HOMELAND SECURITY DISCIPLINES AND THE CYCLE OF PREPAREDNES

William V. Pelfrey

Preparedness is not an abstract concept. It is discrete, calculable (to a degree), and applicable to certain disciplines, organizations, agencies, and individuals. This concept still begs the question "What are we preparing to do?" The Cycle of Preparedness helps to disaggregate Preparedness so it can be addressed more appropriately by various disciplines. Within each of the categories of the Cycle, there are imperatives that must be met, principally by one discipline or another, but in concert with others. In this paper, we will describe the major disciplines associated with terrorism preparedness and examples of the application of the Cycle of Preparedness to those disciplines.

Homeland Security Disciplines[1]

There is no limit to the disciplines affected by or participating in Preparedness. Discipline, in the academic sense, is a field of study or a subject that is selected and taught. In the context of terrorism preparedness, "discipline" is a field of practice, a profession, or a category representing a group of professionals with some common orientation or focus. A synonymous phrase would be "professional collective." Dahrendorf[2] used another term, "imperatively coordinated associations," to describe groups in conflict, but that phrase is useful here to suggest the often non-amicable nature of disciplines associated with Homeland Security. They are often "professionally aligned" as is the case with fire and police, but they compete for resources, prominence, and authority. Systems have been developed to improve the "coordination" of the disciplines, such as the National Incident Management System (NIMS), and the Integrated Command System (ICS), but the fact remains that the set of collectives is quite heterogeneous. The "imperative" that has created this amalgamation, or at least interaction, of the somewhat disparate disciplines is, of course, the threat of terrorism.

The disciplines described here include well-established ones, as well as new, relatively undefined collectives. It is possible to label some as Principally Responsible, and others as Secondarily Responsible, and that will be mentioned within the context of the Cycle of Preparedness. For now, it is important to simply describe the disciplines that are directly related to Preparedness.

Early in the development of the Office for Domestic Preparedness, there was an initiative to perform a "job task analysis" for professions responding to a WMD threat (the descriptive term of enquiry at the time). This work identified ten disciplines, each with response and recovery responsibilities.[3] These disciplines are:

Law Enforcement
Emergency Medical Services (EMS)
Fire Service
Hazardous Waste Operations and Emergency Response (HAZMAT)
Emergency Dispatch Communications
Health Services
Emergency Management Agency (EMA)
Governmental Administrative
Public Health
Public Works

One could argue that the first four of these disciplines, Law Enforcement, Fire, EMS, and HAZMAT, are most directed involved in the initial response to a threat of terrorism, weapons of mass destruction, mass exposure, or mass disruption. That statement, of course, is qualified by the type of threat. A cyber attack, or contamination of a water supply, for example, would be recognized and responded to by other professionals. Conventional weapons of mass destruction would involve response by some or all of these disciplines during the threat recognition and "crisis management" phases.

Public Safety Communications or Emergency Dispatch Communications would be involved at the outset but primarily in gathering information and distributing resources and information to agencies and disciplines. Health Services and medical facilities, while not responding to the location of an attack would respond to the effects of the attack. The next disciplines, Emergency Management Agency, Governmental Administration, Public Health, and Public Works, have coordination roles and responsibilities during the response or "crisis management" phases, as well as the recovery and mitigation or "consequence management" phases. The process is cumulative rather than sequential. The initial agencies, organizations, professionals, and disciplines involved in an incident remain involved, to a greater or lesser degree, while more agencies become involved in the management of the disaster or incident.

Clearly there are more disciplines associated with terrorism prevention, response and recovery than those described thus far. These disciplines could include every agency, organization, and profession in the United States since an event or incident affects every person in the jurisdiction to some degree. The goal here is not to be entirely inclusive but to discriminately identify those disciplines most associated with the Cycle of Preparedness. Some of these "disciplines" are not really disciplines but loose collectives of functional emphases (Business Continuity, for example). Others cross many different organizational lines, such as Skilled Trades and Private Sector. Homeland Security is listed here, even though it may be the amalgamation of all disciplines involved in terrorism prevention, response and recovery. It is, in most states and in many local jurisdictions, an emerging discipline that may be oriented toward law enforcement, military, or governmental administration. There is sufficient variation, however, to suggest that it be viewed as a separate discipline. The purpose is to articulate a *category* with sufficient specificity to describe the roles of these groups in the Cycle of Preparedness. These disciplines are additions to the original list:

Business Continuity

Conveyances

Cyber-security and Information Technology Infrastructure Protection

Educational institutions and organizations

Homeland Security

Private Security, Loss Prevention

Major Event Security and Public Safety

Red Cross, Volunteer and Non-Governmental Organizations providing public assistance

Public Information

Media Management

Public Warning/Alerts

Public Places and Major Facilities

Private Sector

Financial Institutions

Prosecutor

Risk Management

Skilled Trades

Transportation Services

Public/Private Utilities

Military

The articulation of these "disciplines" may seem awkward, overlapping, and unwieldy. It may also appear to dilute the initial focus on "responder" communities and disciplines. However, as we will see in the next section of this paper, prevention and recovery involve each of these agencies and organizations while "response" or crisis management may involve the fewest of the disciplines. Disaggregating the elements of the Cycle of Preparedness must be accompanied by the attribution of responsibilities within each of the elements for Preparedness to become a reality.

