCE, the EU, the Council of Europe, and assisted by the expertise of other institutions such as Europol, Interpol, the Southeastern Europe Cooperation Initiative (SECI), the Central European Initiative (CEI), and the Adriatic Sea Initiative.

The objectives of SPAI and SPOC have been supported by the Council of Europe's *Programme against Corruption and Organised Crime in SEE (PACO)* that targets policies, effectiveness of justice and regional cooperation. Recently a special project aimed at strengthening networking among countries of the region through direct communications among judicial authorities, similar to the European Judicial Network, has been launched. Further efforts in this area will be very much influenced by the recent developments in the EU where most of the South East European countries aspire. The extended internal exchange and cooperation and the establishment of a common border police and rules for fighting money laundering and terrorism will affect the aspirants as well in their efforts to meet the requirements under the Union's third pillar especially regarding the EU policy standards and practices pursued in the reform of law enforcement institutions.

There are other channels that contribute to that end too. By exchange of knowledge and experience the Stability Pact's *Regional Police Training Initiative* aims at bringing forward best regional and international practices and developing a network for cooperation. It will be institutionalised through the *Southeast European Police College* that is supported by the Association of European Police Colleges (AEPC), the Central European Police Academy and the Nordic Baltic Police Academy and intended to enhance police skills, democratic policing, and develop regional networks and cooperation in joint fight against transnational organised crime.

Organised crime, illegal trafficking and terrorism are also items on the agenda of another regional arrangement, the *Southeast European Cooperative Initiative (SECI)*.[9] It is a flexible framework that addresses as well issues like good-neighbourly relations, economic cooperation, infrastructure development, humanitarian, social and cultural contacts. In compliance with the Agreement on cooperation to prevent and combat trans-border crime,[10] the South East European states have agreed to cooperate by providing assistance in the form of information or expertise exchange. A special SECI Regional Centre for Combating Trans-border Crime [11] has been established in Romania to help develop effective joint interagency working relations.

There are other examples that can also be cited to illustrate the dynamic networking in South Eastern Europe like the *Migration and Asylum Initiative* or the *Border Control Initiative*,[12] the forum of East

European intelligence and counterintelligence services, established in May 2002 in Romania, the so called 2+2 initiative involving Bulgaria, Greece, Romania and Turkey and supporting the candidates' aspiration to join NATO but intended to evolve beyond and cover other issues as well, etc. All these tools, designed to manage cooperatively, or support national efforts regarding, regional challenges, have some common features though the kind of response and scope of commitment varies respectively.

The management of non-traditional challenges is a process that relies extensively on exact and timely information for any decision-making at any stage: planning, organisation, implementation or assessment/control. All of the initiatives mentioned above can only be possible if information is exchanged and it is exchanged properly. Therefore, the development of an adequate and effective information environment to support any management attempt is essential. This understanding has facilitated the ever-growing use of computer systems and IT on national and international scales. It also encouraged the introduction and spread of the *Partnership for Peace Information Management System (PIMS)*[13] that is a flexible tool for ensuring efficient and reliable capabilities and information exchange among states and organisations by means of IT and common infrastructure. It is intended to enhance regional cooperation, facilitate communications, workshops, conferences, exercises and daily operations. It is a venue for collaborative information sharing, but also for interoperability enhancement. The PIMS network is enjoyed by state institutions in many countries, incl. ministries of defence, ministries of foreign affairs, civil protection organisations, law enforcement bodies, etc. It is also a secure domain for SEDM and CMEP planning and emergency management.

Since 1999 the PIMS web has been enhanced by the SEDM's *Crisis Information Network (CIN)*[14] that, among others, is intended to expand the reach of PIMS to meet new crisis management requirements by ensuring fast information exchange, interoperability and coordination of national activities in disasters and crises as well as support to C2 systems. It will be further enhanced by the prospective activation of the *Global Disaster Information Network (GDIN)* as a means of exchanging CMEP-related information.[15]

The mechanisms, tools and arrangements described above come to confirm the resolve of countries in the region to sustain communities and networks "for" and not "against", in an environment that is extremely dynamic in development and abundant in opportunities. The diversity of this security environment demands the evolution of capabilities and structures of national security organisations in order to successfully address current and possible future challenges. It is much about changes of concept and mind but it is also about developing certain skills and attitudes that can interact cohesively within the national and international environment and support effectively political strategies. It is also about consistency of philosophy and flexibility of approach that South East European countries have started to gradually adopt in meeting together common security challenges, thus making way for a stable, prosperous and secure future for all.

Annex

CRISIS INFORMATION NETWORK

CONCEPT OF OPERATION

Scope

The multinational Crisis Information Network (CIN) is to provide SEDM 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 primarily oriented toward support of the Engineer Task Force. In the longer term, the initiative could be oriented towards improving interoperability between existing national information systems. In the future, 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.

Mission

The Crisis Information Network (CIN) mission is to provide the participating nations with a reliable, low cost, high technology, interoperable, standards-based communication and information exchange environment to be used for crisis management, coordination of emergency relief and regional civil-military assistance.

Functions

The SEDM nations have agreed that in the near term:

A. The Partnership for Peace Information Management System (PIMS) will serve as the initial phase CIN, alone or in conjunction with national systems.

B. PIMS will provide an initial database and planning capability focused on supporting the SEDM Engineer Task Force (ETF) and Civil-Military Emergency Planning (CMEP) initiatives.

C. A mapping capability should be added (this will require additional PIMS support).

Command and Control, Organisation

In order to implement the initiative as quickly as possible, the following step-by-step approach is proposed:

A. Phase I

(1) Identify users, locations, and types of information to be exchanged in support of small-scale bilateral or multilateral projects to be conducted under the auspices of the ETF.

(2) Initial PIMS connectivity is required for SEEBRlG, PMSC*, and

other non-governmental organisations associated with ETF and CMEP tasks.

(3) The CIN Working Group will form a subgroup devoted exclusively to monitoring the effectiveness of information technology support for the ETF “customer support” needs in each SEDM nation.

B. Phase II

(1) As the PIMS-based CIN matures in its support of the ETF, nations will examine a wider C2 architecture to permit wider coordination, on the following options:

(a) CIN coordinated under the authority of the PMSC.

(b) “Stand alone” CIN with some suitable political-military direction.

(2) Because alternative approaches may imply different multinational system support integration requirements, the CIN Working Group will establish a second subgroup. This subgroup will exist solely to permit a multinational consultation process for:

(a) Improving the interoperability between the separate national Crisis Information Systems.

(b) Considering the development of a mechanism for coordinating assistance and contributions from all sources, in regional emergencies and civil-military assistance situations.

(c) Coordinating the development of a civilian and military council for planning regional cooperation in response to disasters. The schedule of workshops led by Civil Protection organisations of the SEDM nations will be adapted for mutual support with the long-term development of CIN.

CIN System Availability and Composition

Contributing nations determine their level of participation in providing technical support to CIN.

The United States provides the PIMS capability to support initial connectivity required to support implementation of ETF and CMEP activities. If necessary in the future, augmentation of CIN to higher levels of capability beyond PIMS will be at the expense of the participating nations.

The United States agrees to help facilitate discussions among nations in order to coordinate effective multinational collaboration that may result in an enhanced CIN capability above that provided by PIMS.

* Political Military Steering Committee

Notes:

1. *Report of the First Committee*-(A/55/552, 20 December 2000). Resolution adopted by the UN General Assembly
2. <http://daccess-ods.un.org/doc/UNDOC/GEN/N00/561/01/PDF/N0056101.pdf?OpenElement> (6 October 2002).
3. South East Europe Common Assessment Paper on *Regional Security Challenges and Opportunities* (SEECAP), (Budapest, Hungary adopted May 2001), <http://www.nato.int/docu/comm/2001/0105-bdp/d010530b.html> (12 May 2002).
4. Ibid.
5. *Agreement on the Multinational Peace Force South Eastern Europe*, signed September 1998 by SEDM states.
6. Disaster Preparedness and Prevention Initiative (DPPI), *Strategy and Next Steps*, (Regional conference, Bucharest, 25 and 26 October, 2001).
7. Ibid.
8. *SPAI Strategy and Action Plan for 2002 and beyond*, (Formally endorsed at the Budapest Working Table II meeting of the Stability Pact in November 2001), available online at http://www1.oecd.org/daf/SPAIcom/Word/strategy.doc
9. Stability Pact. *Fight against Organised Crime*, (Regional conference, Bucharest, 25 and 26 October, 2001).
10. See http://www.unece.org/seci/.
11. SECI *Agreement on Cooperation to Prevent and Combat Trans-border Crime*, available at http://www.unece.org/seci/crime/agreemnt.htm.
12. Charter of the Organisation and Operation of the Southeast European Initiative Regional Centre (SECI Centre) for the Combating of Trans-border Crime, <http://www.unece.org/seci/crime/charter.htm> (12 April 2002).
13. For more information see http://www.stabilitypact.org.
14. http://www.pims.org.
15. In May 1999, at a meeting of the deputy-ministers of defence of SEDM countries Bulgaria put forward a proposal to create a Crisis Information Network. A Concept of Operation of the Network was approved by the ministers of defence of SEDM countries during their meeting in Bucharest, Romania, in December 1999.
16. Charles R. Myer, “C4ISR Architectural Frameworks in Coalition Environments,” in *Information & Security* 5,

(2000): 60-72, <http://www.isn.ethz.ch/onlinepubli/publihouse/infosecurity/volume_5/a3/a3_index.htm> (12 April 2002).

PETYA DIMITROVA was born in 1975 in Sofia. She holds a Master degree in International Relations from the Faculty of Law of St. Kliment Ohridski Sofia University. She is a senior expert at the Defence Policy department of the Defence Policy and Planning Directorate of the Bulgarian Ministry of Defence. Her area of interest covers issues like European security dimensions, decision-making and strategy implementation, management, etc. *E-mail*: bruja17@yahoo.com.

BACK TO TOP

Networking South East Europe in Managing Non-traditional Challenges

Petya Dimitrova

Keywords: cooperative security, common challenges, regional response, SEECAP, SEDM, Stability Pact for South East Europe

Abstract: South Eastern Europe's delicate security environment has been a challenge in itself for over a decade now. However, positive developments are being underway as well. 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 openness and transparency, as well as joint decision-making and practical cooperation. For the reason of complementarity, a few regional initiatives have been selected to illustrate the extending and expanding networking of willing and able states in South Eastern Europe that have gradually started to transform traditionally negative perceptions and attitudes.

full text

Author: **Todor Tagarev**
Title: **Developing South East European Cooperative Crisis Management Capacity**
Year of issuance: **2003**
Issue: **Information & Security. Volume 10, 2003, pages 73 - 83**
Hard copy: **ISSN 1311-1493**

DEVELOPING SOUTH EAST EUROPEAN COOPERATIVE CRISIS MANAGEMENT CAPACITY[1]

Todor TAGAREV

Table Of Contents:

Background
Proposal
The way foreword
Definitions of Cooperative Crisis Management Capability/ Capacity
Existing regional initiatives related to crisis management
Approach
Mechanics
Potential Support and Beneficiaries
Conclusion
Notes

Background

For a century the Balkans were seen as the powder keg of Europe. Transformations after the end of the Cold War once again triggered violence. Throughout the 1990s, the region drew in considerable crisis management resources benefiting from the efforts of the international community. Practically, the potential for regional security response has not been utilized.

Now, with the launch of the Multinational Peace Force South-East Europe (SEE), the Stability Pact and the encouraging developments in the Federal Republic of Yugoslavia, for the first time in history all SEE countries demonstrated their willingness to cooperate in conflict prevention and crisis management and to take responsibility for security and stability in their own home. However, given cultural diversity, resource constraints, and lack of market experience in some of the countries, the challenge is in their ability to do so.

SEE countries proved their willingness to cooperate through promotion of a number of political and

diplomatic initiatives in various frameworks. The success of the SEE Defence Ministerial (SEDM) process is just one example.[2] The military cooperation quickly expanded to encompass various security and crisis management initiatives.[3] One remarkable achievement is the common assessment of regional security challenges and opportunities in the SEECAP paper [4] setting the stage for comprehensive security cooperation.

However, the cooperative implementation of means for crisis management is often hindered by lack of adequate organisation and appropriate technology, as well as other interoperability challenges. For example, the delay in announcing the operational readiness of the SEE Brigade (SEEBRIG [5]) is caused mostly by lack of common field communications and information system. In other words, a solid political and military effort hangs on a technology need to provide interoperability among national forces contributed to SEEBRIG. That means a lack (or very limited efficiency) of capability to employ operationally an otherwise excellent tool.

Proposal

Currently, given political will and common understanding, the challenge is to build and sustain cooperative capabilities to deal with crises of various nature while efficiently using limited financial and other resources. Most of the capabilities may be nationally owned, but will be prepared and available to deal with crisis in the whole region of South East Europe.

The proposal herein is to launch a *SEE Cooperative Crisis Management Initiative* that would implement a regional *Strategy for Development of SEE Cooperative Crisis Management Capacity*. This strategy shall be "regionally-owned." Once agreed by the SEE states, it may serve as indication for priorities in utilising national and international funding, i.e., funding through the Stability Pact for South East Europe.

This SEE initiative will contribute to the European Union capabilities to perform the "Petersberg Tasks."[6] Adding to the military cooperation among SEE countries, it will allow to develop and sustain, in a coordinated manner, [7] regional cooperative capabilities to meet risks and challenges of [8]:

- Natural disasters including earthquakes, floods, avalanches, volcanic eruptions, massive forest fires and landslides, severe storms and draught, and extreme temperatures;
- Technological disasters, industrial accidents and pollution, i.e., nuclear reactor incident, hazardous material spill, etc.;
- Air crashes, railway accidents and ship wrecks;
- Pandemics;
- Pest infestations;
- Massive refugee flows, particularly as a consequence of armed conflicts and violence;

- Insufficient early warning.

The initiative shall support, to the extent practical, SEE cooperation aimed at preventing risks and dealing with cases of :

- Organised crime, in particular money laundering, illegal trafficking of arms, narcotics, human beings, components and materials for weapons of mass destruction. Links with corruption and finance for terrorist and illegal armed groups activities;

- Destabilising accumulation and illegal transfer of conventional weapons including small arms and light weapons and ammunition;

- Non-observance or circumvention of arms control, disarmament and non-proliferation obligations;

- Illegal migration, especially if connected with organized crime;

- Corruption.

Logic of the proposal

The cooperative approach to crisis management would allow to lower risks to security and stability in South East Europe and to promote common political standards, or "code of conduct," i.e., in devising and implementing strategy and doctrine in an open transparent manner. Broader cooperation in crisis management will contribute to building confidence and trust among governments and people in SEE. It will facilitate rapid dissemination of best practice and the realisation of economy of scale both through intergovernmental cooperation and cooperation in utilising military and civilian crisis management resources.

The way foreword

Definitions of Cooperative Crisis Management Capability/ Capacity

For the purposes of this paper *Cooperative Crisis Management Capability* (CCMC) may be defined as

> *availability* of national and/or multinational *assets* (organised people /formations/, equipment and infrastructure, including crisis and emergency management /command and control/ infrastructure)
>
> with the *ability* (arrangements are in-place; plans are available, procedures are known; people/formations are trained) to *prevent*, *counter* and *manage the consequences* of *a crisis*.

CCM Capability is *relative*. It is assessed against a crisis scenario with a given scope and intensity.

The regional Cooperative Crisis Management *Capacity* may be defined as

> capacity to apply regional CCM capabilities to prevent, counter and manage the consequences in a set of concurrent, overlapping or sequential crises of various nature.

In a broader understanding a "regional" CCM capacity would account for arrangements and assets to call for and utilise out-of-region support.[9]

Existing regional initiatives related to crisis management

The development of cooperative crisis management capacity will build substantially on the existing military cooperation and the cooperation in emergency management. The regional military cooperation is established largely in the framework of the South Eastern Defence Ministerial (SEDM) through the Multinational Peace Force South East Europe (MPFSEE). MPFSEE currently includes one mechanised brigade—SEEBRIG—with units from seven countries and a battalion-sized Engineering Task Force.