Operationalization of Preparedness

Preparedness is the degree to which an organization, agency, or discipline is capable of preventing, responding to, or recovering from a threat, crisis, disaster, incident, or event of mass destruction, mass exposure, or mass disruption. An official definition is:

> The term "preparedness" refers to the existence of plans, procedures, policies, training, and equipment necessary at the Federal, State, and local level to maximize the ability to prevent, respond to, and recover from major events. The term "readiness" is used interchangeably with preparedness.[4]

Preparedness is a process, or as is proposed in these papers, a cycle. These papers posit that the process must begin with "collaboration." The process of determining capability or capacity to prevent, respond to, or recover from an event, includes threat assessment, vulnerability assessment, estimation of consequences, and the determination of risk. The next important step is risk management. Capability assessment logically follows the risk management model by determining the resources (personnel, equipment, plans, abilities to perform the necessary tasks) necessary to address the threats and vulnerabilities in order to manage the risk in an "acceptable" fashion. Next is the determination of those necessary resources that are on hand or available to manage the risks —the needs assessment. Once a jurisdiction or organization gains the resources—personnel, equipment, planning capabilities, and training—to adequately address the risks, the jurisdiction or agency would be considered "prepared." The Office for Domestic Preparedness uses the following model:[5]

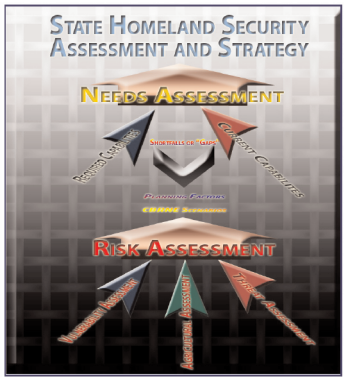

Figure 1.1: Jurisdiction Risk and Needs Assessment Model

Vulnerability is a representation of "the relative likelihood that a particular facility or incident within the jurisdiction may become the target of a terrorist attack. The factors considered include measures of attractiveness and impact."[6] A threat, or, in the glossary of the Office for Domestic Preparedness, a "Potential Threat Element," is "any group or individual in which there are allegations or information indicating a possibility of the unlawful use of force or violence, specifically the utilization of a WMD, against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of a specific motivation or goal, possibly political or social in nature. This definition provides sufficient predicate for the FBI to initiate an investigation."[7]

While these descriptions are useful, they are not as precise as those used elsewhere. The U.S. Department of Transportation, for example, in their Research and Special Programs Administration, Office of Hazardous Materials Safety,[8] has produced the following definitions that could easily be extrapolated into our Preparedness discussion:

> HAZARD is the inherent characteristic of a material, condition, or activity that has the potential to cause harm to people, property, or the environment.
>
> RISK is the combination of the likelihood and the consequence of a specified hazard being realized. It is a measure of harm or loss associated with an activity.
>
> LIKELIHOOD is expressed as either a frequency or a probability. Frequency is a measure of the rate at which events occur over time (e.g., events/year, incidents/year, deaths/year, etc.). Probability is a measure of the rate of a possible event expressed as a fraction of the total number of events (e.g., one-in-a-million, 1/1,000,000, or 1X10-3).
>
> CONSEQUENCE is the direct effect of an event, incident or accident. It is expressed as a health effect (e.g., death, injury, exposure), property loss, environmental effect, evacuation, or quantity spilled.

HAZARD ANALYSIS is the identification of material properties, system elements or events that lead to harm or loss. The term hazard analysis may also include evaluation of consequences from an event or incident.

RISK ANALYSIS is the study of risk in order to understand and quantify risk so it can be managed.

RISK ASSESSMENT OR RISK CHARACTERIZATION is determination of risk context and acceptability, often by comparison to similar risks.

QUANTITATIVE RISK ANALYSIS incorporates numerical estimates of frequency or probability and consequence. In practice a sophisticated analysis of risk requires extensive data which are expensive to acquire or often unavailable. Fortunately few decisions require sophisticated quantification of both frequency and consequences.

RELATIVE RISK ANALYSIS means that a risk is evaluated in comparison to another risk. The type of risk analysis used should be appropriate for the available data and to the exposure, frequency and severity of potential loss.

RISK MANAGEMENT is the systematic application of policies, practices, and resources to the assessment and control of risk affecting human health and safety and the environment. Hazard, risk, and cost/benefit analysis are used to support development of risk reduction options, program objectives, and prioritization of issues and resources. A critical role of the safety regulator is to identify activities involving significant risk and to establish an acceptable level of risk. Near zero risk can be very costly and in most cases is not achievable.

Even these definitions are not comprehensive enough to allow a full discussion of terrorism threats, vulnerabilities and risk. The Office for Domestic Preparedness, in the Strategy Assessment Reference Handbook, the ODP Jurisdictional Handbook, and the ODP State Handbook, has articulated additional terms, terminology, and processes that give breadth and depth to the discussion. Additionally, there are other public and private organizations that have developed robust risk assessment instruments and decision models that can be used to determine the allocation of scarce resources for the prevention of, response to, and recovery from an event or disaster. Even a cursory examination of those processes would require significant attention and that is not the purpose of this paper. Mention will be made, however, of the concept of capabilities assessment introduced above.