The cooperation in emergency management evolves within two main initiatives. The Disaster Preparedness and Prevention Initiative (DPPI) in the Stability Pact already produced a framework document, known as "Gorizia Document"[10] that served to provide strategy outline for common action in seven areas: Information sharing and networking; Standardisation and harmonisation, Preparedness and planning exercises, Cooperative development, conduct and evaluation of disaster management training events; Public awareness and media relations; Strengthening local structures; and Border crossing procedures. Furthermore, the initiative already resulted in a joint military-civil fire fighting exercise "Taming the Dragon – Dalmatia 2002" in Croatia, 22-24 May 2002.[11]

The second major initiative led to the establishment of a Civil-Military Emergency Planning (CMEP) Council for South East Europe.[12] The Council is intended to coordinate efforts in all phases of the disaster management cycle: mitigation, prevention, planning, response and reconstruction. The areas of cooperation include: development of processes and means for practical regional cooperation in disaster management; development of improved coordination methods for all phases of the disaster management cycle; development of regional risk assessment; development of recommended response plans for the greatest risks; development of standard operating procedures and promotion of interoperability; planning, organisation and conduct of exercises and training. In December 2002, CMEP conducted the first large scale exercise using distributed simulation technologies. Greece and the United States were co-hosts of the exercise, based on a scenario involving large earthquake.

Another related project is a follow-up of SEECAP aiming at exchange of political, military and other early warning, conflict prevention, and crisis management information. Known by the abbreviation SEECHANGE, the project has already progressed with the adoption of a Concept Paper[13]. This project is implemented in the framework of the NATO affiliated South East Europe Security Cooperation Steering Group (SEEGROUP).

In South East Europe, there is a recognised need for close civil-military cooperation in crisis management. The implementation of this understanding is facilitated technologically through the US-sponsored project to establish 'National Military Command Centres' (NMCC) in several countries in South East Europe. The NMCC Concept of Operations accounts for the need to assure effective cooperation between civilians and the military in managing variety of crisis and emergency situations.[14]

In a broader understanding of crisis management, the development of CCM capacity shall account for initiatives aimed at countering arms proliferation, anti-corruption initiatives and initiatives that involve cooperative approach to law enforcement.

Certainly, a strategy for development of SEE cooperative crisis management capacity shall account for related sub-regional initiatives or initiatives in overlapping regions, i.e., BlackSeaFor.[15]

Compared to existing initiatives, this proposal adds in scope and level of coordination and cooperation among SEE countries. First, it covers emergency management, disaster preparedness and prevention, expanding the scope to bridge 'civilian emergency management' to the Petersberg tasks and to link more closely civilian structures and the military. It also has the potential to coordinate emergency management to particular aspects of law enforcement. Secondly, while existing initiatives aim to improve planning and preparedness to use *existing* national resources, we envision coordinated, and later – joint, *development* of crisis management capabilities. That shall include coordinated organisational development, joint procurement of the necessary technology and coordinated or joint development of the supporting information infrastructure. Ultimately, it may lead to joint (regional) ownership of crisis management infrastructure and other assets.

Approach

The implementation of the proposal requires clear understanding of objectives and cohesive regional strategy. Efforts need to be well coordinated, avoiding duplication of efforts and guaranteeing increasing levels of interoperability.

- Major components of the approach will aim to achieve:

  Compatibility of conceptualisation and normative regulation of "crisis management."

  For example Bulgaria, with participation of non-governmental organisations, is currently debating a new Concept and a Law for Crisis Management. Experience shows that even in a single country it is not easy to delineate and define in strict legislative terms 'hard' and 'soft' security threats and, respectively, responsibilities of various ministries and state agencies.

  This component is essential to provide commonality of terminology and procedures, standardisation of reporting methods, and overall interoperability of crisis management assets.

- Agreement on procedures for crisis management.

Existing agreements on using the Multinational Peace Force in South East Europe, as well as the progress within DPPI and the CMEP initiative provide a sound basis for elaboration of more general procedures for crisis management.

- Joint or, at least, coordinated procurement.

  Equipment, systems for command and control, infrastructure, etc., shall be developed jointly in well-coordinated manner to provide for: (1) interoperability or, ideally, commonality of equipment, and (2) efficient use of resources both for acquisition (up-front costs) and for life-cycle support.

  As a side effect, joint procurement initiatives may facilitate economic cooperation in SEE.

- Organisational arrangements

  Essential is the establishment of a permanent regional organisation—*Regional Crisis Management Centre*—tasked to coordinate development and implementation of SEE cooperative crisis management capabilities. This Centre may be established on the premises of the SEEBRIG HQ in Plovdiv, Bulgaria, after the HQ transfers to Constanza, Romania, in the autumn of 2003.

  The Regional Crisis Management Centre shall have a permanently assigned staff representing the participating countries. The Centre will serve as a focal point for work coordination. It will provide readily available support to decision makers during crises. The staff will monitor developments in SEE and issue crisis early warning. The Centre will serve as repository for crisis management plans and other information related to status of assets, capability development plans (programmes) and projects, development and support for implementation of crisis management training and exercises, etc. From a technical point of view, one obvious role for the Centre is to serve as developer and holder of the Joint Technical Architecture[16] for the SEE Cooperative Crisis Management Initiative.

Mechanics

The implementation of this proposal would require performing the following steps:

- Agree, broadly, on the scope of a potential *SEE Cooperative Crisis Management Initiative*;
- Agree on the terminology used;
- Create a data bank of existing national and regional crisis management capabilities;

- Create a data bank of regional and major national initiatives, as well as initiatives for overlapping regions, for development of crisis management capabilities;

- Model regional crisis management in order to:

  - Identify gaps in existing and planned crisis management capabilities in SEE;

  - Compare organisational designs and 'command' arrangements;

  - Assess acquisition proposals and initiatives;

- Devise and discuss, prior to the launch of the initiative, a *Strategy for Development of SEE Cooperative Crisis Management Capacity*.

All these steps might be combined in one *feasibility study*. A parallel activity would be needed in order to raise awareness of policymakers and practitioners of the utility of the proposed initiative and the required comprehensiveness of the approach, to cover normative regulation, procedures, organisation, training and technology insertion.

The implementation of the Strategy would imply advancement of a common, or at least coordinated policy for consistent organizational development and technology acquisition. This will include policies for *coordinated*, and in the future – *joint procurement* of technologies and systems for information collection, situational awareness, distributed decision making, communications, command and control in managing multinational multi-agency crisis prevention and response to crises of armed nature, natural disasters, industrial accidents, and humanitarian crises.

It shall account for potential organisational and technology solutions to law enforcement tasks, such as prevention of and counteraction to arms proliferation; illegal trafficking of people, drugs and goods; money laundering, and terrorism.

Of particular interest will be the areas requiring advanced technology implementation in close civil-military cooperation, such as emergency management, control of maritime and river traffic, and coastal zone management. Furthermore, advanced IT, when implemented in a regionally coordinated manner, has the potential to contribute to organizational development plans (development of multinational crisis management formations, civil and civil-military emergency resource planning, disaster preparedness, networked capabilities to fight organized crime, etc.; cooperative command arrangements for conflict prevention and crisis response; common early warning, situational awareness, consultations and distributed decision-making, and management of multi-national multi-agency crisis response.

Thus, technology insertion and development of infrastructure will be an important component of the strategy. However, knowing that technology that is not integrated into crisis management and response systems will not be effectively used during the response,[17] the most important practical result will be the increase of *coherency* of organisational and technological developments of

cooperative crisis prevention and crisis management capabilities.

Potential Support and Beneficiaries

Several on-going initiatives may contribute substantially to the one proposed herein. Main among them are the EU-sponsored Stability Pact for South Eastern Europe, in particular its Working Table 3 [18] and the NATO's South East Europe Initiative and the related South East Europe Security Cooperation Steering Group (SEEGROUP)[19].

The countries in South East Europe are the obvious beneficiaries from the implementation of this proposal. International organisations and donor countries, however, will also benefit from it, since it will allow for more efficient spending of limited resources while building *regional capacity* to deal with the problems of SEE. No less important is that the region itself will define priority needs for cooperative crisis management capabilities. Sound foundation for that is the common regional assessment of security threats and challenges in the SEECAP paper and the process for updating it.

Conclusion

Cooperative approaches to security in South East Europe are strongly encouraged by international organisations. The need for cooperation is also well understood by a number of governments and non-governmental think tanks.

Certain preconditions for such cooperation are already in place. Psychologically, the formation of a common brigade consisting of military units of most nations in SEE, as well as the common assessment of the security challenges, already made a breakthrough. Politically, there is a will to cooperate not only in crisis management, but also in broader security initiatives. Financially, regional resources are limited; however, adding outside assistance, they would allow sizable cooperative development of crisis management capacity.

The main obstacle is in the *lack of in-region organisational capacity* to deal with a problem of such complexity. Furthermore, there is no common understanding of ‘crisis management,’ and the procedures for procurement differ widely among SEE countries. We assume, that there is no instance when countries in the region themselves have managed common funds to acquire equipment under market conditions.

Fortunately, none of these obstacles is insurmountable. Following clear objectives, the implementation of the proposal herein will provide the necessary organisational capacity to guarantee efficient use of resources in SEE, including outside assistance. Thus, it will also increase the credibility of regional initiatives to provide for secure and prosperous future of South East Europe – part of the unified European continent.

Notes:

1. The first version of this paper was presented in May 2002 at the ESCADA meeting in Sofia. The paper was improved benefiting from the Sofia discussion. Improved version was discussed during the ESCADA meeting in Portoroz, Slovenia, in October 2002. For details on the ESCADA (Extending Security Co-operation and Defence Arrangements) project and recommendations the reader may refer to *Security and Defence in South-Eastern Europe*, Harmonie Papers 16 (Groningen, The Netherlands: Centre for European Secxurity Studies, March 2003).

2. For more information see Ognyan Minchev, Valeri Ratchev and Marin Lessenski, eds., *Bulgaria for NATO 2002* (Sofia: Institute for International and Regional Studies, 2002); Todor Tagarev, "Bulgarian Armed Forces and National Security Policy: Shaping the Security Environment in South East Europe," in *Almost NATO: Partners and Players in Central and Eastern European Security*, ed. Charles Krupnick (Lanham, Md.: Rowman & Littlefield, 2003), pp. 119-155. We are not aware of the existence of Web site regularly informing on SEDM activities. Initiatives during the Romanian Chairmanship of the CEDM Political-Military Steering Committee are presented at http://www.mapn.ro/english/news/newsletters/eng4.htm.

3. See the article by Petya Dimitrova in the current volume.

4. South East Europe Common Assessment Paper on Regional Security Challenges and Opportunities (SEECAP), adopted May 2001, Budapest, Hungary. <http://www.nato.int/docu/comm/2001/0105-bdp/d010530b.htm> (5 Nov 2001).

5. SEEBRIG (The South East European Brigade) is the main military formation of the Multinational Peace Force South East Europe. The Headquarter of this combined arms brigade is currently stationed in Plovdiv, Bulgaria, and is scheduled to move to Romania in the fall of 2003.

6. Humanitarian and rescue operations, peace-keeping and crisis management, defined in the Petersberg Declaration of 19 June 1992 as a pivotal element in developing the Western European Union (WEU) as the defence arm of the EU. The Treaty of Amsterdam has specifically incorporated these "Petersberg tasks" in the new Article 17 of the EU Treaty. See *Petersberg Declaration (Petersberg tasks)*, <http://europa.eu.int/scadplus/leg/en/cig/g4000p.htm> (12 June 2002).

7. According to General (Ret.) Carlo Jean, "Greater coordination of the effort of the international community is absolutely necessary." Presentation at the ESCADA Planning Meeting (Groningen, The Netherlands, 19 April 2002).

8. List adapted from SEECAP, the Agreement on the Establishment of the Civil-Military Emergency Planning Council for Southeastern Europe and the Concept of Operations for the National Military Command Centres (NMCC) project. No attempt to prioritise was made.

9. Analogous to the NATO concept of *Host-Nation Support* (HNS) capabilities.

10. *The Gorizia Document*, Regional Report of the DPPI Operational Team (Special Co-ordinator of the Stability Pact for South Eastern Europe, Disaster Preparedness and Prevention Initiative (DPPI), May 2001).

11. "Joint Efforts in Disaster Relief," *Newsletter*, Special Co-ordinator of the Stability Pact for South Eastern Europe, Issue 14 (28 June 2002): 8.

12. For the evolution of the CMEP initiative the reader may refer to A. Martin Lidy, M. Michele Cecil, Edwin J. Pechous, and Edward F. Smith, *Civil-Military Emergency Planning Council*, Bucharest Conference Proceedings (Arlington, VA: Institute for Defense Analysis, 28 July 2000). The Agreement on the Establishment of the Civil-Military Emergency Planning Council for Southeastern Europe was signed in Sofia on 3 April 2001.

13. Chair's Progress Report of the Work in the First Half of 2002 - South East Europe Security Cooperation Steering Group (SEEGROUP), <http://www.nato.int/pfp/romania/seegroupIhalf.htm> (21 August 2002).

14. For details the reader may refer also to Nikolay Petrov, “National Military Command Center – From Idea to Implementation,” *Information & Security: An International Journal* 6 (2001): 69-81. <http://www.isn.ethz.ch/onlinepubli/publihouse/infosecurity/volume_6/a2/a2_index.htm> (12 April 2002).

15. Refer to the article by the Chief of Staff of the Bulgarian Navy Peter Petrov, “Towards Creation of a Unified Information System of the Navies of the Black Sea Countries,” *Information & Security: An International Journal* 6 (2001): 69-81. <http://www.isn.ethz.ch/onlinepubli/publihouse/infosecurity/volume_6/a4/a4_index.htm> (12 April 2002).

16. See for example *C4ISR Architecture Framework*, Version 2.0 (Washington, DC: C4ISR Architecture Working Group, December 1997).

17. John R. Harrald, *Future of Emergency Management in the US following Sept. 11 Terror Attacks* (Institute for Crisis, Disaster, and Risk Management, The George Washington University, October 2001), <http://www.seas.gwu.edu/~icdm/Oct1.htm> (12 Nov 2001).

18. Other Stability activities, such as the *Anti Corruption Initiative* may support this proposal in specific areas. Other activities within Working Table 2 will be of interest, i.e., infrastructure development, e-SEEurope, etc.

19. For details refer to James Appathurai, “NATO's evolving partnerships: Promoting regional security,” *NATO Review* 49, no. 3 (Autumn 2001): 13-15.

TODOR TAGAREV is Director Programmes of the Centre for National Security and Defence Research at the Bulgarian Academy of Sciences. He was the first Director of the Defence Planning Directorate of the Bulgarian Ministry of Defence since its establishment in early 1999. Since May 2001 until late 2001, he served as Director for Armaments Policy and National Armaments Director. He graduated from the Bulgarian Air Force Academy in 1982 with M.Sc. degree in electrical engineering and received a PhD degree in systems and control from Zhukovsky Air Force Engineering Academy, Moscow, in 1989. Dr. Tagarev is a 1994 Distinguished Graduate of the US Air Command and Staff College at Maxwell Air Force Base, Ala., and a 1994 Distinguished Young AFCEAn. He is Editor of *Information & Security: An International Journal* <http://infosec.hit.bg>. Dr. Tagarev specialises in the integration of information technology with security and defence policy, system analysis, computer modelling and prediction of complex processes. *E-mail*: tagarev@space.bas.bg.