Capabilities Assessment

There are two ways to consider capabilities in this context. One addresses the capabilities of the terrorists—that is, their means of accomplishing an attack or mounting a threat of sufficient magnitude to merit attention and action. The two major aspects of terrorism are motivation to accomplish an act or attack, and the current ability, or capability, to launch such an attack. If either one is missing, there is no threat and, therefore, no need to prepare. It is very difficult to accurately assess the capability of the terrorists. Indeed, the nature of asymmetric, covert conflict suggests that there will be insufficient similarly in the forces, and the enemy will display stealth and cunning in strategic warfare. So, accurately assessing the capability of terrorists is very difficult. This aspect is mentioned because the two necessary elements of terrorists' capability, means and motivation, are also the necessary elements of our capacity to prevent, respond and recover.

As a nation, we are interested in enhancing **our** preparedness, that is, in establishing sufficient capabilities (means and motivation) to prevent, respond to, and recover from the threat posed by hazards, either natural or intentional. It is also critical to identify, in general terms, the event, type of incident or threat for which we are preparing. A GAO report, for example, stated:

> Based on their own self-assessments, local fire department officials from most of the cities that we visited said that they are generally prepared to respond to a hazardous material incident. A few officials whom we interviewed said that although their city is prepared to respond to a hazardous material incident, their in-house capability would depend on the types of hazardous materials involved and the scope of the incident. For example, one fire department official said that he is comfortable with his city's capabilities to respond to chemical accidents such as leaking tank cars, spills, and derailments. He believed that his city could adequately respond to a hazardous material incident unless it was a catastrophic event, such as a major derailment involving multiple cars.[9]

That report suggested a risk-based approach to preparedness. Similarly, the Department of Defense suggests risk management, as "an organized method for identifying and measuring risk and for selecting, developing, and implementing options for the handling of risk."[10]

It is necessary to apply the capabilities assessment carefully. As Wilson states, "There will never be enough resources to satisfy all the nation's wants. Thus, we must make *strategic choices*, establish requirements, set priorities, make decisions, and allocate scarce resources to the most critical needs."[11] The application of the ODP Model must, therefore, be in tight concert with the threat and vulnerabilities assessments and be aligned to each discipline and its strategies, goals, and objectives. It is beyond the purview of this paper to do that comprehensively. One gap that has become evident is the application of each segment of the Cycle of Preparedness to the major disciplines, with comments on the capabilities needed to accommodate some tasks within that portion of the Cycle. This is the topic of the next sections.

Cycle of Preparedness

The Cycle of Preparedness represents a process for the assessment of objectives and description of capabilities needed on a discipline-by-discipline approach, using all thirty disciplines described earlier. While this is neither comprehensive nor specific to any particular jurisdiction, it can serve as a model of application.

PREVENTION

The first of the components of the Cycle of Preparedness is Prevention, consisting of Collaboration, Information Sharing, Threat Recognition, Target Hardening or Risk management, and Intervention. Arguably, most of the disciplines should be involved in the "Collaboration" aspects of Prevention. When we assess the objectives of Collaboration, we gain some specificity, however. We will use the different foci to represent the various disciplines associated with Collaboration and each element of Prevention, along with comments on the capabilities needed to successfully attend to the element.

If the objective of Collaboration is to facilitate Information Sharing, the next element of Prevention, the principal disciplines include some public agencies (Law Enforcement, EMA, and Homeland Security, for example) and some private agencies (such as Financial Institutions). This objective of Collaboration, as used here, would be to develop the predicate of collegiality in order to share information to forewarn of a threat or attack, and identify those individuals likely to be involved in the attack. Law Enforcement is the primary discipline in this strategic process. The **National Strategy for Homeland Security** makes it clear that the "roles and responsibilities" for intelligence and information analysis are vested primarily in law enforcement. Since the Emergency Management Agency is so critically involved in every aspect of preparedness, response, and recovery, it seems prudent to include that discipline. Similarly, in the section of the **National Strategy for Homeland Security** titled "Domestic Counterterrorism," there is the stated need to "investigate suspicious financial transactions in order to uncover and prosecute terrorist financing and develop predictive models to help identify future illegal financing"[12] specifying that law enforcement should serve as the lead agency, in concert with Homeland Security. The **Prevention and Deterrence Guidelines** also found that the private sector could be critical to gathering information on the identity of suspicious persons, locations of cells, and movement of persons of interest. These five disciplines, if they are to share information, must collaborate.

The capabilities needed to facilitate collaboration include knowledge of key contacts, social capital, and mutual respect; the physical and technological compatibility to implement the collaboration; and the semantic interoperability to communicate effectively. An underlying capability needed is the motivation to engage in collaboration, enhancing or facilitating the process. That can be represented by plans and processes that are inclusive of the agencies and the representatives, rather than exclusive.

If the objective of Collaboration is Threat Recognition, the disciplines already mentioned are still key but, additionally, those agencies with personnel who might observe events in the preparatory phases, recognize

them as indications of a terrorist threat, have mechanisms for relaying the information and have established a collaborative process for relaying the information, become critical. These disciplines include Emergency Dispatch Communications or Health Services and Public Health, each of which might recognize a pattern of calls suggesting an emerging threat, or Private Security personnel who might recognize patterns in absenteeism or unusual activities. Again, in this category of Prevention, it is the collaborative relationships and pathways that represent the capabilities needed for Preparedness.