BACK TO TOP

Developing South East European Cooperative Crisis Management Capacity

Todor Tagarev

Keywords: SEE security cooperation, joint capabilities, cooperative procurement, emergency management, Petersberg tasks, crisis management architecture

Abstract: In this paper we propose and reason for launching SEE Cooperative Crisis Management Initiative aimed at developing sustainable regional Cooperative Crisis Management Capacity, seen as a set of Cooperative Crisis Management Capabilities to deal with the most probable crises in SEE. The proposal is based on critical assessment of the achievements of related security cooperation in South East Europe. The paper elaborates the purpose, the advantages and the mechanics of implementation of the proposal. Key to its advance is to define the scope so that the initiative adds to, coordinates and streamlines ongoing efforts without considerable duplication. Essential is the establishment of a Regional Crisis Management Centre, i.e., on the premises of the SEEBRIG HQ in Plovdiv, Bulgaria, after the HQ transfers to Romania in 2003.

full text

Author: **Stoyan Avramov**
Title: **Integrating COTS Technologies into a Scalable Mobile Emergency Command Post**
Year of issuance: **2003**
Issue: **Information & Security. Volume 10, 2003, pages 87-96**
Hard copy: **ISSN 1311-1493**

INTEGRATING COTS TECHNOLOGIES INTO A SCALABLE MOBILE EMERGENCY COMMAND POST

Stoyan AVRAMOV

Table Of Contents:

Introduction
COTS Integration and Demonstration Concept
Basic Operational Features
System Architecture Issues
System Communications Module
Basic Communications Module
Universal Communications Module
Technical Architecture
Information Assurance Issues
Notes

Introduction

In terms of emergency command and control, the September 11 terrorist attacks against the United States provide a textbook example of the complexity of the task. A number of organizations needed to coordinate their activities while existing infrastructure elements and capabilities were lost. Timely response was critical. The life of first responders was at great risk.

Yet, this type of emergency situations is not necessarily limited to large-scale terrorist attacks. Nor is it limited to the United States. Although September 11 may be seen as extreme in intensity, the resulting emergency is neither unique nor did it pose extreme resource requirements. Earthquakes, floods, landslides, massive forest fires and other natural calamities, as well as man-made disasters may call for greater involvement of disaster relief assets in coordinated response of variety of national and international organizations.

Adequate response requires advance preparation of assets, emergency management plans, related infrastructure, and elaborate training.[1] In countries, transitioning to market economy and effective democratic governance, two additional factors call for adapting national emergency management arrangements[2]:

- Necessity for coordinated response of several organizations of the security sector [3] with (hopefully) complementing capabilities to counter new security threats; and
- Harsh financial restrictions.

These two factors, together with the set of interoperability requirements, call for extensive use of commercial-off-the-shelf (COTS) technologies in emergency command and control. This article describes an ongoing effort in developing and demonstrating the capabilities of COTS technologies, integrated to provide cost-effective on-site command and control in various emergencies [4]. Using our experience in military command and control and recent architecture development guidance,[5] we designed a Scalable Mobile Emergency Command Post in response to a structured definition of operational, system and technical requirements. The following sections of the paper 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. It 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.

One of the objectives is to test and demonstrate compatibility and interoperability of various communications and information COTS technologies and products, as well as opportunities for scaling of the provided emergency management set. During the exercise we shall test the applicability of COTS technologies to meet current and future requirements of governmental organizations such as the State Agency for Civil Protection, to fit in their concepts of operations and to provide interoperability with legacy systems and equipment. The demonstration is expected to prove that this is a cost-effective approach to providing basic communications and information services in all phases of emergency command and control, allowing also effective integration within national information and communications systems and infrastructure. One side effect is the display of opportunities to integrate products of a number of technology leaders, legacy and advanced systems into a complex emergency management system.

As a result of the demonstration during the exercise the research team, jointly with representatives of the Civil Protection Agency and other potential customers, shall be able to define requirements for procurement of a tailored mobile emergency management set, further development, concept experimentation and technology demonstrations.

COTS Integration and Demonstration Concept

A number of advanced commercially available communications and information technologies have been integrated in a *Mobile Emergency Management Command Post*. During emergencies it shall provide communications and information services to users from variety of governmental agencies and non-governmental

organizations in a cost-effective manner. It allows for integration within the existing communications and information environment adhering to both applications specific security regulations and general information assurance requirements.

The emergency management command post, presented on Figure 1, includes:

- One *System Communications Module* with
  - Dedicated workplace
  - Extended number of interfaces
  - Software for monitoring and diagnostics of system performance
- 3-4 *Basic Communications Modules*, each of them consisting of
  - Dedicated workplace
  - Standard set of interfaces
- 2-3 *Universal Communications Modules* with minimum number of interfaces

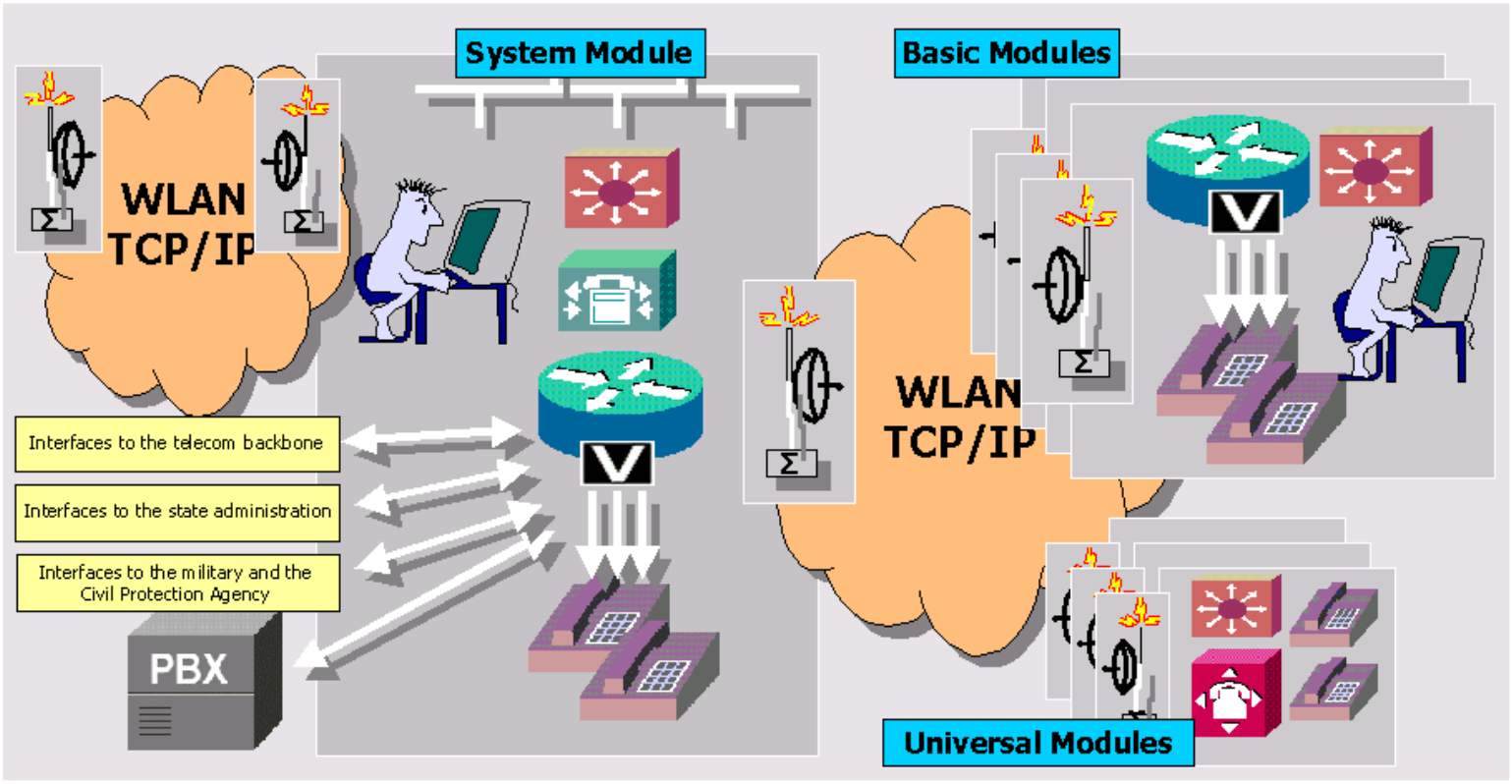


Figure 1: Structure of the mobile emergency command post

Basic Operational Features

This set of the emergency management system is intended to provide on-site command and control. It supports the work of an 'Emergency HQ' with three to five workplaces. It is mobile and may be quickly deployed in the field. Alternatively, the command post may be used in a fixed (stationary) version.

Furthermore, the command post may be embedded in a more complex C3 architecture or to interoperate with communications and information systems of various generations. It provides advanced interfaces to end user devices, sensors, users of information, and visualization tools. It is designed with sufficient reliability and ruggedized for high performance under weather and mechanical impacts in the field during various emergencies, operations other than war, etc.

System Architecture Issues

In mobile emergency management, the command post uses high-speed wireless communications in either ISM or licensed frequency bands. If necessary, it can be connected to the telecommunications backbone using SATCOM and/or VSAT. When the emergency management set is used in stationary conditions, digital and analogous dial-up and leased lines connections may be established. The set provides capabilities for simultaneous work in stationary and mobile communications networks.

System Communications Module

This is the main communications module in the emergency management command post. It provides monitoring and management of the whole communications infrastructure. This module provides also all necessary interfaces to the telecommunications backbone and other networks. One possible configuration of the

Systems Communications Module with some of the technical products used is represented on Figure 2. It is also possible to use other commercially available products.

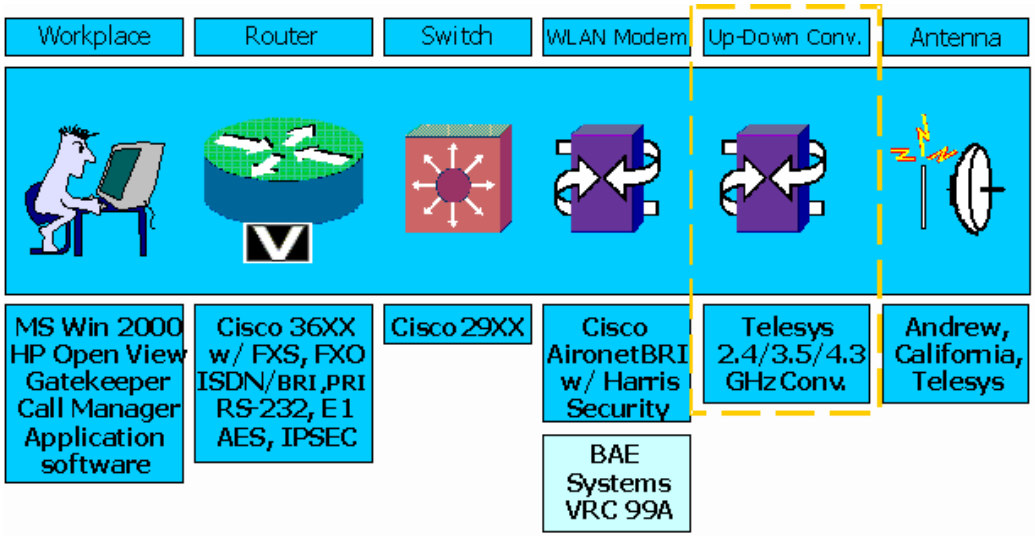


Figure 2: Configuration of the Systems Communications Module

The Systems Communications Module includes

- Workplace – PC with software for management and monitoring the performance of the whole communications infrastructure. It may be additionally used as server for system applications;
- Router – provides the main functions for routing within the system, as well as the main communications interfaces within the system and to other systems;
- Switch – provides effective network connectivity to other workplaces within the System Module;
- WLAN Radio Modem – This is the main device providing remote communications access with packet switching and routing in the radio environment. It has embedded capabilities to guarantee secure information exchange;
- UP-DOWN Converter – allows the implementation of commercially available tools designed for ISM frequency bands in licensed bands used by the respective agencies. It can provide the necessary power levels;
- Antenna - provides antennae systems with directional or omnidirectional pattern in the respective frequency band.

A typical number and type of communications interfaces required in the field are listed in the Table 1:

Table 1. Interfaces in the System Communications Module

Type	Number
For local workplaces and interfacing local systems	
Ethernet 10/100 Mbps	8
For local users of telephone services	
POTS/DTMF FXS	4
For local or remote interface to PSTN or PBX	
POTS/DTMF FX•	4
ISDN/BRI	2
ISDN/PRI (w/ voice)	1 (optional)
For remote access to the telecommunications backbone	
V.35 / 2 Mbps	1
For interfacing the military and other governmental agencies	
V.35 / 2 Mbps	1 (optional)
ISDN/PRI (w/ voice)	1 (optional)
POTS/DTMF FX•	2
POTS/DTMF FXS	2
Ethernet 10/100 Mbps	2

For interfacing Air Traffic Control Authorities and the Air Force	
V.35 (w/ ASTERIX-IP converter)	2

Basic Communications Module

The basic communications module in the emergency management set provides a workplace for the users in the system—the emergency responders—and the basic communications interfaces to the local systems. One possible configuration of this module with the implemented technical devices is presented on Figure 3.

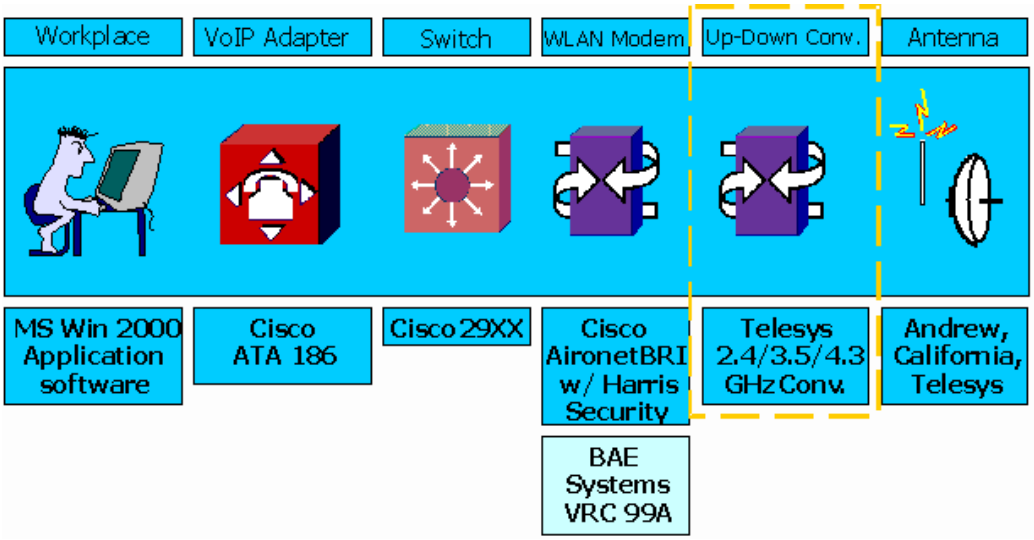


Figure 3: Configuration of the Basic Communications Module.

The module includes:

- Workplace – PC with user-oriented software applications;
- VoIP adapter providing the necessary voice communications;
- Switch providing effective network environment for other workplaces in the basic module;
- WLAN Radio Modem – This is the main device providing remote communications access with packet switching and routing in the radio environment. It has embedded capabilities to guarantee secure information exchange;
- UP-DOWN Converter – allows the implementation of commercially available tools designed for ISM frequency bands in licensed bands used by the respective agencies. It can provide the necessary power levels;
- Antenna - provides antennae systems with directional or omnidirectional pattern in the respective frequency band.

The following types and number of interfaces are required for implementation in field conditions:

- 8 Ethernet 10/100 Mbps interfaces for local workplaces and interfacing the local systems;
- 2 POTS/DTMF FXS interfaces for local users of telephone services.

Universal Communications Module

The universal communications module in the emergency management set provides the minimum number of services to single users in the system and the interface to a few local workplaces. A possible configuration of the universal module is presented on Figure 4. The figure also lists possible technical devices.

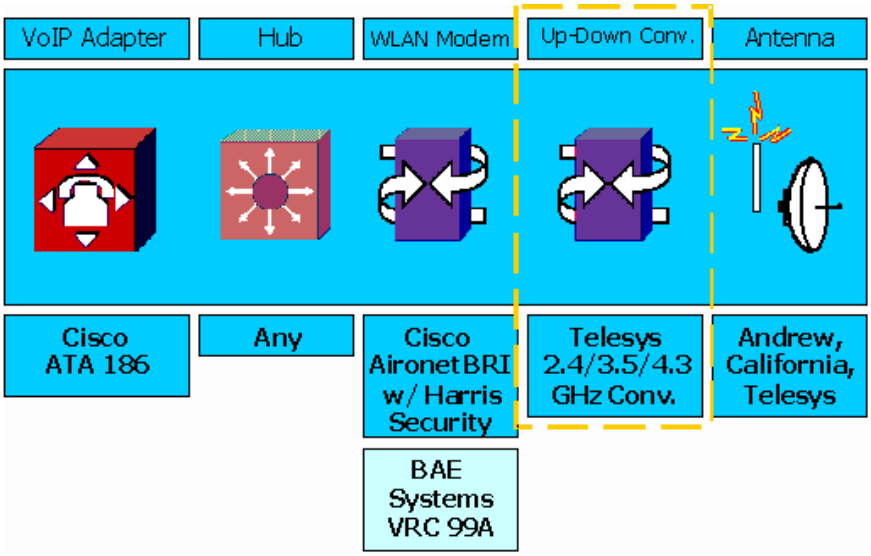


Figure 4: Configuration of the Universal Communications Module.

The module includes:

- VoIP adapter providing the necessary voice communications;
- Switch or HUB to provide effective network environment for other workplaces within the universal module;
- WLAN Radio Modem – This is the main device providing remote communications access with packet switching and routing in the radio environment. It has embedded capabilities to guarantee secure information exchange;
- UP-DOWN Converter – allows the implementation of commercially available tools designed for ISM frequency bands in licensed bands used by the respective agencies. It can provide the necessary power levels;
- Antenna - provides antennae systems with directional or omnidirectional pattern in the respective frequency band.

The following types and number of interfaces are required for implementation of universal modules in field conditions:

- 4 Ethernet 10/100 Mbps interfaces for local workplaces and interfacing the local systems;
- 2 POTS/DTMF FXS interfaces for local users of telephone services.

Technical Architecture

In order to standardize the technical devices within the emergency management set and to provide for its efficient and effective scaling, we developed the three types of modules following a set of technical requirements and standards.

Communications protocols and standards

For routing in the system	TCP/IP with QoS, PPP
For voice and voice teleconferencing	H.323, VoIP
For monitoring and management	SNMP
For information assurance	IPSEC, AES, WEP
For video surveillance and video teleconferencing	MPEG
For location, identification and management of moving objects	GPS, ASTERIX, NMEA-183

Communications interfaces

General purpose	Ethernet 10/100 Mbps
For phone and fax services	POTS/DTMF, ISDN BRI
For connectivity with sensors and local information sources	RS-232 / Up to 115 Kbps

Software environment

Servers and protocols	HTTP, FTP, POP3, SMTP
General purpose applications	MS Win2000, XP; MS Office
Preferred interface to applications	WEB based

Information Assurance Issues

Accounting for known security problems in the WLAN technology,[6] the research team is developing additional measures to be applied in specific scenarios, the sensitivity of the information exchange, and the requirements of particular customers. Generally, security in the Mobile Emergency Management Command Post is provided through cryptographic protection and through implementation of a set of additional software methods and tools for information assurance. The implementation of crypto devices is presented on Figure 5.

Among the additional software tools [7] there can be implemented commercially available tools for :

- Network monitoring & control;
- Intrusion detection;
- INFOSEC control;
- Crypto keys management;
- Call management;
- Voice recording;
- Data logging.

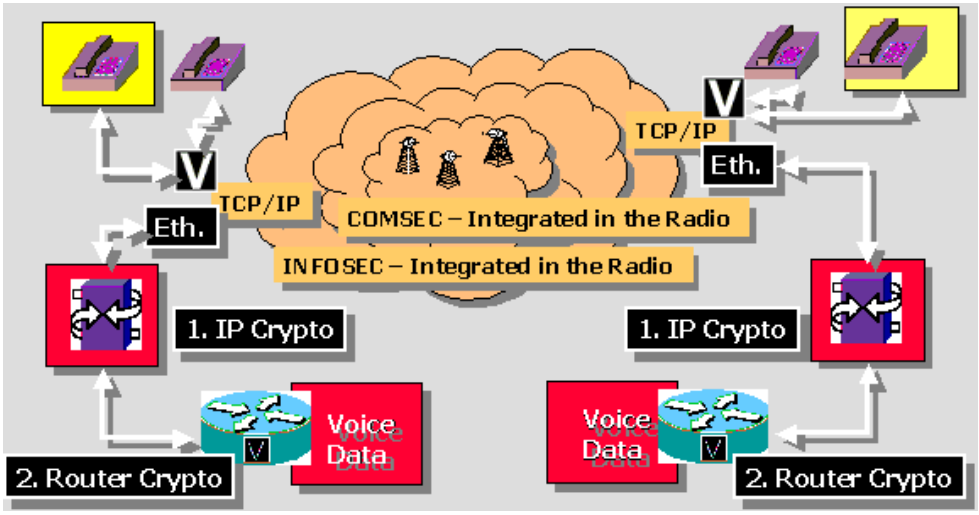


Figure 5: Possible protection of information in the emergency management set.

In sum, there are remaining challenges, i.e., to provide secure information exchange when a number of governmental agencies are involved. Nevertheless, the currently available mobile emergency management set provides adequate, cost-effective solution to the needs of first responders in variety of emergencies. Our efforts were successful through extensive use of advanced commercial-off-the-shelf technologies and systems.

Notes:

1. Andrew Borden, “Command and Control in Crisis Management,” *Information & Security* 10 (2003): 15-23.
2. Todor Tagarev, “From Military Capabilities to Capabilities of the Security Sector,” *Military Journal* 110, 2 (2003): 23-29.
3. Although not unique for the post-communist countries, this factor is listed here because of the impact of the rapid restructuring of individual organizations and the security sector as a whole. For definition of ‘security sector’ the reader may refer to the “Report of the Ad Hoc Working Group on Security Sector Reform to the Working Table III” (Budapest: Stability Pact 27 November 2001), <http://www.stabilitypact.org/stabilitypactcgi/catalog/view_file.cgi?prod_id=5664&prop_type=en>.
4. For an independent parallel development the reader is referred to Robert K. Ackerman, “Mobile Command Center Controls First Responses: Command and communications are no longer a military exclusive,” *SIGNAL* 56, 10 (June 2002): 37-40. Related R&D in Europe within the 6th Framework Programme follows several tracks, i.e., in the GMES thematic area to stimulate satellite-based information services by development of sensors, data and information models, and disaster management technologies, <http://fp6.cordis.lu/fp6/home.cfm>.
5. The Bulgarian Government has not issued elaborated guidance on developing C4ISR architectures. Therefore we currently adhere to *DoD Architecture Framework*, Volumes I, II and III, Version 2.1, First Draft (Washington, DC: DoD Architecture Framework Working Group, October 2000).
6. *Wireless LAN Security White Paper* (The Wireless LAN Alliance, August 1999), <http://www.wlana.com/resource/whitepaper.html> (20 March 2003); Torben Rune, *Wireless Local Area Networks* (30 September 1998), <http://www.netplan.dk/New/index.asp?ArticleID=2834> (20 March 2003); B. Justin Ross, *Containing the Wireless LAN Security Risk*

(Portland, OR: SANS InfoSec Reading Room, 4 November 2000), <http://www.sans.org/rr/wireless/wireless_LAN.php> (23 March 2003).

7. See also Andrej L•c, "Analysis of Spread Spectrum System Parameters for Design of Hidden Transmission," *Radioengineering* 4, 2 (June 1995); *Technical Considerations for Converging Data, Voice, and Video Networks*, White Paper (Cisco Systems, 3 July 2000), <http://www.cisco.com/warp/public/cc/so/neso/vvda/avvid/tecon_wp.htm> (23 March 2003).

STOYAN AVRAMOV is Head of the C4ISR Laboratory at the Space Research Institute of the Bulgarian Academy of Sciences. He graduated from the Bulgarian Air Force Academy in 1984 with a M.Sc. degree in Electronics Engineering and received a PhD degree in Radar Systems and Technologies from Zhukovsky Air Force Engineering Academy, Moscow, in 1991. Until 1995 he served in the Bulgarian Air Force in a variety of positions related to the development of automated C2 systems. Dr. Avramov is member of the Editorial Board of Information & Security: An International Journal. He specializes in technology integration, systems design and prototyping C4ISR systems. Address for Contacts: Space Research Institute – Plovdiv Branch, "Ivan Vazov" Str. 50 A, Plovdiv 4000, Bulgaria. E-mail: stav@digsys.bg .

BACK TO TOP

Integrating COTS Technologies into a Scalable Mobile Emergency Command Post

Stoyan Avramov

Keywords: C4ISR, emergency management, operational, system, technical architecture, information assurance, information security, drill, exercise, field command and control

Abstract: The article 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. It 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.

full text

Authors: **David Perme, Mark Whelan and William P. Loftus**
Title: **Achieving Interoperability of Command and Control Systems Using Translation Gateways**
Year of issuance: **2003**
Issue: **Information & Security. Volume 10, 2003, pages 97-104**
Hard copy: **ISSN 1311-1493**

ACHIEVING INTEROPERABILITY OF COMMAND AND CONTROL SYSTEMS USING TRANSLATION GATEWAYS[1]

David PERME, Mark WHELAN and William P. LOFTUS

Table Of Contents:

Introduction
Issue of Interoperability
Layered Translation Gateways
High-level Development Approach
Example
Summary
Notes

Issue of Interoperability

Over the last several decades, the military has greatly benefited from the increased knowledge and capabilities provided by using computerized command and control systems. As this use has expanded exponentially, so has the need to integrate these systems. The breadth of computing technology at the component, functional, and mission level has further complicated the issue of interoperability. By their nature, these disparate systems have varying levels of fidelity, granularity, quality and availability. The cost of establishing collaboration between these systems is typically high, and is complicated by differing organizational readiness levels, willingness, and technical ability to affect collaboration. The opportunity to enable interoperability, therefore, has great value, provided it can address these factors and more.

The need for translation of information and data to forms that are readable and interpretable has continuously challenged users of computer systems. Over time, the technologies employed to accomplish interoperability have evolved. Initially, and still prevalent today, one-to-one interfaces explicitly define how two systems interact. This type of approach works but does not scale. Other approaches, such as shared databases, common data repositories, and defined common standard messaging and interface formats, present solutions to some interoperability issues but are not

panaceas. Each approach is appropriate in given circumstances. Attempts to provide a single solution for all scenarios typically fall short due to technical challenges, adoption resistance, and funding availability.

The following sections present an approach that we have used successfully to simplify system communication and interoperability by a system-neutral layered gateway. The approach addresses the realities and complexities of the systems' environment and leverages domain expertise and emerging technologies including web technologies and expert systems.

Layered Translation Gateways

The best response to the issue of system interoperability is one that recognizes that successful systems are those that add value, minimize impact to existing systems, and can evolve over time. Our experience in integrating diverse systems (such as C4I systems) is that layered gateway architectures enable successful interoperability between systems, while isolating the impact of changes to any system. Value is derived by delivering to a system only that information that is used by that system. Moreover, layered translation gateways deliver and receive information to or from a system, in the format and medium native to that system. Additionally, a well designed layered architecture provides the opportunity to insulate layers from the impact of change (new systems, modification to existing systems, system retirement), thereby reducing the overall impact facilitating evolution of the gateway when change occurs.

At the core, system communication is translation. 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 gateway must be able to deal with all of these factors. The data, format, and medium translation challenges are relatively straightforward, discrete, and solvable transformations. The context translation challenge is more complex and involves the application of subject matter knowledge and expertise.

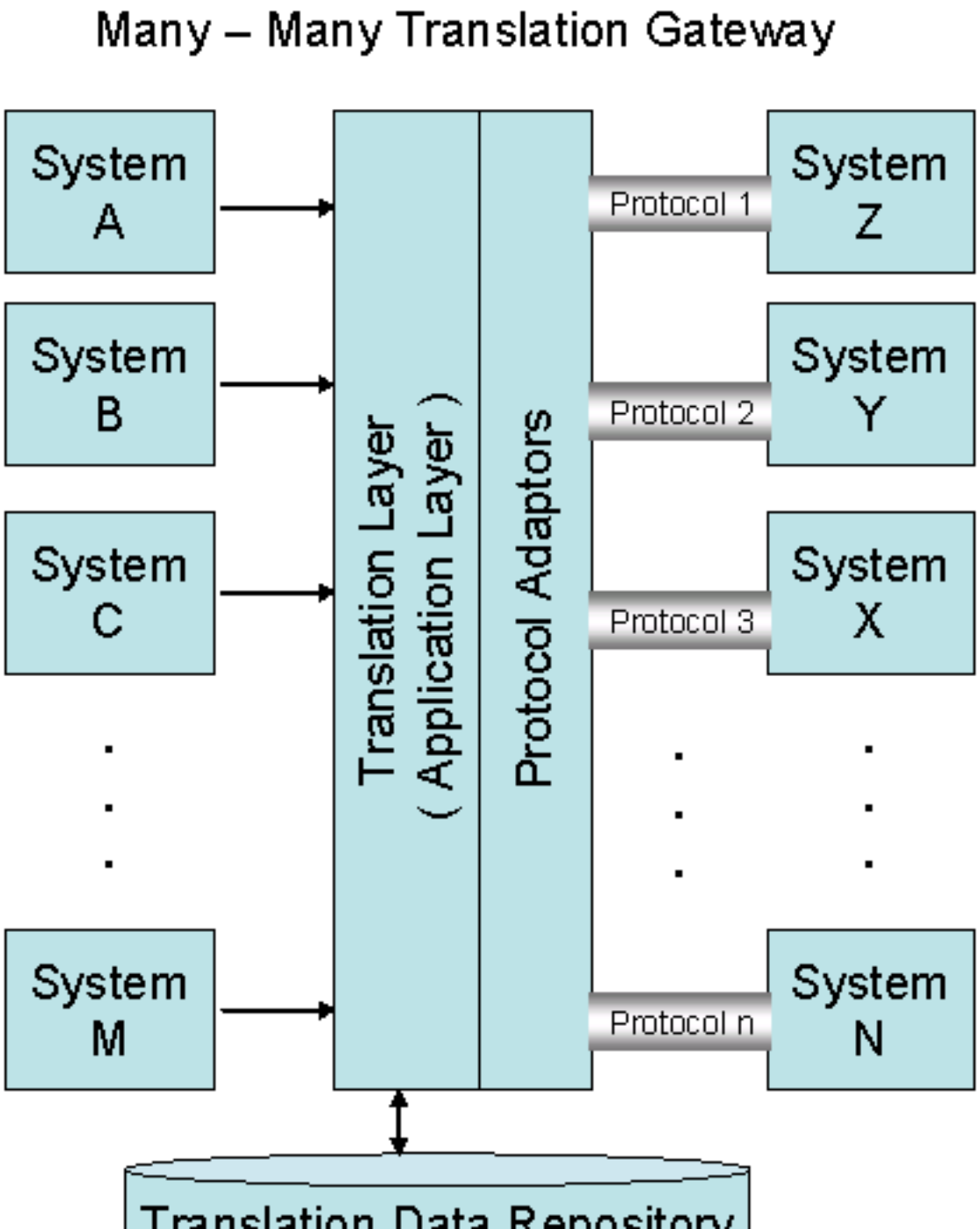
There are for basic components to flexible and adaptable gateway architectures:

1. System-neutral data interchange format
2. External systems interface layers
3. Translation layer
4. Intelligence layer

The first step is to define a *system-neutral, data interchange format*. By developing a common data model and schema, a gateway repository or data warehouse is created to facilitate the integration of disparate systems. Today, this data model is usually described by class diagrams and an XML schema. With a defined data model, appropriate programming interfaces to the data translation layer are easily

described and developed.

The focus of the *external systems interface layer* is the integration with various lower level architectures and protocols using reader-writers and adaptors. This approach provides the greatest flexibility for many-to-many system integrations as depicted in Figure 1. Within a system of systems, there exist three types of relationships: one-to-one, one-to-many, and many-to-many. A one-to-one relationship is often referred to as a point-to-point interface. Two systems talk to each other directly through a defined method or protocol. There is only one interface and changes to a system will result in changes to, at most, one interface. A one-to-many relationship describes multiple interfaces from a single system to a number (N) of other external systems. A change to the single system has the potential to affect N interfaces. A many-to-many relationship describes interfaces among and between a number of systems (N). Every system has an interface with every other system. While this provides the maximum potential for information exchange, it also creates [N*(N-1)]/2 interfaces. These relationships, however, can be normalized using the system-neutral data interchange format by reducing a many-to-many relationship to a one-to-many relationship. Each system needs to only read and write a single canonical format.