These disciplines have information gathered through the normal course of their services, that could forewarn of a threat or provide valuable information to law enforcement, if collaboration has been established. Capabilities needed to facilitate the collaboration are the means (knowledge of key contacts, social capital, and mutual respect; the physical and technological compatibility to implement the collaboration; and the "semantic interoperability" or common language, terms, and terminology to communicate effectively) and the motivation to engage in the sharing of information that could lead to threat recognition. Additional capabilities include the knowledge of behavioral cues that would lead an observer to identify the person or the actions as a potential threat, the knowledge of appropriate response to the behavior, and the present ability to share the information with the correct agencies and people.

If the objective of Collaboration is Target Hardening or Risk Management, arguably, many other disciplines would now be fully engaged in the process. The Private Sector, and those other private agencies with 85 percent of the Nation's critical infrastructure, would have particular need to establish a collaborative relationship with those agencies possessing intelligence so that the correct potential targets could be hardened. Plans, based on collaborative relationships, could be more effectively developed by Business Continuity, Educational Institutions, and other disciplines.

The collaboration processes become much more complex as we move along the other elements of the Cycle and there is the need for discipline-specific capabilities that still revolve around means and motivations. Again, it is critical that there be a central facilitator if collaboration with so many diverse disciplines is to be effective. Semantic interoperability is a key constraint but motivation (partnership, inclusiveness, quid pro quo) is the key enabler. Again, the **Prevention and Deterrence Guidelines** provides some excellent examples of tasks and activities that represent desired capabilities to accomplish target hardening.

If the objective of Collaboration is Intervention, a few key disciplines are most associated with the element. These are Law Enforcement, Prosecutors, Homeland Security, Governmental Administrators, and the Military. Unless collaborative relationships have been established in advance, far less will be accomplished on a timely basis.

The exact scope and nature of the threat, the number and types of attackers, and the capabilities of the enemy, to include the type of weapons thought to be possessed, each determine the disciplines engaged in successful intervention. Capabilities for this objective of Collaboration could go beyond the somewhat intangible and social ones mentioned earlier, and require access to sufficient force and personal to effect the apprehension successfully, public protection, containing the threat, and executing the process in a legally-regular and acceptable fashion.

Other papers in this series will address Prevention, Response, and Recovery so the conceptual basis of these components of the Cycle of Preparedness will not be fully discussed here. However, it will be instructive to list each of the elements of Preparedness with some examples of the disciplines and the necessary capabilities. First we will address the elements of Prevention:[13]

COLLABORATION

Some of the major tasks and activities associated with Collaboration include:

- Establish a system, center, or task force to serve as a "clearing house" for all potentially relevant domestically generated terrorism data and information, ensuring interpretation and assessment of the data and information.
    - Disciplines: Law Enforcement, EMA, Homeland Security, Private Security, Loss Prevention.
    - Capabilities: Technical, social, and physical connectivity. Motivation to engage in the process.
- Prepare MOUs and formal coordination agreements between appropriate agencies (public and private) describing mechanisms to exchange information regarding vulnerabilities and risks, coordination of responses, and processes to facilitate information sharing and multi-jurisdictional preemption of terrorist acts or events.
    - Disciplines: Governmental Administrative, Homeland Security, Law Enforcement, Fire, EMS, EMA, HazMat, Public Health, Private Sector.
    - Capabilities: Technical, social, and physical connectivity. Common definitions, terms, understanding of "need to know" restrictions. Plans and protocols. Motivation to engage in the process.
- Explicitly develop "social capital" through collaboration between the private sector, law enforcement and other partners so that data, information, assistance, and "best practices" may be shared and collaborative processes developed.
    - Disciplines: All.
    - Capabilities: Means for establishing connectivity and motivation to engage in collaboration.

INFORMATION SHARING

Some of the major tasks and activities associated with Information Sharing include:

- Enhance analytic capabilities for linking information on potential threats.
    - Disciplines: Principally Law Enforcement, EMA, and Homeland Security.
    - Capabilities: Technical, tactical, and investigative abilities to establish fusion centers with gathering, analysis, and dissemination plans.

- Establish a framework for sharing information/intelligence and prevention strategies, on a "need to know" basis, particularly between Law Enforcement and other agencies.
    - Disciplines: Principally Law Enforcement, EMA, and Homeland Security.
    - Capabilities: Technical, tactical, and investigative abilities to establish fusion centers with gathering, analysis, and dissemination plans. Knowledge of and conformity to legal restrictions. Establish common definitions for data as well as information.
- Ensure reliable capability to alert officials and emergency personnel of terrorism threats, with warnings initiated, received, and relayed to alert or inform key decision makers and emergency personnel regardless of the threat or operational involvement, as well as a robust, redundant, timely system for sharing information with other agencies, organizations, and the public.
    - Disciplines: EMA, Homeland Security, Public Information, Media Management, Public Warning/Alert
    - Capabilities: Technical ability to establish reliable warning systems, voice and data, with connectivity to all appropriate users.
- Establish a multi-disciplinary approach to public information for education and awareness and protective action information.
    - Disciplines: All.
    - Capabilities: Awareness level for all disciplines, by threat (CBRNE), with detailed information (shielding, secure in place, personal protection, prophylaxis)
- Develop a dynamic, adaptive, organic architecture facilitating information sharing.
    - Disciplines: All.
    - Capabilities: Establishment of plans and procedures nimble and adaptive enough to accommodate asymmetric nature of terrorism.
- Provide sufficient information to appropriate agencies to allow investigation and prosecution of criminal conspiring to commit terrorist attacks.
    - Disciplines: Law Enforcement, Prosecution, Governmental Administrative.
    - Capabilities: Information gathering system sufficient to generate actionable intelligence. Legal mechanisms to disseminate and act on the information.

THREAT RECOGNITION

Some of the major tasks and activities associated with Threat Recognition include:

- Map infrastructure threats and capabilities for preemptive action.
    - Disciplines: Law Enforcement, EMA, Homeland Security, Fire, Public Works, Private Sector, Major Events, HazMat, Information Technology, Private Security, Public Places, Transportation, Utilities, Conveyances.
    - Capabilities: Technical, social, and physical connectivity. Common definitions, terms, understanding of "need to know" restrictions. Plans and protocols. Inventory of assets. Motivation to engage in the process.

- Train law enforcement personnel and others, using standard definitions, criteria, and terms, to recognize as clearly as possible the behavioral, observable, and legal criteria to establish a suspected terrorist.
    - Disciplines: Law Enforcement, EMS, Fire, Public Works, Health Care, Private Security.
    - Capabilities: Technical, social, and physical connectivity. Common definitions, terms, understanding of "need to know" restrictions. Plans and protocols. Knowledge of behavioral cues. Motivation to engage in the process.
- Develop chemical, biological, and nuclear recognition and tracking systems in public and private sectors, consistent with threat and risk analysis models.
    - Disciplines: Law Enforcement, EMS, Fire, Public Works, Health Care, Private Security, Public Health, Transportation, Military.
    - Capabilities: Technical equipment and training in calibration and utilization.
- Maintain current and complete inventory and accountability system for hazardous materials and biological agents, even during transporting, coupled with procedures for reporting irregularities.
    - Disciplines: Law Enforcement, EMS, Fire, Public Works, Health Care, Private Security, Public Health, Educational Institutions, Transportation, Conveyances, Military.
    - Capabilities: Technical, social, and physical connectivity between agencies, laboratories, and individuals. Common definitions, terms, understanding of "need to know" restrictions. Plans and protocols. Motivation to engage in the process.
- Recognize the threat potential for land, air, water, rail, and mass transit, and other elements of the critical infrastructure, consistent with an analytical risk assessment model, and recommend appropriate prevention strategies.
    - Disciplines: Law Enforcement, EMS, Fire, Public Works, Health Care, Private Security, Public Health, Educational Institutions, Transportation, Conveyances, Military.
    - Capabilities: Technical, social, and physical connectivity between public and private sectors. Common definitions, terms, understanding of "need to know" restrictions. Plans and protocols. Motivation to engage in the process.

Some of the major tasks and activities associated with Target Hardening include:

- Adopt or develop an appropriate analytic "risk management" model to assess risk or vulnerability and identify probable treatment methods to reduce risk.
    - Disciplines: All.
    - Capabilities: Analytical ability and recommended models. Motivation to engage in assessments.
- Assist and collaborate with the private sector to (1) identify the most serious vulnerabilities and risks, while suggesting the use of a common analytical model, (2) collaborate with the private sector to implement risk management (target hardening), and (3) inform the private sector of threats and efforts that could be taken to prevent incidents or minimize damage, in concert with the actions taken by public sector agencies
    - Disciplines: All.
    - Capabilities: Analytical, technical, and theoretical ability to understand and apply approaches. Motivation to engage in applications.
- Identify and include in planning documents innovative approaches to disrupt potential actions of terrorists at strategic locations or during sensitive times (such as religious holidays or anniversaries of events).
    - Disciplines: Law Enforcement, Fire, EMS, EMA, HazMat, Private Sector.
    - Capabilities: Knowledge, technology, and personnel to engage in activities. Motivation to engage in the activities.
- Conduct vaccinations, as appropriate, to reduce vulnerability to biological agents.
    - Disciplines: EMA, Public Health, Health Services, Public Information, Media Management.
    - Capabilities: Sufficient pharmaceuticals, robust process of assessing risk, motivation to participate.
- Establish or review quarantine authorities and include in the risk management plan and model, levels of isolation and quarantine to prevent contamination or infection of unaffected persons or places.
    - Disciplines: Governmental Administration, EMA, Public Health, Health Services, Law Enforcement, Military, Public Information, Media Management.
    - Capabilities: Analytical risk sufficient to establish probable events and preferred responses. Dissemination process. Motivation to participate.