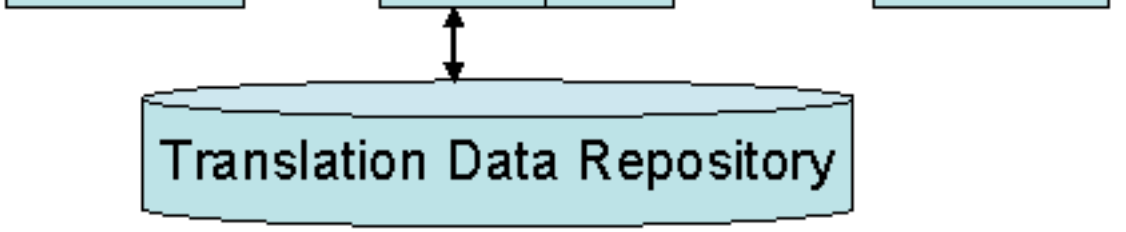


Figure 1: Translation Gateway

A *translation layer* transforms the data from the exporting systems into the common representation. The protocol adaptor extracts information from the repository, formats it, and communicates the information in the correct protocol to the receiving systems. Gestalt's experience in integrating real world C4I systems with simulation models has shown that a common representation becomes a forcing function for the information and is necessary to be able to translate the intent of the communication. The focus of a translation layer is to manage both data and business rules. Data is the information that is exchanged between systems. Business rules apply the logic of translation and transformation.

The data becomes the focus point for the incorporation of intelligent agent technology, via an *intelligence layer*. This layer reduces man-in-the-loop dependencies, enables smart system-wide decision making, and maintains meaningful communication. Often the business rules for the transformation and communication can be encapsulated into the intelligence layer. This approach allows the entire gateway translation to be applied to an enterprise, where the intelligent agents manage the variance between organizations.

High-level Development Approach

To develop a system-independent translation protocol, the data models and business rules of the target systems must be examined. In addition, current and future requirement sets for these systems should be understood. From this examination, a common system and data-neutral data schema can be designed and developed. The first step is to select an appropriate set of candidate systems that will form the basis for the development of a common system-neutral data schema. Typically, these systems are large in scale and produce complex message sets. There is a need to examine these message sets to identify key data elements and business rules associated with the data contained in the messages themselves. From this examination, a data population set from each of the systems can be derived. In this step, data discovery and cataloging is performed. The cataloging can be as simple as capturing the data population set in a spreadsheet. The key is to represent a system's data in a template form that retains information regarding its native schema while allowing the commonality of a template to begin the process of relating data elements from separate systems to each other.

Once all the data has been categorized from the candidate systems, the initial step of an object-oriented analysis can begin, that is, to build an initial Unified Modeling Language (UML) class diagram of the intended data-neutral data schema. The purpose of establishing a class diagram is to represent the class structures and hierarchies as well as the relationships between the class structures. The task of normalization is to then analyze the UML class diagram and promote like attributes into superclasses, compress the depth of the class structure wherever possible and test it against scenarios developed in the data discovery and cataloging phase.

Once the data to be communicated is well-understood the functions and duties of each layer in the architecture must be defined. The interfaces between the layers must also be defined and documented. Armed with the class diagram, the interface between the native system data format and the common data model can be defined and designed. In our experience, the best approach for reuse and interoperability is to use a loosely-coupled Application Programming Interface (API) approach as the interface into each layer. An API for the architectural layer performs the data transformation into the common data model. This API should allow for interfaces with all of the exporting systems that are selected and should be designed to allow for extensibility to future systems integration. XML has quickly gained traction in the commercial field as the document interchange description format for interoperability between systems. In the digital world today, there exist multiple XML vocabularies as well as software that perform the translation from one XML vocabulary to another. XML also brings along many tools, which enable XML documents to be processed with a minimum of programming effort. For these reasons, an XML schema should be derived from the class structure defined in the above steps.

The last step of a successful translation gateway is incorporation of business rules. This refers to the data fusion or disaggregating of incoming or outgoing data explicit for each integrated system. These rules must exist in a dedicated architectural component of a translator. This component is normally defined as an interface API between the normalized and the system-specific data representations. The success of a translator is dependent on the ease of configuring the business rules. Rule-based expert systems can be used to accomplish a flexible implementation of business rules. More specifically, commercially available open system standard software tools can be used. The use of these tools eliminates specific translation idiosyncrasies from the overall translator, and instead allows the inference engine and corresponding rules to ensure that the correct business rules are applied. These translations can be tested and easily adjusted or tuned to produce the desired outcomes. By isolating the business rules in a separate architectural layer, the impact of tuning on the translation software baseline is minimized.

Example

In the late 1990s, Gestalt personnel began the integration of the Air Operations Center (AOC) command and control systems to a suite of simulations. The AOC to Simulation Interface (ASI) initially integrated the Air Force’s Air Warfare Simulation, AWSIM, to the main AOC command and control system. Since that initial integration several command and control systems have been integrated including the Theater Battle Management Core System (TBMCS). ASI employs a layered architecture. Three primary layers constitute the ASI architecture. Two service layers, the Simulation Services Layer and the C4I Services Layer, handle the data capture and dissemination processes. These processes employ publish and subscribe mechanisms, and are compatible with both the Aggregate Level Simulation Protocol (ALSP) and the High Level Architecture (HLA) Runtime Infrastructure (RTI), and produce USMTF, TADIL, and XML messages. The third ASI architectural layer is the Translation Service Layer that provides the data translation services between the integrated systems using Gestalt’s proprietary Command and Control Data Interchange Format (C2DIF), a common, system neutral data representation that acts as the data and knowledge repository. The ASI system has been used at every major exercise (well over 70) since 1997 and has consistently demonstrated its versatility and viability. ASI’s layered architectural approach is

extensible, providing the capability for easily establishing interoperability between and among other existing legacy, joint, and coalition systems, as well as future systems. The ASI system has been extended beyond its original objectives via the integration with numerous simulation models including the National Air and Space Warfare Model (NASM), and the Navy's Research, Evaluation and System Analysis Simulation (RESA) and Joint Semi-Automated Forces (JSAF) models.

In 2002, the Gestalt team, sponsored by the Air Force Research Lab (AFRL), initiated the deployment of the Intelligent Mission Controller Node (IMCN) system. The IMCN system employs expert system technology using an intelligent agent framework. Concurrent with this development effort, the C2DIF data representation was expanded and matured to incorporate a more robust representation of the information elements associated with air missions and air warfare. The IMCN system is implemented to reason over any of the C2DIF data elements, providing the ability to develop intelligent agents that act across multiple air mission tasks. Using IMCN allows data to be represented devoid of any consideration for the business rules of any particular translation, knowing that the expert system can handle the business rules. A system prototype was first successfully used at Blue Flag '00-4 and at all major exercises since, including UFL '01.

The key success factor in the use of intelligent agents is to define them such that the complexity of the rule base does not outweigh the value gained by their use. Seeking a complex rule base to address all issues would have resulted in failure. However, Gestalt segmented intelligent agent scope and functionality, establishing reasonable rule sets that could be easily implemented and extremely impactful.

One example of an intelligent agent we have employed in this fashion is in air mission route planning which automates the ingress and egress of air missions, taking into account ground-based threats. Another example is in weaponeering, i.e., the automation of the process of pairing squadrons and airframes with weapons and targets.

Overall, ASI and IMCN have allowed the Air Force to integrate several command and control systems with a suite of simulators. The business results have been significant. ASI is a system that has reduced manning budgets by a factor of four, produced higher-quality execution, and lower future integration costs.

Summary

Translation gateways are a viable method for increasing interoperability between systems and decreasing the complexity of the integration. The development and use of system-neutral data schemas, coupled with translation services, enables the exponential power of many-to-many collaborative relationships for the linear cost and complexity of a one-to-many integration. This is achieved through an approach that incorporates sound design principles (rigorous analysis and object-oriented techniques), commercial best practices (Application Programming Interfaces and XML), and advanced technologies (intelligent agents).

Notes:

1. This article is based Technical Report 2002-CC-01-TG of Gestalt LLC. The company provides products and services to governments and Fortune 500 companies that address their collaboration and interoperation needs related to network-centric decision support systems including command and control, modeling and simulation, and enterprise business systems. Gestalt is an information technology firm that helps decision-makers increase their return on investment in existing systems through the application of state-of-the-art interoperation technologies.

DAVID PERME has twelve years experience in the executive management and operations of advanced software solution providers, beyond his ten years of experience in the Air Force. He holds a BS degree in Aerospace Engineering, Kent State University, and MS in Computer Science, Boston University. Mr. Perme has directed, supported, and evaluated hundreds of US Air Force, NATO, and Joint exercises and experiments world-wide. He was a principal lead and developer on one of the most successful interoperability programs in use today, the Aggregate Level Simulation Protocol (ALSP). His work and influence enabled the US Army's standard aggregate level simulator, the Corps Battle Simulation (CBS), to interoperate with the US Air Force's standard aggregate level simulation, the Air Warfare Simulation (AWSIM). The program, originally designed to be a prototype only, was so successful in execution that it has yet to be supplanted today. Mr. Perme was the designer and principal developer of the most successful C4I-to-simulation development effort to date. The program, initially begun as a Defense Modeling and Simulation Office effort termed *Project Real Warrior* (PRW), has evolved into the AOC Simulation Interface (ASI). Mr. Perme restructured and selectively re-engineered components of the C4I interface prototype, at the same time that the system was being used for major joint exercises. Currently, Mr. Perme is a Managing Director and Co-Founder of Gestalt, LLC. Contact address: 11 Federal Street, The Ops Building, Camden, NJ 08103, USA. Fax: 276-200-0541. *E-mail*: dperme@gestalt-llc.com.

MARK WHELAN has twenty years experience in information technology, systems integration, and web services. He holds BS in Computer Science, Penn State University, and MBA, St. Joseph's University, Philadelphia. His background includes various management positions in engineering and technology arenas serving the government and commercial sectors. Mr. Whelan combines strong experience in modeling and simulation, operational excellence through technology innovation, and strategic consulting. Prior to Gestalt, Mr. Whelan was Vice President, Operations, for Breakaway Solutions. Mr. Whelan led all professional services activities in the Mid-Atlantic region covering systems development and integration of web services for e-business, e-commerce, content management, and customer relationship management solutions. Currently, Mr. Whelan is the Managing Director of Gestalt. *E-mail*: mwhelan@gestalt-llc.com.

WILLIAM P. LOFTUS has seventeen years experience in the executive management and operations of advanced software solutions providers. He holds BS and MS in Computer Science, Villanova University, Villanova, PA. Currently he is the President, CEO, and Co-Founder of Gestalt, LLC. Previously, Mr. Loftus has served as the CEO of Breakaway Solutions, Chief Development Officer of the same company, founder and CEO of WPL Laboratories, manager of R&D at Unisys. Mr. Loftus has consulted numerous Fortune 500 and emerging companies as well as a number of investment bankers and venture capitalists. Mr. Loftus has co-authored numerous papers, IEEE standard P1430, and a best selling textbook, *Java Software Solutions*, currently used in over 400 universities world-wide and translated into Korean and Italian. He has also contributed to research in compiler theory, real-time software, software architectures, and interoperability. Mr. Loftus has received many awards including a Special Achievement Award from DARPA, recognition by the City of Philadelphia as one of the 40 most accomplished individuals under 40 years old in 1999, and was named as a finalist for the E&Y Entrepreneur of the Year award in 1999. *E-mail*: wloftus@gestalt-llc.com.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

Achieving Interoperability of Command and Control Systems Using Translation Gateways

David Perme, Mark Whelan and William P. Loftus

Keywords: C4I, simulation, proxy server, software architectures, context translation

Abstract: Over the last several decades, the military has greatly benefited from the increased knowledge and capabilities provided by using computerized command and control systems. As this use has expanded exponentially, so has the need to integrate these systems. The cost of establishing collaboration between these systems is typically high, and is complicated by differing organizational readiness levels, willingness, and technical ability to affect collaboration. The opportunity to enable interoperability, therefore, has great value, provided it can address these factors and more. In this paper, the authors present an approach to achieving interoperability through 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 gateway must be able to deal with all of these factors. The data, format, and medium translation challenges are relatively straightforward, discrete, and solvable transformations. The context translation challenge is more complex and involves the application of subject matter knowledge and expertise. 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.

full text

Author: **Information & Security**
Title: **Total Information Awareness (DARPA's Research Program)**
Year of issuance: **2003**
Issue: **Information & Security. Volume 10, 2003, pages 105-109**
Hard copy: **ISSN 1311-1493**

TOTAL INFORMATION AWARENESS (DARPA'S RESEARCH PROGRAM)

Information & Security

In response to September 11, 2001, the Defense Advanced Research Projects Agency (DARPA) created the Information Awareness Office (IAO) to research, develop, and demonstrate innovative information technologies to detect terrorist groups planning attacks against American citizens, anywhere in the world [1]. DARPA's mission is to research and demonstrate innovative technologies to solve national-level problems such as the grave terrorist threat. The mission of IAO is to imagine, develop, apply, integrate, demonstrate, and transition information technologies, components, and prototype closed-loop information systems that will counter asymmetric threats by achieving total information awareness in support of preemption, national security warning, and national security decision making.

The Total Information Awareness (TIA) is the main program of IAO beginning in fiscal year 2003. The stated goal of the program is to "revolutionize the ability of the United States to detect, classify and identify foreign terrorists – and decipher their plans – and thereby enable the U.S. to take timely action to successfully preempt and defeat terrorist acts."[2] The TIA objective is to create a counter-terrorism information system that: (1) increases information coverage and affords easy future scaling; (2) provides focused warnings within an hour after a triggering event occurs or an evidence threshold is passed; (3) can automatically queue analysts based on partial pattern matches in a patterns' database that covers 90 percent of all known terrorist attacks; and, (4) 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.

Figure 1 graphically presents the TIA vision. The strategy is to integrate appropriate technologies into a series of increasingly powerful prototype systems to be tested in operationally relevant environments, using real-time feedback to refine concepts of operation and performance requirements. The program is focusing on the development of architectures for a large-scale counter-terrorism database, for system elements associated with database population, and for integrating algorithms and mixed-initiative analytical tools; novel methods for populating the database from existing sources, create innovative new sources, and invent new algorithms for mining, combining, and refining information for subsequent inclusion into the database; revolutionary new models, algorithms, methods, tools, and techniques for analyzing and correlating information in the database to derive

actionable intelligence.

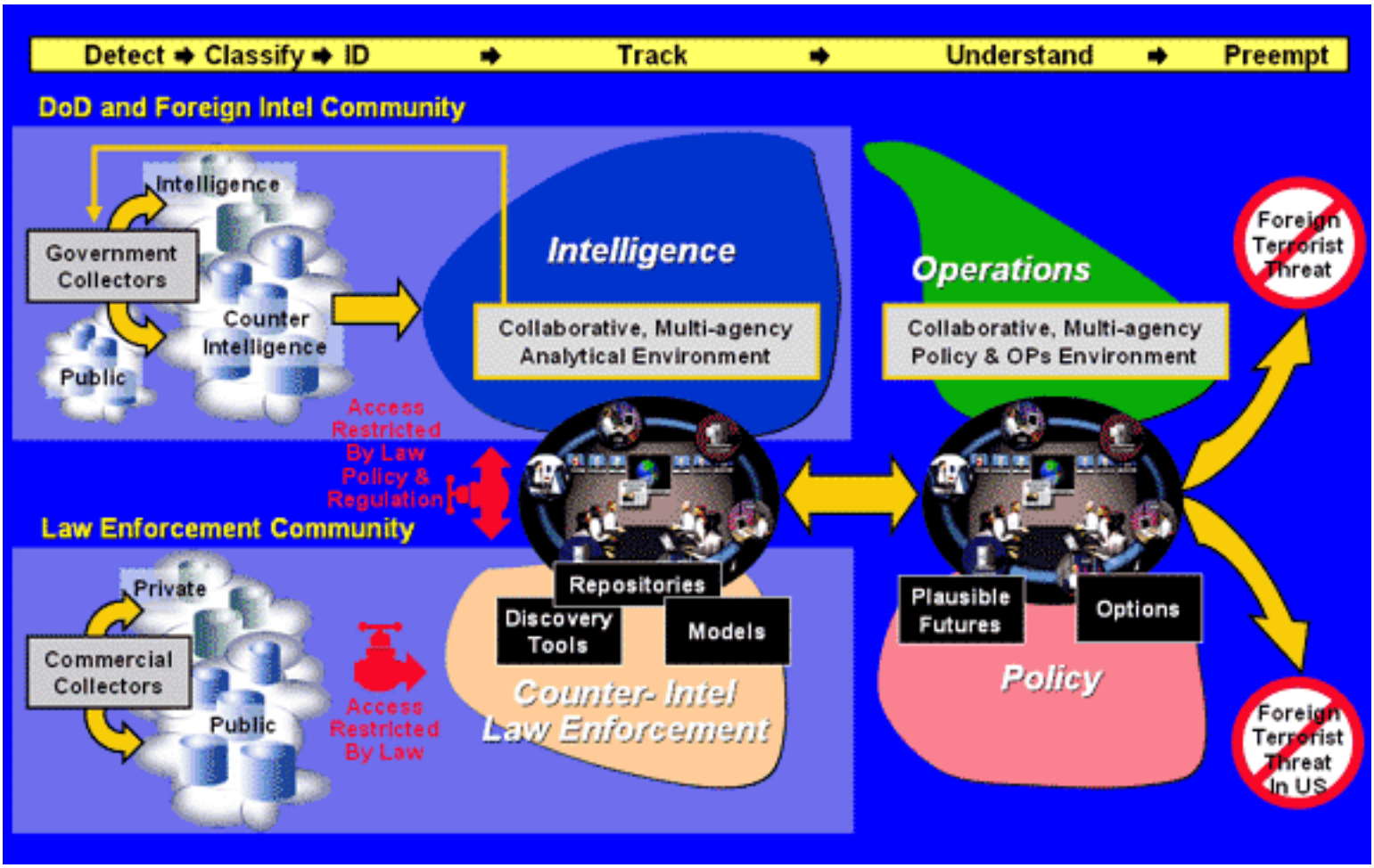


Figure 1: Overview of the Total Information Awareness system.

TIA is an overarching program paralleled by a dozen of technology programs.[3] Three of these deal with language processing challenges. The goal of the *Babylon* program is to develop rapid, two-way, natural language speech translation interfaces and platforms for the warfighter and shall be used in field environment. The *Translingual Information Detection, Extraction and Summarization* (*TIDES*) program is developing advanced language processing technology to enable English speakers to find and interpret critical information in multiple languages without requiring knowledge of those languages. The *Effective Affordable Reusable Speech-To-Text* (*EARS*) program is developing automatic speech-to-text transcription technology whose output is substantially richer and much more accurate than currently possible. The program seeks to develop a robust technology with an error rate of five to ten percent for broadcast and conversational speech.[4] The expectation is that machines will do a much better job of detecting, extracting, summarizing, and translating important information thus allowing humans to understand what was said by reading transcripts instead of listening to audio signals.

A related program called *Communicator* is expected to develop and demonstrate “dialogue interaction” technology that enables warfighters to talk with computers. The objective is to make information accessible on the battlefield or in command centers without ever having to touch a keyboard. The Communicator Platform will be wireless and mobile, and will function in a networked environment. Software enabling dialogue interaction will automatically focus on the context of a

dialogue to improve performance, and the system shall be capable of automatically adapting to new topics so conversation is natural and efficient.

A number of programs deal with information storage and processing challenges. The goal of the program *Genisys* is to produce technology enabling ultra-large, all-source information repositories. In order to predict, track, and preempt terrorist attacks, the U.S. requires a full-coverage database containing all information relevant to identifying potential foreign terrorists and possible supporters, their activities, prospective targets, and operational plans.

The *Evidence Extraction and Link Discovery* (*EELD*) program is developing technologies and tools for automated discovery, extraction and linking of sparse evidence contained in large amounts of classified and unclassified data sources. EELD is expected to provide detection capabilities to extract relevant data and relationships about people, organizations, and activities from message traffic and open source data. It will link items relating potential terrorist groups or scenarios, and learn patterns of different groups or scenarios to identify new organizations or emerging threats.

Project *Genoa*, which is being finalized, provides structured argumentation, decision-making and corporate memory to rapidly deal with and adjust to dynamic crisis management. It creates virtual collaborative environment for both analyst and policy making communities (Figure 2). The *Genoa II* program was launched in FY03. It will focus on developing information technology needed by teams of intelligence analysts and operations and policy personnel in attempting to anticipate and preempt terrorist threats to US interests. The goal is to make such teams faster, smarter, and more joint in their day-to-day operations. Genoa II will apply automation to team processes so that more information will be exploited, more hypotheses created and examined, more models built and populated with evidence. As a result, it is expected that teams will be able to deal with more crises simultaneously.

Advances in decision-making are supported by modeling terrorist behavior in the *Wargaming the Asymmetric Environment* (*WAE*) program. Its goal is to develop and demonstrate predictive technology to better anticipate and act against terrorists. WAE is a revolutionary approach to identify predictive indicators of attacks by and the behavior of specific terrorists by examining their behavior in the broader context of their political, cultural and ideological environment.

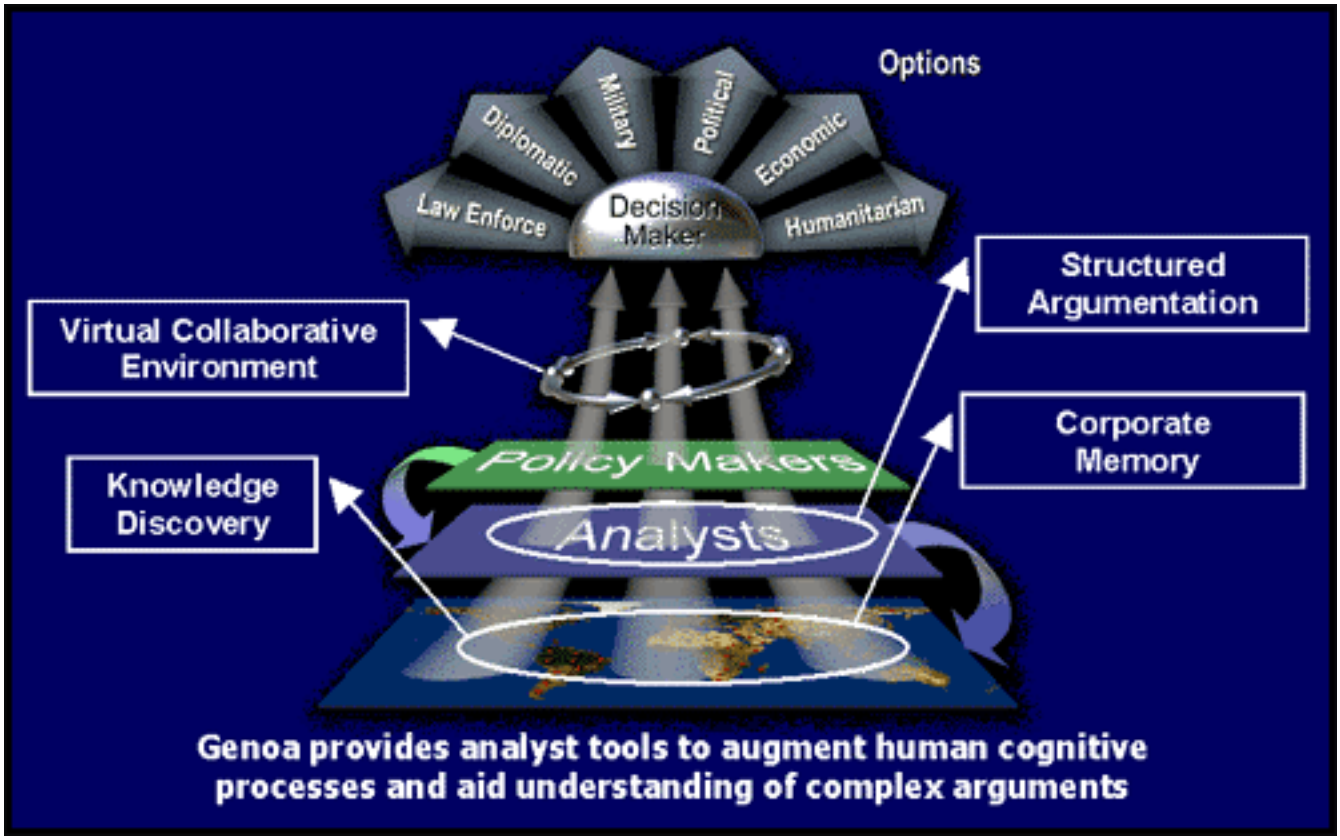


Figure 2: Structured argumentation and decision-making environment.

TIA is expected to benefit also from related business technology developments. The *Futures Markets Applied to Prediction* (*FutureMAP*) program is a follow-up to a current DARPA program named *Electronic Market-Based Decision Support*. FutureMAP will concentrate on market-based techniques for avoiding surprise and predicting future events. Strategic decisions depend upon the accurate assessment of the likelihood of future events. This analysis often requires independent contributions by experts in a wide variety of fields, with the resulting difficulty of combining the various opinions into one assessment. Market-based techniques provide a tool for producing these assessments. Potential applications may include analysis of political stability in regions of the world, prediction of the timing and impact on national security of emerging technologies, analysis of the outcomes of advanced technology programs, etc. In addition, the rapid reaction of markets to knowledge held by only a few participants may provide an early warning system to avoid surprise.

TIA further incorporates bio-surveillance programs designed to provide early warning and detection of incidents of bioterrorism. The goal of the *Bio-event Advanced Leading Indicator Recognition Technology* (*Bio-ALIRT*) program is to develop the necessary information technologies and resulting prototype capable of detecting the covert release of a biological pathogen automatically and significantly earlier than traditional approaches. Early detection is considered the key to mitigating a biological attack. Given the availability of appropriate medications, as many as half the expected casualties could be prevented if an attack is detected only a few days earlier than it would have otherwise been identified. For contagious biological agents, early detection is also clearly paramount. The Bio-ALIRT program shall dramatically increase the ability to detect a clandestine biological warfare attack in time to respond effectively and to avoid potentially thousands of casualties.

Finally, the *Human Identification at a Distance* (*HumanID*) program aims at developing automated

biometric identification technologies to detect, recognize and identify humans at great distances. These technologies are expected to provide critical early warning support for force protection and homeland defense against terrorist, criminal, and other human-based threats, and to prevent or decrease the success rate of such attacks against operational facilities and installations of the Department of Defense. Methods for fusing biometric technologies into advanced human identification systems will be developed to enable faster, more accurate and unconstrained identification of humans at significant standoff distances.

The research conducted under TIA will provide the tools for obtaining information pertaining to activities of terrorists, and if connected together, this information could alert authorities before terrorists' plans are carried out. Overall, the development of these anti-terrorism tracking tools is expected to allow the agencies to better execute their missions. While the research to date is promising, TIA is still only a concept.[5]

TIA is not collecting or gathering any intelligence information. The US Government confirms that this is and will continue to be the responsibility of the US foreign intelligence/ counterintelligence agencies, which operate under various legal and policy restrictions with congressional oversight. This technology development program does not alter the authority or responsibility of the intelligence community. TIA is a research program designed to catch terrorists before they strike.

Notes:

1. The Information Awareness Office at http://www.darpa.mil/iao/index.htm .
2. http://www.darpa.mil/iao/TIASystems.htm .
3. Described also in "Researchers Leave Terrorists Nowhere to Hide," *SIGNAL* 57, 6 (February 2003): 43-46.
4. "Researchers Leave Terrorists Nowhere to Hide," p. 45.
5. "Total Information Awareness (TIA) Update," *DefenseLINK* No. 060-03 (February 7, 2003), <http://www.defenselink.mil/news/Feb2003/b02072003_bt060-03.html>.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

Total Information Awareness (DARPA’s Research Program)

Information & Security

Keywords: homeland security, terrorist threat, ultra-large database, structured argumentation, data mining, collaborative decision-making, speech recognition, automatic translation, biometric identification, early warning, preemption

Abstract: The most serious asymmetric threat facing the United States is terrorism, a threat characterized by collections of people loosely organized in shadowy networks that are difficult to identify and define. In response, the Defense Advanced Research Projects Agency (DARPA) created the Information Awareness Office (IAO). IAO plans to develop technology that will allow understanding of the intent of these networks, their plans, and potentially define opportunities for disrupting or eliminating the threats. To effectively and efficiently carry this out, sharing, collaborating and reasoning shall be promoted to convert nebulous data to knowledge and actionable options.
The 'Total Information Awareness' is the main program of IAO aimed to "revolutionize the ability of the United States to detect, classify and identify foreign terrorists - and decipher their plans - and thereby enable the U.S. to take timely action to successfully preempt and defeat terrorist acts." The program objective is to create a counter-terrorism information system that increases information coverage, provides focused warnings, automatically queue analysts based on partial pattern matches, 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..

full text

Author: **Information & Security**
Title: **I&S Library Update**
Year of issuance: **2003**
Issue: **Information & Security. Volume 10, 2003, pages 113-125**
Hard copy: **ISSN 1311-1493**

GOVERNMENT AGAINST THE TERRORIST THREAT OF TWENTY FIRST CENTURY

James M. Smith and William S. Thomas, eds., *The Terrorism Threat and the U.S. Government Response: Operational and Organizational Factors*
(Colorado Springs, CO: USAF Institute for National Security Studies, 2001),
<http://www.usafa.af.mil/inss/terrorism.htm>

After the end of the Cold war, slowly but surely, the terrorism threat established itself on the top of the US national security agenda. Before September 11th that may have not been obvious to the outside observer. For the national security community, however, it seems that that was considered ground truth, the proof being reflected in this book.

Published in the spring of 2001, this compendium treats extensively the terrorist threat, the issues of preemption, prevention, deterrence and denial of terrorism actions, and organizational factors of the US governmental response to terrorism.

Although twelve authors contribute their own chapters, they all seem to agree that terrorism is "calculated violence applied toward coercive intimidation or provocation" with two central differentiating factors: "dedication to a political cause" and "instrumental reliance on violence."[1] Further adhering to the classical works of David Fromkin, the authors agree that terrorism "achieves its goal not through its acts but through the response to its acts. … terrorist actions aim at psychological result. But even that psychological result is not the final goal. Terrorism is violence used in order to create fear; but it is aimed at creating fear in order that the fear, in turn, will lead somebody else—not the terrorist—to embark on some quite different program of action that will accomplish whatever it is that the terrorist really desires."

The book provides detailed analysis of the shift in the terrorist threat. Out of this analysis we shall underline three points:

- Ever stronger combination of a political objective with ethnic and religious components;
- Shift from violence measured to fit a political agenda to increased lethality associated with a total, holy war;

- Shift from a state sponsorship to a marriage of terrorism with organized crime and drug cartels, leading to "privatization of terror."[2]

In part I, to this general analysis of the changing nature of terrorism, the contributors present more focused investigation of the potential terrorist use of weapons of mass destruction and cyber threats.

Four contributions in part II focus respectively on preemption of terrorist threats, combating international terrorism, antiterrorism via counterproliferation, and the role of intelligence and force protection.

Part Three would be of highest interest to the readers of this special issue of *Information & Security*. Recognizing the primary role of law enforcement in the fight against terrorism, the authors provide detailed analysis of the role of the military and of the State Department. Their analysis is based on existing legislation and experience, prudently distinguishing between prevention, response, and consequence management, as well as between domestic and international terrorism—quite a challenging endeavor given the ever blurring boundaries between the two.

One example of the complexity of the issue is the debate in Chapter 10. William Thomas provides meticulous analysis of current legislation and distinguishes not only between law enforcement and the military, but also among various branches of the military. Listing the twelve Emergency Support Functions (ESF) provided by FEMA:[3] (1) transportation; (2) communications; (3) public works and engineering; (4) firefighting; (5) information and planning; (6) mass care; (7) resource support; (8) health and medical services; (9) urban search and rescue; (10) hazardous materials; (11) food; and (12) energy, Thomas points out roles of various active, reserve and National Guard units.