INTERVENTION

Some of the major tasks and activities associated with Intervention include:

- Train law enforcement personnel in tactical capabilities with special teams of law enforcement, emergency response, and military resources, to respond quickly and appropriately during a potential terrorism event, with the objective of intervening in an impending attack.
    - Disciplines: Law Enforcement, Governmental Administrative, EMA, Military.
    - Capabilities: Sufficient knowledge, technical resources, and adequate plans to accomplish intervention.
- As indicated in an analytical Risk Management Model, establish plans and needs assessments for deployment of resources to meet known or anticipated threats to preempt or deter events.
    - Disciplines: Law Enforcement, Governmental Administrative, EMA, Military.
    - Capabilities: Sufficient knowledge, technical resources, and adequate plans to accomplish intervention.

Response

The response to an attack or threat is the segment of the Cycle of Preparedness that has attracted the most attention since 1999. The Office for State and Local Domestic Preparedness Support, the predecessor of the Office for Domestic Preparedness, was focused on enhancing the ability of jurisdictions to respond to a threat or an attack. Carafano, for example, states "Emergency preparedness and response includes the preparation, response, and recovery from a terrorist attack, including planning, logistical support, maintenance and diagnostics, training, and management as well as supporting the actual activities at a disaster site and post-recovery after the incident."[14] While response is necessarily and by definition "reactive," a great deal of planning is implemented pre hoc so that disciplines and capabilities can be identified.

The National Response Plan provides the following guidance:

Response includes activities to address the immediate and short-term actions to preserve life, property, environment, and the social, economic, and political structure of the community. Response activities include:

1. Emergency shelter, housing, food, water and ice;
2. Search and rescue;
3. Emergency medical and mortuary services;
4. Public health and safety;
5. Decontamination following a chemical, biological or radiological attack;
6. Removal of threats to the environment;

7. Emergency restoration of critical services (electric power, water, sewer, telephone);
8. Transportation, logistics, and other emergency services;
9. Private sector provision of needed goods and services through contracts or donations; and
10. Secure crime scene, investigate and collect evidence.[15]

These activities, while broad in scope, provide information on the mobilization of disciplines to respond to an event. There are, however, problems associated with a timely and organized response. As stated in the National Strategy for Homeland Security:

> Americans respond with great skill and courage to emergencies. There are, however, too many seams in our current response plans and capabilities. Today, at least five different plans—the Federal Response Plan, the National Contingency Plan, the Interagency Domestic Terrorism Concept of Operations Plan, the Federal Radiological Emergency Response Plan, and a nascent bioterrorism response plan—govern the federal government's response. These plans and the government's overarching policy for counterterrorism are based on a distinction between "crisis management" and "consequence management." In addition, different organizations at different levels of the government have put in place different incident management systems and communications equipment. All too often, these systems and equipment do not function together well enough.[16]

While this statement suggests (and in other parts of the National Strategy for Homeland Security it states) that "crisis management" is an outdated term to describe the initial phase of response, it is a term that is sufficiently focused that we reintroduce it here. In 1975, Kupperman, Wilcox and Smith[17] introduced the term as a process used by a manager to meet goals during the deteriorating situation of a crisis. It implies that correct allocation of resources, accurate communications, and appropriate decisions—effective and efficient—must be made in the urgency of the situation. The preferred term seems to be "incident management" and the National Incident Management System (NIMS) serves as the operational arm of the national response to an intentional or natural disaster. The development of NIMS does provide structure and common terms and terminology so that incidents are more likely to be managed properly. The use of the Incident Command System, Unified Command, and Multi-Agency Coordination Systems make it more likely that an incident will be managed in an organized and orchestrated fashion. The benefit of the concept of "crisis management" is the description of an initial, urgent response, followed by a more measured response as the NIMS is fully implemented.

Some of the tasks[18] that are encountered early in the response phase (crisis management), and the disciplines associated with them are:

- Identify agents based on signs and symptoms. (Be able to recognize illness and/or injury caused by different WMD agents based on presenting signs and symptoms. Be able to recognize trends in victim signs and symptoms to indicate a WMD incident. Differentiate WMD casualties from more common illnesses based on agent-specific signs and symptoms.)

- Perform victim rescue. Be able to extricate victims from site while ensuring self protection by understanding risks and utilizing proper protective measures based on knowledge of agents and toxic effects and triaging victims, "walking wounded," and "walking worried."
    - Disciplines: First Responders, such as Fire, EMS, Law Enforcement, as well as others who might be "first observers" such as Private Security, Public Works, and Health Services.
    - Capabilities: Knowledge of signs and symptoms, by type of agent or pathogen, ability to connect multiple events or victims, awareness of potential attacks, ability to maintain personal protection during response, and the methods for relaying information to the central repository.

These disciplines are responsible for the initial life saving, scene protecting activities. As was evident in New York City on September 11, 2001, these responders face significant dangers in fulfilling their roles. Their responsibilities place them in harms way and, depending upon the type of incident, the capabilities needed include personal protection equipment, interoperable communications, materials, resources, and personnel sufficient to rescue, remove, and treat the initial victims, while mitigating the harm potential.

In the next phase (there may be only minutes per phase) of an incident, additional disciplines become fully engaged. Some tasks associated with this phase include:

- Control the scene. Understand and identify differences in control zones (i.e. hot, warm and cold zones). Secure or isolate the incident scene by managing ingress and egress, preventing contaminated persons from leaving and on-lookers from entering.
- Coordinate evacuation/sheltering and protect in place activities. Know general population protection through consequence analysis. Be able to determine and implement appropriate protective measures, including shelters (public or in place), instructions regarding traffic control, and mass care measures.
    - Disciplines: First Responders, such as Fire, EMS, Law Enforcement, as well as HAZMAT, EMA, Major Events, Private Security, Public Health, Public Works, and Health Services.
    - Capabilities: Knowledge of special risks associated with a terrorist attack (secondary devices, plumes, wash and drainage), ability to maintain personal protection during response, legal aspects of response, presence of response plans, ability to work in ICS, and the methods for relaying information to the central repository.

As the incident matures, the incident management should become smoother and more measured. That is not to suggest that a calm occurs. Surge capacity in medial facilities, for example, and transportation difficulties in the removal of victims and transport to treatment facilities is delayed, cause significant problems. The incident management has likely segued into the "consequence management" phases, even as transport, treatment and mitigation of victims is occurring.

Some tasks likely to cycle into the incident at this stage, depending of course on the type of incident, are:

- Coordinate human services to include shelter, health, and welfare for emotional and physical needs. Know and understand mass care plan implementation through needs assessment.
- Coordinate public warning, instruction, and information updates. Direct the timely, accurate, and unified release of public information, emergency instructions, and public alerts. Conduct an effective public information campaign, ensuring all releases are coordinated. Develop an organized warning alert information and dispersion process through centralized control and coordination.
    - Disciplines: All.
    - Capabilities: Plans to guide the process, a structure, such as ICS to manage the process, sufficient resources to accommodate the needs of the agencies, facilities, and citizens, and the willingness (motivation) to work together to mitigate the harm while gathering evidence and information for the identification and prosecution of suspects.

At this stage as crisis management and *consequence management* merge, all disciplines are engaged. The capabilities vary depending on the phase at which the discipline enters the incident, as well as the level or tier of activity to which they have been trained. Those requiring the most resources are those in the most dangerous, and critical positions in the incident ("warm" and "hot" zones of certain types of incidents). This observation is supported by the types of materials and equipment, as well as personnel needs and capabilities, identified through various after-action reports.

Depending on the most likely threat, the greatest vulnerabilities, potential consequences, and available resources, agencies and organizations can identify the human, social, and technical materials, resources, and equipment needed to adequately respond to an incident.

Recovery

Recovery is the element in the Cycle of Preparedness that has been given the least direct attention in the literature. That is not to depreciate the importance of recovery, it is simply to note that recovery is so dependent upon the type of incident that it cannot easily or even effectively be planned until the magnitude of the event is determined. No jurisdiction can constantly maintain preparations for the recovery from most apocalyptic event.

The National Response Plan says this of recovery:
Recovery involves actions, and the implementation of programs, needed to help individuals and communities return to normal. Recovery programs are designed to assist victims and their families, restore institutions to sustain economic growth and confidence, rebuild destroyed property, and reconstitute government operations

and services. Recovery actions often extend long after the incident itself. Recovery programs include mitigation components designed to avoid damage from future incidents. Typical recovery actions may include:

1. Repair and replacement of disaster damaged public facilities (roads, bridges, municipal buildings, schools, hospitals, qualified non-profits);
2. Debris cleanup and removal;
3. Temporary housing and other assistance for disasters victims and their families;
4. Low-interest loans to help individuals and businesses with long-term rebuilding and mitigation measures;
5. Restoration of public services (electric power, water, sewer, telephone);
6. Crisis counseling and mental health;
7. Disaster unemployment; and
8. Planning and programs for long-term economic stabilization, community recovery and mitigation.

Clearly it is possible to have contingency plans, memoranda of understanding, redundant capabilities for the most critical of activities, and resources to support the recovery plans. All disciplines are engaged in the recovery process and some of the tasks associated with that process include:[19]

- Coordinate structural recovery and "cleanup." Be able to design and implement a program of recovery and restoration of facilities. Coordinate site rehabilitation through assessment and evaluation.
- Understand and exercise as appropriate, emergency powers and declarations among local, state, private, and federal entities. Review or develop inter-jurisdictional emergency powers agreements. Review legal authorities and define process to execute emergency powers and declare emergency.
- Coordinate clean up with contractors. Understand critical factors that must be considered or evaluated in order to coordinate the remediation of a WMD site with contractors, law enforcement, public works, private sector, and public health. Know emergency management and intergovernmental agency relationships and responsibilities.
- Integrate criminal investigation with epidemiological investigation.
- Administrative documentation completion. Prepare concise and accurate reports and communications. Be familiar with all appropriate forms and reports and documents needed during and after an event.

The capabilities required of each discipline, are determined by the discipline, the objective, and the event—type and magnitude. It would be impossible to list or even provide sufficient examples of the capabilities needed without employing a risk management model.

Conclusion

The purpose of this paper was to describe, with some particularity, the disciplines associated with a terrorist threat or event. In a general sense, "capabilities" was used to establish the need for a reliable method of assessing preparedness needs, by threat, vulnerability and risk. Tasks associated with each of the major categories in the Cycle of Preparedness were presented as examples and some mention of the disciplines and capabilities associated with the tasks or the stage of the event were included. These examples are far from complete. They are presented only to sever as examples. In reality, the interrelationship between and among the disciplines is the key factor in the success or failure of the stage of the Cycle. In graphic terms, that interrelationship determines the magnitude of the incident and the extent of the damage.

In 1999 Philip Anderson described a strategic management approach that appears to have utility here. He was describing how and under what circumstances complex organizations can develop more effective ways of solving emerging problems.

> Complex adaptive system models represent a genuinely new way of simplifying the complex... Applying complex adaptive systems models to strategic management leads to an emphasis on building systems that can rapidly evolve effective adaptive solutions.[20]

These sentiments were later reflected in an article by Comfort who focused on the process of "auto-adaptation" during a terrorist threat or incident. "Auto-adaptation offers a mode of improving intergovernmental coordination in response to extreme events."[21] The model she described "builds on the human ability to learn and adapt to new information, but acknowledges that this capacity can only occur with the support of an appropriate information infrastructure." That is the objective here: create a set of auto-adaptive systems within the disciplines so that whatever the threat, event, or hazard, the collective organizations will be able to effectively and nimbly adapt to the exigencies.

[1] For a complete set of the disciplines and the definitions for each, see Appendix to this paper.

[2] Dahrendorf, Ralf. **Class and Class Conflict** in Industrial Society, Stanford: Stanford University Press, 1959.

[3] William V. Pelfrey, William D. Kelley, Jr., and John W. May, Jr. **The Office for Domestic Preparedness Training Strategy.** Washington, DC: U.S. Department of Justice, Office of Justice Programs, Office for Domestic Preparedness, 2002. (Also published in electronic form by Community Research Associates, Inc., under Cooperative Agreement WMD-97-281-CRA-3354.)

[4] George W. Bush. "**Homeland Security Presidential Directive 8: National Preparedness**" December 17, 2003, p. 2.

[5] Office for Domestic Preparedness, **ODP Jurisdictional Handbook** (2003) p. xi.

[6] Office for Domestic Preparedness, **ODP State Handbook** (2003) p. 188.

[7] Office for Domestic Preparedness, **ODP State Handbook** (2003) p. 185.

[8] http://hazmat.dot.gov/risk.htm. Similar information is available in the document, by ICF Consulting, **Risk Management Framework for Hazardous Materials Transportation. Washington, DC: U.S. Department of Transportation**, Research and Special Programs Administration, 2000.

[9] General Accounting Office. "Rail Safety and Security: Some Actions Already Taken to Enhance Rail Security, but Risk-based Plan Needed." **Report to Congressional Requesters** GAO-03-435. April 2003. p. 27.

[10] Systems Management College. **Systems Engineering Fundamentals**. U.S. Department of Defense. 2001 (Retrieved via http://www.dau.mil/pubs/pdf/SEFGuide%2001-01.pdf) P. 134.

[11] Wilson, Isaiah. "Analyzing the Shift from a Threat-based to Capabilities-based Approach to U.S. strategic Planning." Unpublished paper, United States Military Academy, April 2002. p. 3.

[12] Office of Homeland Security. (2002). National Strategy for Homeland Security. Washington, DC: Government Printing Office. P. 28.

[13] These tasks are extracted from Office for Domestic Preparedness. **Guidelines for Homeland Security: Prevention and Deterrence**. Washington, DC: Department of Homeland Security, June, 2003, mentioned in this document as "Prevention and Deterrence Guidelines."

[14] Carafano, James Jay. "Preparing Responders to Respond: The Challenges to Emergency Preparedness in the 21st Century." **Heritage Lectures**. No. 812. October 22, 2003.

[15] Department of Homeland Security, **Draft National Response Plan**, February 25, 2004. p. 16.
Office of Homeland Security. (2002). **National Strategy for Homeland Security**. Washington, DC: Government Printing Office. P. 42.

[16] Kupperman, Robert H., Richard H. Wilcox, and Harvey A. Smith. "Crisis Management: Some Opportunities." **Science**. Vol. 187 (4175), February 7, 1975. pp. 404-410.

[17] The tasks presented in the sections Response and Recovery are adapted from some developed and described in William V. Pelfrey, William D. Kelley, Jr., and John W. May, Jr. **The Office for Domestic Preparedness Training Strategy**. Washington, DC: U.S. Department of Justice, Office of Justice Programs, Office for Domestic Preparedness, 2002. (Also published in electronic form by Community Research Associates, Inc., under Cooperative Agreement WMD-97-281-CRA-3354.).

[18] Again, these tasks are drawn from **The Office for Domestic Preparedness Training Strategy.**

[19] Anderson, P. (1999). "Complexity Theory and Organization Science." **Organization Science 10**(3): 216-232.

[21] Comfort, L. K. (2002). "Managing Intergovernmental Responses to Terrorism and Other Extreme Events." **Publius: The Journal of Federalism** 32(4): 29-49.

This monograph may only be used in connection with the Office of Domestic Preparedness Officer Professional Development Program during calendar years 2004 and 2005.

This monograph has been licensed from William V. Pelfrey by Teleologic Learning LLC for limited purposes. No reproduction or further distribution is allowed under penalty of law.

Copyrighted in 2004 by William V. Pelfrey. All rights reserved.

Quotation of this material for ordinary professional or academic purposes is allowed with attribution to William V. Pelfrey.