The book is explicitly focused on experience, practices, organization and challenges to US Government. Nevertheless, it certainly is of value to policy makers and experts from other countries, as well as to those from intergovernmental and some non-governmental organizations.

Ironically, published only a few months prior to September 11th, the book refers to Al-Qaeda and bin Laden in its introductory sentences, listing the terrorist and his organization first among the new terrorist threats. And as often happens, it proves that academics are often too optimistic. In chapter 9 the author calls for "… developing information and analysis that enables us to better predict how, when, and where the terrorists will strike because we have fed them the information on which they will likely act."[4]

In a complex world exact prediction is problematic, if not entirely impossible. There are no easy answers to terrorism. This book, and—unfortunately—life itself, confirms that. What is needed is a complex answer including, among others, legislative, procedural, and organizational changes, innovative use of technology, and new levels of international cooperation.

Books like this one definitely contribute to the search for answers. We look forward to volumes like this one, accounting for the tragic experience of September 11th and the response of the United States and the international community of democratic nations.

Notes:

1. James M. Smith and William S. Thomas, *Chapter Two*: *The Terrorist Threat in Strategic Context.*
2. Ibid.
3. William S. Thomas, *Chapter 10: The Military's Response to Domestic WMD Terrorism.*
4. Peter S. Probst, *Chapter 9:Intelligence and Force Protection vs Terrorism.*

POLICE ACTION AGAINST THE THREAT OF SPECIAL WEAPONS OF MASS DESTRUCTION

John W. Ellis, *Police Analysis and Planning for Chemical, Biological and Radiological Attacks: Prevention, Defense and Response*
(Springfield, Illinois: Charles C. Thomas, 1999).

For decades the defense against weapons of mass destruction (WMD) was almost exclusive responsibility of military organizations, and in some cases - paramilitary civil protection agencies. With the end of the Cold War, however, we witnessed rapid increase in the involvement of law enforcement organizations to counter two interrelated concerns - WMD proliferation and rising terrorist threat.

Drawing on his experience both in the military and in the police, John Ellis presents a comprehensive treatment of *police* operations against chemical, biological and radiological threats. In separate chapters he describes these special WMD, presents framework for assessment of terrorist use, assessment of vulnerabilities to such attacks, and outlines preventive, defensive and response actions.

The book is rich of historical examples of dealing with chemical, biological and radiological effects, whether they have resulted form military use, industrial accidents or terrorist attacks. The author further provides detailed account of the 1986 accident at the Chernobyl nuclear power plant.

John Ellis favors integrated police prevention, defense and response to special WMD. Often referring to a companion book,[1] he extends the vision for integration to cover potential use of *conventional* weapons of mass destruction. But although he describes functions and capabilities of other US governmental organizations in regard to these threats, he does not volunteer with proposals for joint governmental response to terrorist threats.

Instead, using the language of an experienced practitioner, in every particular case Ellis punctually describes kill zones, survival zones, barriers, parameters, etc., assuming one or only a few points of

attacks or release points. Unfortunately, this approach is of little help when terrorists use different attack pattern, such as in the post-September 11th anthrax attacks in the continental United States.

The author carefully examines the legal aspects of the issue, starting from UN Charter, declarations and resolutions, and discussing specifics of state legislation when needed. Thus, the comprehensive treatment of legal, organizational, operational and technical issues makes the book a useful reference for the law enforcement practitioner. Further, it may be a useful entry level reading for IT specialist who intent to work on technology development projects in this particular area of security.

Todor Tagarev

Notes:

1. John W. Ellis, *Police Analysis and Planning for Vehicular Bombings: Prevention, Defense and Response* (Springfield, Illinois: Charles C. Thomas, 1999).

CHEMICAL AND BIOLOGICAL WEAPONS TERRORISM: FORGING A RESPONSE[1]

The 11 September 2001 terrorist attacks in the United States changed fundamentally threat perceptions regarding the use of weapons of mass destruction by terrorists. The ability to use such weapons is all the more credible because sophisticated delivery systems are not required to conduct a terrorist attack. As a consequence, governments have reviewed longstanding plans to respond to terrorist incidents and have sought to identify weaknesses and address these where possible.

Effectiveness of the response may increase through international cooperation and coordination in a number of areas. Priorities should include sharing intelligence; improving cooperation among likeminded states; sharing information about national activities and programs, etc. Forging a coordinated response will require governments and counter-terrorist practitioners to produce relevant threat assessments, including chemical and biological (CB)-related threat in the context of all terrorist-related risks; to improve public information and relations strategies; to strengthen existing international arms control regimes; to improve fundamental public health care; to consider how regional approaches may best be developed; to ensure that plans to deal with an incident are tested through regular exercises, etc.

National Responses

National responses to the CB terrorism threat will inevitably be affected by countries' past experience with terrorism, the nature of their political system and existing national counter-terrorism plans and capabilities. Sharing information on the challenges faced by different countries and on their responses

will enable those dealing with the problem to benefit from lessons learned.

The US case. The US 120 Cities Program is designed to prepare 'first responders' (police, fire and medical staff) to respond to chemical, biological, radiological and nuclear (CBRN) terrorism. The program drew on existing Department of Defense (DoD) capabilities and experience and it was coordinated by the US Secretary of the Army. Training was given to local 'responders' in the use of detection equipment; monitoring and prevention; protection of 'first responders' and the public; and decontamination. Key prerequisites for a successful response which were identified through conducting the program include: ensuring coordination at a very senior political level (e.g. the Secretary of Defense in the US); understanding that the improvement of 'national' (rather than local) capabilities is essential if a country is to be able to respond effectively; maximizing the convergence of all agencies and actors involved.

It is generally recognized, that in order to combat terrorism effectively, cooperation between agencies is essential both during and outside crises. This said, cooperation need not mean 'agreement' and it involves debate and strong differences of opinion. The need for debate must be balanced against the need for decisions to be taken. US counter-terrorism activity involves many agencies and programs: national security; biological weapons and related control regimes; US Homeland Defense issues. For example, Homeland Defense and biological weapons-related issues involve the Department of Defense, US allies, the Department of Transport, medical R&D agencies; various intelligence agencies, etc. Lead agencies for combating terrorism are the State Department (Overseas); the FBI (on US soil); FEMA (consequence management). The National Security Council plays a coordinating role on occasion, although its role post-11 September has yet fully to be clarified (as indeed is the case for other agencies).

Cooperation in this context prompts three difficult questions: who is in charge, who is to pay, whose interests are threatened by possible cooperation? Departmental competition for appropriations prompts strenuous efforts to defend related programs and expenditure and this may limit agencies' willingness to cooperate.

Additionally, the US response system has been enhanced by the newly-developed US Bio Defense Initiative that will also require high-level coordination and a lead agency to draw all related agencies and communities into the program. The newly-created Office of Homeland Security could be charged with this role, although it currently lacks the funding and command and control capabilities needed. However, the size of the US bureaucracy and interdependent responsibilities demand interagency cooperation to optimize results of national security programs in general, and counter-terrorism efforts in particular. A comprehensive national strategy is necessary to facilitate this cooperation while an effective program and budget oversight authority is required to ensure that this occurs.

The UK Experience. The United Kingdom Government has given overall authority for the coordination of counter-terrorism to the Home Office, which works in cooperation with the Foreign and Commonwealth Office, intelligence agencies, and other relevant departments. Implementation of legislation deriving from the Chemical Weapons and Biological Weapons Arms Control Regimes rests with the Department of Trade and Industry (DTI).

Post-11 September, a review of UK policies has been undertaken. Themes of particular interest include: transport security, CBRN terrorism, suicide attacks, macro-casualty attacks, spectacular/concurrent attacks, crisis/incident management, consequence management, legal frameworks, policy/decision structures, public information structure, terrorist use/abuse of IT, threat perception. Dealing with the last issue pointed to a number of key requirements and problems as well as the need to:

- have multi-agency, trained, equipped and well-exercised ‘first response’ personnel;
- include risk assessment expertise;
- have effective command and control;
- establish a public ‘help-line’;
- have sufficient laboratory analysis capability to permit speedy identification of substances;
- divide ‘initial’ from ‘first responders’;
- train police, fire, and ambulance personnel to respond in a cooperative manner;
- provide coordinated accurate public information quickly; a media emergency forum is being established in the UK to bring crisis management personnel together with media ‘leaders’ to consider how best to deal with crisis situations in the future;
- develop and deploy equipment ‘at street level’ to detect BW as well as CW effectively in differing conditions and situations, etc.

UK experiences in dealing with suspect maritime cargoes (possibly including CW or BW) offer the pointers for future action such as: strengthening and correctly locating C2 facilities; giving further consideration to how best to locate and dispose of CBW; considering how best to involve ‘new’ partners in addition to the ‘expected’ agencies, e.g. maritime agencies and organizations, and related industries as source of potentially useful advice and support. Other lessons drawn from the UK experience include dealing with CBW as part of an overall and broader counter-terrorism effort; managing complacency, and maximizing interagency cooperation to protect the public and pursue terrorists. Additional key areas of concern include improving border controls; considering possible changes in the involvement of military forces in dealing with the problem; balancing the protection of society from physical danger with the maintenance of human and civil rights of individuals; the maintenance or introduction of suitable oversight mechanisms.

EU and Europol Responses. The adopted response mechanisms have been designed not only for EU member states but also for candidate countries and other European neighbors. Cooperation efforts had to overcome differing political interests of member states vis-•-vis ‘rogue’ nations; lack of a common definition of terrorism and disagreements which organizations are ‘terrorist’; lack of a common

strategy (states seek to retain oversight of their essentially national reactions); different legal systems in different countries; lack of conformity of national approaches to crime fighting and counter-terrorism (e.g. police cooperation with the intelligence services is close in the UK but virtually forbidden in Germany); language problems and resulting associated bureaucracy.

Despite this, a common response to organized crime and terrorism has been developed. Measures agreed include: setting new tasks for Europol; developing closer police-security service cooperation between member states; increased harmonization of national laws; agreement on an EU Warrant of Arrest.

Efforts are underway to agree on a common approach to counter-terrorism. An operational crisis center has been established to work on a 24-hour-a-day basis to gather and research all available information and intelligence about terrorist attacks and related investigations in Europe. The Center facilitates operational analysis of data collected and the dissemination of key developments to expert contact points in member states. A counter-terrorist task force has been established. It includes experts from the law enforcement agencies of all EU member states and specialists from security services. An inventory list of anti-terrorism security measures has been provided by EU member states in the EU with the aim of helping them to compare their security measures, their assessments of the CBRN threat and to share best practices. A key goal has been to produce a threat assessment to help member states to calculate terrorist risks, including the risks associated with CBRN weapons.

The risk assessment reached the following conclusions:

- it is highly unlikely that terrorists could manufacture and detonate a nuclear device without assistance from a rogue state;

- a crude radiological dispersal device (dirty bomb) seems to be within the current capabilities of terrorist organizations and poses a realistic threat;

- BW and CW are unlikely to be already available to terrorist networks. If such weapons were available, the problems concerning transport and dispersion remain.

Problems to be addressed in the future include: providing adequate financial resources for Europol to undertake its new tasks effectively; recruiting more personnel; improving arrangements for information-sharing both within the EU and with the US; building on existing cooperative links with the UN, Organization for the Prohibition of Chemical Weapons (OPCW), EURATOM, and interested states; improving expertise on CB weapons to facilitate better contacts with other interested expert communities.

Israel's Way. The Israel-Palestinian conflict provokes a particularly intense interest in the issue of CB terrorism in Israel. As suicide bombers constitute the 'end point' of an organized activity, they need not be schooled in CBW-related knowledge which can be provided by planners and organizers elsewhere in the system. Israel's first priority remains to address the threat of war through deterrence, early warning, prevention, and active and passive defenses. This strategy has been adjusted to meet the threat of terrorism and the two are perceived to be closely linked not least because some WMD-

capable states in the Middle East actively support terrorist groups.

The Israeli response is governed by three major principles: international cooperation (because the threat is global); prevention; mobilization of all national resources to meet the threat. International cooperation involves political-diplomatic activity; military security and technical cooperation; economic activities, legal issues, public education. It is intended to directly combat terrorists, undermine the infrastructure which supports them (whether states or international non-state actors as well as local organizations, labs, etc), change the culture which is supportive of terrorist activity.

Prevention is stressed because it preserves life, effectively marshals resources and prevents panic. It requires good intelligence, international cooperative action, effective combat capability, acting within the law, a 'layered' effort from borders to the High Street, understanding the terrorist mindset and anticipating unusual or novel methods of attack, monitoring what is going on in laboratories and universities and the activities of their personnel. Centralized responsibility for consequence management rests with the Ministry of Defense and its Home Front Command. Its mission is to support the civilian population during wartime and to prepare civilians for war during the peace. It coordinates activities of civilian organizations in wartime and prepares and trains them for this eventuality.

Maintaining a high degree of readiness is a central Israeli concern. C2 and coordination exercises are held regularly to ensure that those involved have a common approach to dealing with a crisis situation. Particular efforts have been made to prepare the medical system to deal with a CB event, which may come without warning and therefore require early detection if widespread casualties and/or infection are to be avoided. Much work has been done on public information and how this affects public behavior in a crisis. A lack of information and instruction tends to generate panic. Therefore, sufficient, correct, reliable and authoritative information must be available in 'good time' to ensure effective control of a situation.

The Impact of New Technologies

Developing technologies are of particular use in threat assessment, e.g. surveillance and tracking of individuals and material, iris and palm scanning technologies to control entry to sites; risk assessment, e.g. assessing the likely impact of release of BW through mathematical modeling which will assist planning and decision-making; increasing general levels of security and the security of particular assets, e.g. aircraft, chemical loads in transport to be tracked by satellite, designing the structures of potential targets – for example CB plants – to maximize physical protection.

Technologies also have much to contribute if a CB event actually occurs. Chemical detectors are already available and deployed with police forces in a number of countries. Street-level detection of BW remains a 'holy grail'; the science already exists which permits the screening of a wide range of organisms and systems are already available commercially. Single-molecule detection is also technically possible. However, the challenge is to produce equipment which is easy to use, reliable, has no false alarms, and is usable in varied environments.

Technology can also facilitate clinical diagnosis and the protection of those affected. The design of

vaccines ‘to order’ is now possible which will improve their effectiveness. Genetic screening will permit to identify individuals at risk and best able to respond.

‘Cleaning up’ after an event remains problematical as well, not least because the clean-up agents are themselves dangerous and toxic. Furthermore, a wide range of environments could be involved, each requiring differing attention and treatment.

Improving criminal detection methods is also a priority. DNA profiling is already a very powerful tool. It will have a vital role to play in dealing with BW release and the identification of strains and sources of material involved. The barriers to use technology in counter-terrorism include the high costs involved (requiring a ‘weighing’ of risk and perceived risk against cost); concerns about human rights and implications for individual freedoms; the need to ensure that they are working ‘as advertised,’ reliably, and with few or no false alarms; medical safety regulations and the need for testing.

The protection of advanced technologies is an important issue, for they may be used against society. However, cooperation will be difficult if technology is too protected, and some systems will need to be multilateral. Efforts to develop cooperation will also be affected by concerns about fair trade and the maintenance of security of information collected on individuals.

It is possible for individuals to provide related information to terrorist groups. Apparently, there is lack of concern in industry about this and related issues. Therefore, it will be essential to establish effective control over organism design to ensure that the focus of work is on destruction of organisms rather than making them more toxic, etc., and make systems broadly focused to permit them to be updated and changed as needed. How to keep sensitive information secure will inevitably be problematical in the face of any drive for more scientific openness.

Technology will not offer a panacea for the counter-terrorist community. If properly handled, it will have much to contribute. It is important that developments be both technology- and user-driven; a dialogue between the two concerned communities is essential and must be regular and ongoing to ensure that the right sort of equipment is developed and deployed.

Intelligence Sharing

The interstate exchange of CBRN terrorism-related intelligence is problematic but encouraged by the nature of the threat, the size of the (possible or imagined) consequences, the focus on prevention, the need for technical know-how and shared inexperience. In turn, intelligence-sharing is required inside states between key organizations engaged in combating.

The difficulties of engaging in intelligence exchange include: the requirement to protect sources of information; diverging perceptions of the problem and agency interests; fears of a breach of confidentiality on the part of those to whom information is given; legal commitments; constraints and incompatibilities; the competence of those outside the intelligence agencies to handle the information provided, etc.

Facilitating cooperation within the country should take due account of the differing responsibilities and world views of the agencies involved. Intelligence agencies are policy-oriented and forward-looking and information has to be 'good enough' to feed into the policy-making process. In contrast, law enforcement agencies make considerable use of intelligence after an event has occurred, given their interest in securing convictions. Material has to be of sufficient quality to withstand the legal process and achieve convictions in a trial. In addition, it is likely that the 'war on terrorism' will not be an exclusively governmental enterprise; it will be necessary to involve the public, local police and industry to achieve success and how information is to be shared with these communities requires further consideration.

There is also the concern that the structures of national governments are ill-suited to deal with the new threat of international terrorism and the role of national militaries is outward-looking and less focused on internal defense roles and efforts which may need to be reexamined. Furthermore, the validation of information (ensuring its authenticity) as well as effective oversight of what is being shared, and with whom needs to be assured.

US domestic arrangements also point to future key requirements: dealing with the fact that many of the agencies and organizations which need to be mobilized lack any security clearance and fail to receive intelligence as a consequence; the need to improve the collection and analysis of domestic intelligence and to develop an overall strategy which is adaptable and flexible.

For a successful information exchange it is essential that information from whatever source is presented to others in a form which they can utilize effectively. Actually, some difficulties will not be solved and will remain part of the environment within which intelligence is shared and the war on terrorism is conducted in the decades ahead.

Information & Security

Notes:

1. This is an excerpt of Wilton Park Conference (WP671, 22-24 March 2002) report, prepared by Dr. Richard Latter. The full text is available at http://www.wiltonpark.org.uk/web/conferences/reportprintwrapper.asp?confref=WP671.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

Author: **Information & Security**
Title: **I&S Resources**
Year of issuance: **2003**
Issue: **Information & Security. Volume 10, 2003, pages 126-134**
Hard copy: **ISSN 1311-1493**

SELECTED INTERNET SOURCES ON CIVIL EMERGENCY AND LAW ENFORCEMENT ISSUES

US Federal Emergency Management Agency (FEMA)

http://www.fema.gov

FEMA is the lead agency in the United States to response an event that has occurred and consequence management. The FEMA site provides emergency management courses for self-study.

Awareness of National Security Issues and Response (ANSIR)

http://www.fbi.gov/ansir/

The ANSIR program of the United States Government is designed to provide unclassified national security threat and warning information to US corporate security directors and executives, law enforcement and other government agencies. It focuses on the response capability unique to the jurisdiction of the Federal Bureau of Investigation in both law enforcement and counterintelligence.

Interagency Group on Counterterrorism

http://www.state.gov/s/ct/

In the US, The Department of State is the lead agency for overseas terrorist actions and supports the Office of the Coordinator for Counterterrorism that chairs the Interagency Group on Counterterrorism.

The International Policy Institute for Counter-Terrorism (ICT)

http://www.ict.org.il

ICT, established in 1996, focuses solely on the subject of counter-terrorism. It approaches the issue of terrorism as a strategic problem. The Institute raises public awareness and provides advice to decision makers. The site provides articles by ICT staff, terrorist organizations' profiles and databse of terror attacks.

Defense Threat Reduction Agency (DTRA)

http://www.dtra.mil/

DTRA is a US Department of Defense Agency with the mission to reduce the threat to the United States and its allies from nuclear, biological, chemical (NBC), conventional and special weapons through the execution of technology security activities, cooperative threat reduction programs, arms control treaty monitoring and on-site inspection, force protection, NBC defense, and counter proliferation; to support the US nuclear deterrent; and to provide technical support on weapons of mass destruction matters to DoD components.

Chem-Bio Defense

http://www.dtra.mil/cb/cb_index.html

Chemical and biological weapons, sometimes referred to as the "poor man's nuclear weapons," pose a significant threat in the post-Cold War environment. In order to counter these threats more effectively and develop better means of responding, DTRA draws upon the disparate chemical and biological weapons defense expertise in the Department of Defense in acting as the focal point for DoD technical expertise in these areas. In doing so, the Agency directs and manages Chem-Bio defense efforts in a centralized and focused manner in pursuit of proper preparation and response in the event of a chemical or biological weapons attack against U.S. forces or territory, or those of allies.

Environmental Protection Agency, US

http://www.epa.gov

EPA's mission is to protect human health and to safeguard the natural environment — air, water, and land — upon which life depends. The EPA's Chemical Emergency Protection and Preparedness Office <http://www.epa.gov/ceppo> offers technical assistance to prevent and prepare for chemical emergencies, respond to environmental crisis, and inform the public about chemical hazards in their

community.

US National Domestic Preparedness Office, Department of Justice

http://www.ndpo.com

The mission of NDPO is to coordinate all federal efforts, including the efforts of the Department of Defense, FEMA, Department of Health, Department of Energy and the Environmental Protection Agency to assist state and local first responders with planning, training, equipment and exercise necessary to respond to an incident with conventional or non-conventional weapons of mass destruction. NDPO provides training, coordinated equipment, coordinated exercises and integrated planning.

US National Infrastructure Protection Center

http://www.nipc.gov/

The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The mission of the NIPC is to: detect, deter, assess, warn, respond, and investigate unlawful acts involving computer and information technologies and unlawful acts, both physical and cyber, that threaten or target our critical infrastructures; manage computer intrusion investigations; support law enforcement, counterterrorism, and foreign counterintelligence missions related to cyber crimes and intrusion; support national security authorities when unlawful acts go beyond crime and are foreign-sponsored attacks on United States interests; and coordinate training for cyber investigators and infrastructure protectors in government and the private sector.

Comprehensive Risk Analysis and Management Network (CRN)

http://www.isn.ethz.ch/crn/

CRN is an electronic platform for promoting the risk profiling dialogue. The site contains methodologies, procedures, tools and case studies for the security risk profiling process at national, sub-national and local levels. CRN is developed by the Center for Security Studies and Conflict Research at the ETH Zurich with the Swedish Agency for Civil Emergency Planning (•CB) <www.ocb.se> and the Swiss Federal Office for Civil Protection <www.zivilschutz.admin.ch>.

UNOCHA - The United Nations Office for the Coordination of Humanitarian Affairs

The Emergency Relief Coordinators functions of UNOCHA are focused in three core areas: (a) policy development and coordination functions in support of the Secretary-General, ensuring that all humanitarian issues, including those which fall between gaps in existing mandates of agencies such as protection and assistance for internally displaced persons, are addressed; (b) advocacy of humanitarian issues with political organs, notably the Security Council; and (c) coordination of humanitarian emergency response, by ensuring that an appropriate response mechanism is established, through Inter-Agency Standing Committee (IASC) consultations, on the ground. **International Strategy for Disaster Reduction (ISDR)** is one of the UNOCHA projects. The mission of the project is to help communities reduce the risk of longer-term social and economic disruption in the face of a natural hazard by helping then assess their vulnerabilities to these risks and plan to increase their resiliency to disaster. For more information see http://www.unisdr.org/unisdr/safer.htm.

The Fribourg Forum: Managing Crisis

http://www.reliefweb.int/fribourg/

The Fribourg Forum is part of the European Cooperation Program that aims at creating favorable environment for effective crisis management and humanitarian action within existing regional mechanisms. The purpose of the Fribourg Forum is to convene senior policy makers responsible for international humanitarian assistance in Europe and the USSR successor states in order to obtain their support and commitment for an enhanced coordination and cooperation in the provision of humanitarian assistance in the region. In this respect, the Fribourg Forum gives opportunity to governments and international/regional organizations to present initiatives and programs addressing the current challenging crisis management situation as well as identifying areas of concern calling for particular attention.

International Civil Defense Organization (ICDO)

http://www.icdo.org/

The International Civil Defense Organization (ICDO) is an intergovernmental organization whose objective is to contribute to the state development of structures ensuring the protection and assistance of populations and safeguarding property and the environment from natural or man-made disasters. These structures are generally known as civil protection, civil defense or civil safety and are all concerned with the management of emergency situations. ICDO is active mainly in international cooperation in civil protection matters, development of national civil protection structures, and

promotion of disaster prevention

Hazard and Risk Assessment within OECD

The Organization for Economic Co-operation and Development (OECD) groups 29 member countries in an organization that, most importantly, provides governments a setting in which to discuss, develop and perfect economic and social policy. They compare experience, seek answers to common problems and work to co-ordinate domestic and international policies that increasingly in today's globalized world must form a web of even practice across nations. OECD has ongoing projects in the following areas:

Hazard / Risk Assessment

Many activities on hazard/risk assessment are currently going-on within the OECD. The activities are being carried out under various programs (e.g. Existing Chemicals Program, and the Pesticides Program). Of particular interest is the promotion of risk communication and the convergence of chemical risk assessment and socio-economic analysis <http://www.oecd.org/ehs/hazard.htm>.

Chemical Risk Management

OECD's Environmental Health and Safety Program publishes a Chemical Risk Management series at http://www.oecd.org/ehs/risk.htm.

International Futures Program

The OECD has launched a promising initiative to conduct a thorough examination of the changing nature of systemic risks and its implications. The purpose of this OECD "Futures Project on Emerging Systemic Risks" is to provide OECD governments, major players in the business sector as well as civil society, with a comprehensive picture of possible future developments in this field. It will also offer an opportunity for the development of a common assessment of the means needed to ensure that risk management can contribute fully to the sound and sustainable evolution of the OECD area and the world economy at large over the coming decades. <http://www.oecd.org/sge/au/risks.htm>

The OECD/IPCS Database on Hazard/Risk Assessment Methodologies

The OECD/IPCS Database on Hazard/Risk Assessment Methodologies includes hazard/risk assessment methodologies for industrial chemicals and pesticides and for human health and environmental assessments. <http://www.oecd.org//ehs/RA/risk-assessment-methodologies.htm>

EUR-OPA Major Hazards Agreement

http://www.europarisks.coe.int/

The mission of the Cooperation Group for the Prevention of, Protection against, and Organization of Relief in Major Natural and Technological Disasters is to provide for open dissemination of information and training of populations in the field of risk management, establishment of a permanent telecommunications link between the persons responsible for risk management in the member states of the EUR-OPA Major Hazards Agreement, resolution on cooperation between the EUR-OPA Major Hazards Agreement and international institutions, resolution on the network of specialized centers of the Agreement, and establishment of a "Risk Culture."

The CERT Analysis Center

http://www.cert.org/analysis

The CERT analysis Center seeks to assess and predict online threats. The site currently provides documents on cyberwar, information security trend analysis, cyberterrorism, and intelligence analysis for Internet security.

OECD Anti-Corruption Activities

http://www.oecd.org/ <Corruption>

At its web site, the Organization for Economic Co-operation and Development (OECD) maintains information on international policy initiatives, conventions and reports on: Bribery and Export Credits; Corruption and Development; Ethics and Corruption; Fighting Bribery and Corruption; and Tax Treatment of Bribes. Furthermore, OECD pays special attention to money laundering. The latest annual report, 22 June 2001, of the Financial Action Task Force on Money Laundering is available at http://www1.oecd.org/fatf/pdf/AR2000_en.pdf .

SEECAP

http://www.nato.int/docu/comm/2001/0105-bdp/d010530b.htm

The South East Europe Common Assessment Paper on Regional Security Challenges and Opportunities (SEECAP) is endorsed by the States of the region of South Eastern Europe as a first hand perception of how these challenges and opportunities can guide the common efforts to foster lasting peace, stability, freedom and prosperity. The paper pays special attention to non-conventional

security challenges such as organized crime and terrorism.

UN Center for International Crime Prevention

www.odccp.org/about.html

The United Nations Office for Drug Control and Crime Prevention (ODCCP) is a global leader in the fight against illicit drugs and international crime. Established in 1997, ODCCP consists of the United Nations International Drug Control Program (UNDCP) and the United Nations Center for International Crime Prevention (CICP).

UNDCP

www.odccp.org/undcp.html

Founded in 1991, the United Nations International Drug Control Program UNDCP works to educate the world about the dangers of drug abuse. The Program aims to strengthen international action against drug production, trafficking and drug-related crime through alternative development projects, crop monitoring and anti-money laundering <www.odccp.org/money_laundering.html> programs. UNDCP also provides statistics and helps to draft legislation and train judicial officials as part of its Legal Assistance Program.

CICP

www.odccp.org/crime_cicp.html

Established in 1997, the Center for International Crime Prevention (CICP) is the United Nations office responsible for crime prevention, criminal justice and criminal law reform. The CICP works with Member States to strengthen the rule of law, promote stable and viable criminal justice systems and combat the growing threat of transnational organized crime through its Global Program Against Corruption <www.odccp.org/corruption.html>, Global Program Against Organized Crime <www.odccp.org/organized_crime.html> and Global Program Against Trafficking in Human Beings < www.odccp.org/trafficking_human_beings.html> and its Terrorism Prevention Branch (TPB) <www.odccp.org/terrorisam.html>.

INCB

www.odccp.org/incb.html

The International Narcotics Control Board (INCB) is the independent and quasi-judicial control body for the implementation of the United Nations drug conventions. It was established in 1968. INCB is

independent of Governments as well as of the United Nations; its 13 members serve in their personal capacity.

UN Commission on Crime Prevention and Criminal Justice

www.odccp.org/crime_cicp_commission.html

The 40-member UN Commission on Crime Prevention and Criminal Justice formulates international policies and recommends activities in the field of crime control. The Commission offers nations a forum for exchanging information and to settle on ways to fight crime on a global level. The Commission is a subsidiary body of the Economic and Social Council. The Commission formulates draft resolutions for action by the Council. These resolutions eventually direct the work of the CICP.

Institute for Crisis, Disaster, and Risk Management

http://www.seas.gwu.edu/~icdm/

The Institute for Crisis, Disaster, and Risk Management (ICDRM) at The George Washington University was established in August 1994 as an interdisciplinary academic center affiliated with the University's School of Engineering and Applied Science, School of Medicine and Health Sciences, School of Public Health and Health Services, and Elliott School of International Affairs. The Institute integrates the existing diverse expertise and research related to crisis, disaster, and risk management at the George Washington University and is unique in its interdisciplinary focus and structure. This interdisciplinary approach produces innovative research, training, and education to enhance crisis and emergency management, risk management, contingency planning, emergency response, and disaster recovery. Some of its research results are presented on-line, e.g., the report on "Future of Emergency Management in the US following Sept. 11 Terror Attacks," October 2001 <http://www.seas.gwu.edu/~icdm/Oct1.htm>.

Disaster Preparedness and Prevention

http://www.stabilitypact.org/stabilitypactcgi/catalog/cat_descr.cgi?subcat=1&prod_id=48

The Disaster Preparedness and Prevention Initiative (DPPI) is an effort by the Stability Pact for South Eastern Europe to contribute to the development of a cohesive regional strategy for disaster preparedness and prevention. It aims to bridge the gap between international and local efforts and to encourage the full participation and mutual support of all regional countries. An operational team, with expert personnel from the Bulgaria, Croatia, Italy, Sweden, the United States, the International Federation of Red Cross and Red Crescent Societies (IFRC), NATO, and the United Nations Development Program (UNDP), was established to provide the technical background work. As the

first stage in developing a strategy, the DPPI undertook an assessment in each country of the region. The team assessed disaster preparedness and prevention needs and capabilities, reviewed natural and technological disaster risks and existing disaster management and preparedness plans, and identified ongoing emergency response projects, coordination structures and procedures. The findings will serve as basis for the development of a comprehensive Disaster Preparedness and Prevention Strategy for South Eastern Europe. This strategy will be developed in cooperation with the countries and validated by them. The main strategies and lines of work identified for improving the overall disaster management capacity in the region will be addressed at the national, bi-national, multi-national or regional level.

GAMMA-EC

http://www.tno.nl/instit/fel/gamma_ec/

International research project within the European Union on technology, methods and organization to increase public safety in a number of hazards and emergencies.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg