ASSESSING THE UNCONVENTIONAL MODES OF TERRORISM: CYBER, CHEMICAL, BIOLOGICAL, AND NUCLEAR

D. V. LeMone, Ph.D., P.G.
University of Texas at El Paso
P.O. Box 3, 500 West University
El Paso Texas, 79968

S. G. Gibbs, Ph.D.
1100 North Stanton, Suite 110 C
University of Texas Health Science Center at Houston School of Public Health
El Paso, Texas 79902

J. W. Winston, Jr., M.S.
Radiological Physics, Inc.
4333 Donnybrook Place
El Paso, Texas 79902

ABSTRACT

Conventional terrorism may be defined as encompassing assassination, kidnapping, hostage taking, and non-radiological/nuclear explosive devices. What is currently necessary is to evaluate the four modes of unconventional terrorism (cyber, biological, chemical, and nuclear) in order to rank them in order of their importance and, consequently, prioritize those areas in which our limited national human, operational, and financial resources are to be allocated. All four unconventional modes have historical records.

Two fundamental terror weapon types are recognized, each resulting in a different pattern of consequences: weapons of mass destruction (WMD), weapons of mass disruption or hysteria (WMH). Suitability of weapon type is determined on availability, level of security encountered, low- or high-technical knowledge required, personnel to be used, weapon deliverability, and cost.

Any realistic evaluation of these four modes will require an analysis of what the impact each of these actions would have upon the national infrastructure and, consequently, the defense and economic security of the United States. Any evaluation should also include potential physiological and psychological trauma in terms of chronic and acute impacts on individuals and the population of the local region. Several analytical approaches are possible; the consensus seems to be expert systems.

All four unconventional modes have potentially disastrous results and will require a hardened infrastructure and a determined political will to overcome such actions should they occur. In ranking the potential damage and the impact on the public and the infrastructure, the sequence would seem to be (from most to least critical): Cyber-terrorism, Bioterrorism, Nuclear Terrorism, and Chemical Terrorism.

INTRODUCTION

Since the events of September 11, 2001, there has been a major shift in governmental policy and public thinking with reference to the security of our national infrastructure. Standard procedures have long been in place for what may be referred to as conventional terrorism, which would include assassination, kidnapping, hostage taking, and non-radioactive/nuclear explosive devices. The potentially disastrous unconventional terrorist threats to the infrastructure are fourfold: cyber, biological, chemical, and nuclear. All of these come with historical precedent. Therefore, it would be desirable to develop a ranked

evaluation of the level of risk of each of these modes. The purpose of ranking is to establish prioritization and allocation of the available human and financial resources of the nation. In order to more clearly visualize the problem, three fundamental factors need to be addressed: the national infrastructure, the potential deliverability of weapon systems, and the assessment of the national and transnational adversaries.

Infrastructure

President Clinton's Executive Order 13010 (1996) defines the infrastructures that are critical to the defense and economic security of the United States. That definition of eight infrastructures remains valid today; they are: electrical power; gas and oil production, storage, and delivery; telecommunications; banking and finance; water supply systems; transportation; emergency services; and governmental operations. All of these infrastructures rely on computers, computer networks, and the internet. [1]

Deliverability

Weapon deliverability depends on weapon type, device size, and whether its mode of transport is low-tech or high tech. Individuals transporting weapons by foot, bicycles, cars, trucks, rowboats, or planes may be considered to be low-tech delivery methods. Transnational terrorist organizations and weaker nation states in today's world, unwilling to confront a major enemy, invariably use these systems [2]. The actual development and low-tech deliverability of so-called and most feared nuclear suitcase bombs, as well as their size and yield, is debatable.

High tech delivery is via missiles. Missiles are normally classified into a series of five different categories: short range ballistic missiles (SRBM) < 1000 km; medium range ballistic missiles (MRBM) 1001-3000 km; intermediate range ballistic missiles (IRBM) 3001-5000 km; intercontinental range ballistic missiles (ICBM) 5000 km+; and submarine launched ballistic missiles (SLBM) (range not available). [3,4] The development and accessibility of these missiles is increasing available to rogue nations, especially in short and medium ranges. Advances in technical sophistication to high tech levels invariably leaves footprints that cannot be hidden.

Transnational And Nation State Adversaries

Hamme's (2004) geopolitical thesis is a vision of the future that includes antagonistic transnationals and those nation states influencing other nation states to act against global and/or American interests. If this view is reasonable and correct, it requires some additional thought as to future strategies are to be used with current and future 21st century adversaries. [2]

Transnationals, organizations that owe no allegiance to any nation state, include such groups as religious sects, narcotic traffickers, etc. Al Qaeda is such a group. Laqueur [5] clearly tracks the centuries old history of terrorism that has been used by the far left, extreme right, radical nationalists, and fanatical religious sects. It would seem that the use of terrorism is more a strategy to gain power, not to support an ideology. He points out that "old terrorism" was primarily against the "establishment," whereas, the modern, Al Qaeda type is aimed at the indiscriminate annihilation of a generalized enemy. An examination of the Al Qaeda Manual [5] should clarify their aims. Additionally, Laqueur [6] has mapped the global distribution of some 25 terrorist organizations and summarizes the geography of international terrorist incidents from 1995-2003 (e.g., Middle East. 335 attacks, 5582 casualties; South America, 996 attacks, 440 casualties).

Hamme [2] analyzes Al-Qaeda as a vertical, hierarchical system of control with power concentrated at the top. The organization is divided into three divisions: Islamic studies, financial, and military. Islamic

studies is responsible for indoctrinating trainees in organization dogma, establishing schools for recruitment and public acceptance, and developing a scholar's group to support dogma. The financial unit deals in maintaining the financial integrity of the organization by maintaining cash flow and disbursement of funds in addition to producing cyber-related financial terrorism. The military cadres are divided into basic, advanced, and specialized units. Their military manual is 7,000 pages in length and issued in 11 volumes. The first 10 volumes are on CD. The 11th volume is restricted and deals with chemical and biological warfare [2].

China is an example of a nation state influencing other nation states to act against global and/or American interests. [2] Qiao and Wang [7] outline the strategy of having third party nations attacking and crippling the nation's information and economic infrastructure. This infrastructure carries the larger part of national logistical and administrative data. The release of technology in the construction of weapons of mass destruction and missile capability to antagonistic states (Iraq, Iran, North Korea) would validate this thesis. It has also been suggested that the Chinese helped Pakistan become a nuclear power to bind up India in their continuing dispute, thus avoiding India's concerns in reference to the Himalayan region.

NATIONAL RESPONSE PLAN

The Department of Homeland Security (DHS) in January released the National Response Plan (NRP). [51] The report covers the full range of the complex, continually changing, interagency and multi-jurisdictional requirements, including: anticipation and response to the threats or acts of terrorism, major and lesser disasters (natural and man-made), and provides a basis for mitigation and long-term community recovery. The NRP develops a responsible chain of command as well as a sequence of actions from local (city, county) to state and tribal to the national level of concern. It provides the basis for and the subsequent routes for the declaration of an Incident of National Significance (INS), which will require DHS coordination. The National Incident Management System (NIMS) (March 2004) together with the NRP amalgamates the capabilities and resources of the governmental entities (signed off by 15 Departmental Secretaries [e.g., Treasury] and 14 agencies [e.g., EPA]), non-governmental organizations (NGOs) (signed off by 3 organizations [e.g., American Red Cross]), and the private sector into a seamless blueprint for domestic incident management. [51]

Implementation of the NRP will be a three-phased system. Phase I (Transition Period, 0-60 days) is the time given for all of the signatory agencies above to come into line by: modifying their training, designating a staff for NRP, and becoming familiar with NRP processes, structures, and protocols. Phase II (Plan Modification Period, 60-120 days) provides time for the departments and agencies to have the opportunity to modify existing Federal interagency plans in order to integrate with NRP. Phase III (Initial Implementation and Testing Period, 120 days-1 year) is the time in which the plan is fully implemented. DHS will assess the implementation process and evaluate its effectiveness in line with the specific objectives outlined in Homeland Security Presidential Directive (HSPD-5 - Management of Domestic Incidents, issued 2/28/03). After an initial first year review, the NRP will initiate a 4-year review and re-issuance cycle. [51] The National Response Plan in combination with National Incident Management System should provide an adequate template for combating unconventional terror on the Federal level. [51]

National security concerns on unconventional terrorism concerns can be broken down into four broad categories: cyber-terrorism, bioterrorism, chemical terrorism, and nuclear terrorism. Examination of these of each of these four concerns should allow for a non-numerical evaluation of the magnitude of each.

CYBER-TERRORISM

Cyber-terrorism may be defined as the execution of an attack to disable, disrupt, or destroy a nation's

critical electronic information infrastructures. With the now-universal utilization of the internet, the question of information security is of paramount concern. The central problem encountered in cyber-terrorism is the software utilized. For example, it is of concern that today software development is in part being outsourced (e.g., India, China, etc.). Mossberg (2004)[8] is of the opinion that Microsoft's Windows-based PC is the central element in the development of a criminal class of virus and spyware writers. Tens of billions of dollars in sales of Windows-based software comes with inadequate security measures. The money and effort spent correcting these internal flaws is deplorable. It has, however, given rise to a cottage industry in patching the system. Apple-based systems are considered by many to be more secure and superior; however, their use accounts for only 2% to 5% usage. [8]

Symantec estimates 50 new software vulnerabilities/week and 100 new viruses/week. [9] In 2003-2004 the estimated costs to businesses of the six major viruses (Sasser, NetSky, MyDoom, SoBig, Blaster, Slammer) is placed at 17 billion dollars. Cost for viruses in the preceding 4 years (1999-2002) was 16.25 billion dollars (mainly Klez, CodeRed, LoveBug, Melissa), with LoveBug being the worst in 2000 at a cost of 8.75 billion dollars. [11] Most viruses and useware prey to a great degree on Microsoft Operation Systems. Industry pays a large cost for choosing, overwhelmingly, to use Microsoft software.

Viruses and worms are mostly distributed by E-mail and are the result of malicious intent, ego-tripping, or criminal purpose. E-mail, however, is not the only delivery mechanism. Some viruses on infected PCs will infect vulnerable systems by attacking known network software vulnerabilities. Others attack unsuspecting users through malicious web sites.

Recently, the development of spyware and phishing, both of which are web-based vulnerabilities, has introduced a new method of potential criminal and terrorist utilization. [10] Spyware programs monitor a user's keystrokes to steal information (e.g., passwords). Phishing for credit card data involves the "hijacking" of a web site in order to steal their identity so that when a user posts confidential information on it, the data are revealed. "Mimicking" has been suggested as a more accurate term than phishing. The phenomenon has been growing at a rate of over 110% per month.

Wireless networking is visibly taking the market with sales increasing from 4.5 million wireless devices in 2002 to 27.7 million being projected for 2005. [12] Popular, low cost wireless networking connecting with mainframe computers evolved from old hard-wired desktops to easily secured mobile laptops using modems and phone lines to the wireless systems of today. Unfortunately, wireless probes (beacons) do not distinguish between authorized and unauthorized users. The result is that formerly secure corporate systems are being breached. Additionally, this technology allows drive-by viruses to be sent from laptop to computer. The hacker at the airport, sitting with his laptop, could be probing for your password and credit card data. Unfortunately this is only the tip of the iceberg. All in all, there are major flaws in security with or without cyber terror. Basically, wireless communications are insecure or insufficiently secure. [13] Major industry players, as well as developers, are working on resolving this, but still lag behind with development of systems under current technology.

As discussed earlier [14], the world of this century is a globally integrated web of international businesses, corporations, and financial institutions. The internet data transmitted by these entities are vulnerable to such scenarios as threats, attacks (both directly and as Trojan horses), and viruses. Further examples of the problem's dimensions are network flooding resulting in "denial of services" by overloading certain targeted internet services, criminal and/or terrorist intrusions into corporate intranets through firewalls erected to protect internal data, and failure to implement safeguards which now have compounded problems with the recognition of internet anonymity. [15] Properly confined secure systems are in general secure enough; however, attackers are constantly developing new technologies and discovering new vulnerabilities, making security an ever changing process, not an end.

Military and governmental entities are in the process of developing new equipment and tighter procedures for handling "sensitive" and "secret" data. The Nuclear Regulatory Commission (NRC), immediately after 9/11, removed data from their website (e.g., schematics of nuclear power plants, documents related to scenarios and responses to severe accidents, etc.). The Department of Energy (DOE) has removed sensitive data concerning locations of all nuclear storage facilities, reactors, surplus plutonium sites, etc. [1] In general, reassessment of security is always desirable. New threats and technology may change the need to secure specific data.

In response to these challenges, a new area of security for modern digital communication has been evolving. Encryption of messages by multiple means is one of several developed and developing solutions. Parallel to secure data transmission concerns is the fundamental problem of the identification and authentication of an individual, not only within the areas vulnerable to cyber-terrorism, but also in any potentially sensitive area. In order to solve this relatively universal security problem, it is necessary to implement the technology of the rapidly evolving discipline of biometric security. Chirillo and Blaul [16] state that for today's obligatory verification multiple processes must be applied (i.e., electronic identification card and uniquely recognizable physical and/or behavioral biometrics). Physical biometrics consists of seven or more features: fingerprints (pattern); facial recognition/location (measurements); hand geometry (shape and pattern analysis); iris scan (features of the colored ring of the eye); retinal scan (blood vessel analysis); vascular patterns (vein patterns); and DNA (genetic analysis). [16] Behavioral biometrics include: speaker/voice recognition, signature/handwriting analysis, and keystroke/patterning. [16]

In terms of the vulnerability of the physical layer connecting systems to the internet, the greatest threat is the detonation of a strong atmospheric nuclear blast capable of generating an electromagnetic pulse (EMP). This nanosecond pulse is capable of knocking offline, either temporarily or permanently, both unprotected computer systems and network components. Weldon [4] also points out another worrisome device that works on the same principle, the radio frequency (RF) weapon which is small, highly portable, and capable of delivering a similar EMP blast to individual unprotected electronic targets. The 9 cooperating agencies of the critical Cyber Incident Annex are developing a coordinated, broad-based, multidisciplinary plan to prepare for, respond to, and recover from cyber-related impacts.

CHEMICAL TERRORISM

Chemical terrorism has a long list of agents that may be used as weapons. These agents kill, maim, debilitate (acutely and also chronically), and have genetic implications that appear in succeeding generations (e.g., the severe birth effects occurring in Iraqi Kurdish children). Chemical agents are typically liquid and dependent on their volatility and rates of reaction for effectiveness. Therefore, such natural conditions as the surface they are deposited on, temperature, humidity, wind direction, and wind velocity are critical. Normally chemical agents are heavier than air and have a tendency to drain into lower topography. Chemical agents may be broadly classified on the basis of the reactions they elicit to the human system as: nerve, blister (vesicant), and choking (pulmonary irritants) [17].

Nerve agents disrupt the muscle functions of the body. Large doses are lethal and are preceded by a tight chest, blurred vision, nausea, convulsions, and coma. Sarin, developed in the 1930s, is lethal by either inhalation or skin contact. The Japanese sarin nerve gas attacks that occurred in Matsumoto (1994) and in Tokyo's subway (1995 with 29 deaths) are recent examples of the random use of chemical warfare agents against the general public. In this incidence the perpetrators were the Aum Shinrikyo, a Doomsday cult. This cult in 1995 was politically active in Japan, had some 10,000 members with offices in 20 Japanese cities as well as in the United States, Russia, Germany, and Sri Lanka. Yeso Seto [18] details the forensic analysis and identification of the nerve gas agent used and ultimate tracking to its source and the identification of the guilty participants. [17] Nerve agents are listed into a G series: GA (tabun), GB

(sarin), GD (soman), and GF (cyclosrin), named for the German teams that created them during and shortly after WW II. The second somewhat oily nerve agents are listed in the V series (VE, VG, VM, VX). These agents are 10 times more toxic than sarin (GB) and are persistent agents (not easily degraded or washed away). [19]

Three common blistering (vesicant) agents are: mustard gas, lewisite, and phosgene oxime. Mustard gas was used extensively in World War I (WW I). It causes blistering on exposed parts of the body as well as affecting the internal organs. Blindness usually preceded respiratory failure and death.

Choking (pulmonary irritant) agents are typified by chlorine and phosgene gases, which damage the respiratory system. Such an agent first appears as a minor irritant and is followed 4-5 hours later by pulmonary edema which fills the lungs with water and suffocates the subject to death. Phosgene is cited for 80% of the American chemical fatalities in WW I. Chlorine gas, a strong upper and lower respiratory tract irritant, is included in this category. [17, 20] After World War I the 1925 Geneva Protocol (Rules of War) prohibited further use of chemical and biological weapons (the protocol was never ratified by the United States), and has long been ignored by terrorist organizations. All of these chemical weapons are now classified as weapons of mass destruction (WMD) (UN Resolution 687). Production and stockpiling of chemical weapons was outlawed by the Chemical Weapons Convention of 1993 (brought into force as so 4/29/97). [19]

Rieders [21] divides chemical weapons into two major categories: "stand-up" chemical weapons and "stealth" chemical weapons. The "stand-up" or sudden bio-impact variety of chemical agent has an immediate adverse effect on the exposed life forms. The "stealth" or delayed bio-impact agents are produced to deliver a delayed toxicity. These agents are activated by the body's metabolic processes (toxic bio-transformation). Chemical weapons invariable leave unique "chemical finger prints". These chemical agents utilize thickeners to increase the viscosity and stickiness, stabilizers to prevent early release, and carriers to aid in distribution. Additionally, additives such as the reagents in which the agent is dissolved in, aerosols, explosive agents, and penetrators (for breaching the clothing and skin) are forensically traceable elements. Organizations or nation states proven to be involved in chemical terrorism invite an attributable retaliatory response. [21,22].
Chemical terrorism does not have an independent NRP Annex. It is referred to in the Oil and Hazardous Materials Incident Annex Scope as a hazardous material (WMD chemical agents). It is also referred to within the Planning Assumptions and Considerations of the Terrorist Incident Law Enforcement and Investigation Annex as chemical materials.

BIOTERRORISM

Regen [23] enumerates four key factors to evaluate the threat of bioterrorism today: first, an increasing number of nations are processing, seeking, or acquiring biological weapons; second, production of genetically modified organisms (GMOs); third, detection of biowarfare development is difficult to establish, because it is intertwined with agriculture and medicine; and lastly, applied bioagents may not only have incubation periods of days but also be difficult to diagnose.

Biological warfare is defined as the utilization of living organisms (plants, fungi, bacteria, etc.) and/or their toxins to harm, incapacitate, or exterminate an adversary's military forces, civilian population, flora, and/or fauna, including livestock [24]. This can be accomplished by utilization of any naturally occurring living organism, including the modern genetically modified ones, and/or bioactive substances. These, consequently, may be delivered either by increasingly proliferating conventional warheads [49] or by less technologically advanced civilian delivery means (e.g., anthrax through the mail system) [25]

Chaudhuri and others [24] conclude that biological weapons are nearly impossible to detect and control because new biotoxins are being discovered every day. They list some 86 wild and cultivated plants that are toxic to animals (human). The capsules and seeds of the castor bean *(Ricinis communis),* for example, are the source of ricin. The biotoxin ricin is 6,000 times more poisonous than cyanide and 12,000 times more lethal than rattlesnake venom. Add to this the fact that today, by utilizing genetic technology, we can modify old biotoxins with recombinant DNA manipulation methodology to make them more effective. [25].

The written history of biological warfare records use in India, China, and the Roman Empire in the ancient world. The Romans routinely fouled besieged stronghold water supplies with dead animals. The legendary Kisha Kanya was a maid from India with a poison touch. Rotting bodies and poisonous plants were used in China. The Black Death (bubonic plague) was launched by Tartars catapulting cadavers into the Crimean city of Caffa (Feyodosiya). British policy in the 1700s was to issue smallpox-infested blankets to the Native Americans. [26] During World War I the Germans in South America and Europe reportedly used anthrax on cattle.

Since the attack of September 11, 2001, we have seen bioterrorism by letter-delivered assaults using silica-coated, modified anthrax here in the U.S. [25] Bioterrorism refers to the non-specific targeting of individuals or a population in order to maximize the psychological impact even when it results in low casualties. The indiscriminate nature of the offense separates the perpetrators from either guerilla or combatant status under the Geneva Convention. Hoaxes and threats alone produce psychosis even where actual deployment is not made [23]. It is appropriate to remember that; "…infectious biological agents are on the order of a thousand to a million times more hazardous than chemical agents." (E. Steubing, Head Aerosol Sciences, U.S. Army, Edgewood). [27]

In 1995, the CIA indicated that 18 nations were involved in bioweapon research. That research included natural biotoxins as well as their GMOs. Nature also has gifted humanity with relatively newly emerged human infectious viruses (Ebola, HIV, and West Nile). Additionally, the last two decades has seen new strains of tuberculosis, diphtheria, and cholera, which have arrived by means of mutation, resistance to antibiotics, and other processes of natural selection [25]

Relative low cost genetic engineering (genetic technology, gene cloning, recombinant DNA technology, etc.) is a specialized discipline started in the 1970s, and it has recorded explosive growth since that time. [25] It manipulates recombinant DNA in order to alter the genetic constitution of cells or individuals by inserting a piece of foreign DNA [25], thereby altering the activity of a specific gene or set of genes.

Biotoxin is a poisonous substance that is synthesized and stored in a living organism or, after hydrolysis, can produce a toxic chemical. "Phytotoxin" specifies that the toxic chemical is from a plant source (e.g., alkaloids = tobacco, atropine, quinine; glycosides = poisonous nightshade, sprouting potato plant, etc.). Toxigenes are created by genetic engineering. Chaudhuri and others [24] list common wild and cultivated plants and those parts that are lethal to animals (e.g., Azalea (leaf), Laurel (leaf and flower), Loco Weed (all parts), etc.)

Sarkar [28] reviews examples of toxic poisoning throughout the marine food web. These poisons include both cytotoxins (classified in five different areas of cell damage) and neurotoxins (classified in three areas as to damage to the central nerve system). The most potent toxin from natural marine sources is Ciguatoxin, which has been isolated in the viscera of the moray eel, within the tissues of some 36 species of other poisonous fishes, and in algal dinoflagellates. It exhibits a powerful excitatory effect on smooth and cardiac muscles. In a purified form, a toxin like botulism is approximately 2 million times more lethal than sarin (chemical agent). [28]

Epidemics, the occurrence of cases of an illness clearly in excess of expectancy, have been with us since the advent of man and have had a profound effect on history. Here in America, as an example, Philadelphia was laid waste by mosquito-borne yellow fever in 1793. At that time it was the largest city in the U.S. and the capital. It suffered 5,000 casualties or 9% of the population (55,000). [29].

Public health surveillance has a reasonably good record in retrospective studies. In the advent of biological warfare, there is concern that the incubation and consequent spread of the bioagents used may be well advanced before being detected; for example, forms such as anthrax are lethal if not diagnosed early [30].

Two approaches define epidemiology: classic (tracking number and patterns of cases) and molecular (tracking the genetic makeup of the pathogen). The classic approach utilizes the epidemic curve which summarizes the rate of new case increase, considering also such confounders as seasonality, long-term trends, past outbreaks, etc. [30] An example of the molecular approach would be the development of a phylogenetic tree describing the molecular makeup of a new pathogen. An effective responding system to an epidemic must combine rapidity, accuracy, sensitivity, and, hopefully, have an early-interpreted output. The basic purpose of this or any system dealing with an epidemic is the rapid verification of the pathogen of concern at either the hospital or the physician interface. The confirmation of pathogen kind enables the ordering of such actions as: quarantine, vaccination, and/or specific treatment(s) to the populace.

The Center for Disease Control and Prevention (CDC) acts as a clearinghouse for disease information. The major problem has not only been communication between doctors and the CDC but also between doctors and hospitals. The emerging difficulties associated with maintaining patient privacy are also producing problems [31]. The CDC classifies biotoxins as Class A, B, or C. Class A is of the greatest concern (e.g., anthrax, plague, smallpox, tularemia, and 32 others). These are those agents producing rapid death, causing significant societal disruptions, and having the capability of spreading terror within the civilian population. Class B listing include Q fever, typhus, etc., whereas Class C concerns emerging infectious diseases like hantavirus. [23]

The victims of bioterrorism are typically the elderly and those with either immature or weakened immune systems. Deliverability is not that great a problem as many of these forms are virulent, resilient, easily cultivated, possibly weaponized (like anthrax), and transferable and releasable as aerosols in a variety of systems ranging from sophisticated to primitive. The World Health Organization (WHO) estimates that 60 kg of anthrax spores used on a population of 500,000 would lead to a lethal dose of 95,000 (LD_{19}) with some 125,000 hospitalized. The CDC estimates that a small crop duster plane dusting a 100,000-person suburb would have a LD_{20} and produce 25 billion dollars of damage. A single infected individual could infect a multitude of others before symptoms were visible. [23]

Older stock bioagent vaccines may no longer be viable because of either evolution of the form or development of a genetically engineered form. Side effects can only be guessed at. Time and cost necessary for the generation of a new vaccine is another aspect of the problem. Bacteria require antibiotics. Unlike vaccines, antibiotics react with other medications, have side effects, and are taken daily. Furthermore, antibiotics may not necessarily be effective against bacterial strains, their toxins, or GMOs. [23, 32]

The Department of Homeland Security (DHS) is currently spending 60 million dollars annually on environmental detectors that monitor outdoor air for bioweapons. Many, however, consider them ineffective. Earlier biodetection efforts resulted in a device deployed nationwide (30 major cities). An additional 32 million dollars has been used to launch 14 outside research teams to develop a high-priority

detect-to-treat systems (identify bioagents within 3 hours) and detect-to-protect (identify within 2 minutes). [27].

In response to the bioterrorism threat, President Bush proposed the formation of a biodefense BioShield program that will be funded for 6 billion dollars during the next decade [48]. BioShield has been formed to spur the development and procurement of the next generation of medical bio-measures, such as vaccines, as well as basic research in microbial geonomics. In addition to BioShield, there are two other counter-terrorism projects under development. The first, Baywatch, is an interagency effort to produce an early warning system using atmospheric sampling technology for the detection of potentially hazardous bioagents. The second project is Biosensor that has been formed to reduce the time lag between the release of bioagent and the time it takes officials to react. These programs and others were addressed at the second Federal Defense Research Conference held in Washington, D.C. It would seem that those organizations and nation states involved in bioterrorism, as with chemical terrorism, run a considerable risk of leaving a forensic trail [21], inviting an attributable retaliatory response. [22]

The NRP Biological Incident Annex includes more than a reaction to biological terrorism event. It also monitors pandemic influenza, emerging infectious diseases, and novel pathogen outbreaks. The biologically related Food and Agriculture Annexis scheduled to be published in a subsequent version of the NRP. [51]

NUCLEAR TERRORISM

The areas of concern in nuclear terror are fourfold: the physical facilities of the nuclear power cycle from the front end (exploration and mining) to the back end (waste repository), transportation and interim storage of nuclear materials, radiation dispersal devices (RDDs) [50] (a.k.a. "dirty bombs"), and nuclear weaponry.

The nuclear power cycle is vulnerable to the risks of terrorism. Each step in the process from mine facilities to repository structures is susceptible. The fundamental target within the cycle would seem to be the operational nuclear power plant reactor. These plants are vulnerable to terrorist bombs delivered by air (9/11 by airliners), water (USS Cole by dinghy), and land (1995 Oklahoma City Federal Building by truck). All power plants are to an extent vulnerable from the air; however, air space has been and is restricted in addition to the facilities typically having a heavily hardened encasement. Plants on land are often placed close association to available water, thereby producing another basic parameter to be considered in plant security.

Plants need to be individually examined as to their vulnerability. The ideal approach is to develop an integrated blend of solid engineering designs that will give the most robust protection for the plant. Campagna and Sawruk [45] use an approach of full spectrum risk analysis. This concept is based on an evaluation of the individual plant's strengths (positive features), weaknesses (areas of vulnerability), opportunities (positive improvements not currently planned), and threats (downside risks, anything that can go wrong). In addition to evaluating these four items for the individual plant, they stress that a properly equipped, well-trained, and highly motivated security force is the fundamental key for successful security. [45] The necessity of such a force is often overlooked in these systems. Pools and dry storage casks are potential targets when associated with plants in addition to the reactor and its system.

The transportation of radioactive materials or wastes has been of intense interest to the public for the last three decades. Considerable efforts by the government and the industry have been made to promote the safety of the system. Recently (2002) the Department of Energy (DOE) has published a resource handbook (National Transportation Program) which formulates the basis for conducting transportation risk assessments. [46] A substantial increase in transportation activity in the immediate future is certain.

The most familiar transportation model is the one involving transuranic waste (TRU) being transported to the WIPP facility at Carlsbad. DOE, taking only non-commercial TRU waste, estimates that the facility will be receiving approximately 38,000 truck shipments from 22 sites over the next 35 years. [46] If legal-weight truck transportation is required for the transport of spent nuclear fuel rods (SNF), it should require some 50,000 truck shipments and 300 rail shipments over a 24 year period from the 72 commercial and 5 DOE sites. [46] The transport of TRU waste is a very unlikely target. The potential risk with reference to SNFs, special nuclear fuels, and high-level waste is difficult to assess.

In the nuclear weapons area, the primary and continuing concerns have been with the control and proliferation of nuclear weapons of mass destruction and the security of commercial nuclear power plants. A less dramatic aspect of the nuclear problem is that posed by radiation dispersal devices (RDDs). These devices are not detonated by fission and fusion nuclear reactions; the Department of Defense defines RDDs as any device, weapon, or equipment that is designed utilize radioactive materials by disseminating them in order to cause destruction, damage, or injury by decay of such material. [14] High security subcritical highly enriched uranium (HEU), weapons grade uranium (WGU), and high-level waste could be used as an unlikely source material, in the broadest sense of the definition.

The primary source materials for these devices are either sealed radioactive sources (SRSs) and/or greater than class C low-level (GTCC) radiation materials. Among the more important issues today is the monitoring and recovery of operational and lost, spent, and disused (orphan) sealed sources along with the legacy, military, and civilian accumulating masses of Greater Than Class C low-level waste (GTCC). Serious radioactive dispersal devices (RDDs) can be made from both of these sources. [14]

The IAEA categorizes 11 radioisotopes of concern from their perspective of safety; they are: Co-60, Cs-137, Ir-192, Sr-90, Am-241, Cf-252, Pu-238, Ra-226, Pd-103, Kr-85, and Tl-204. [22] The legacy radium from earlier sealed radioactive sources (SRSs) is no longer a major concern. The Center for Nonproliferation Studies (CNS) classifies only the first seven radioisotopes of the IAEA list (Co-60, Cs-137, Ir-192, Sr-90, Am-241, Cf-252, Pu-238) to be of concern and identifies them as the reactor-produced radioisotopes that pose the greatest security risks [3] The problem is that these radioisotopes and their devices have extensive industrial and medical users. As a result of this, there are 10's of thousands of end users and the consequent potential for radionuclide loss, theft, or abandonment.

Ferguson and others [3] separate the seven reactor-produced radioisotopes that are primarily either major gamma and/or beta sources (Co-60, Cs-137, Ir-192, Sr-90) or major alpha sources (Am-241, Cf-252, Pu-238). The most important commercial reactor-produced sources utilizable for RDDs are Co-60 (pellets) and Cs-137 (powder). The accidental releases of these radionuclides in Juarez [33] and Goiana [34, 35] clearly indicate the potential dangers involved. Accelerator-produced isotopes, legacy DOE GTCC waste, and operational and decommissioned GTCC wastes are also potential, but less likely, sources.

The tactical effects of an RDD are dependent on delivery style, target location, effectiveness of conventional detonation, and most critically on type and quantity of radioactive material. The result of the use of standard and sophisticated RDDs is: blast and fragmentation effects; immediate and long-term radiation exposures; and instillation of fear and panic in the target population. The multiple strategic purposes of RDDs are: to inflict deep psychological damage; to induce panic and disruption in the target population with a resultant chaotic situation at and adjacent to the site of detonation; to deliver political impact for either military or domestic purposes; and, lastly, to wreak economic damage from the ensuing requisite cleanup.

RDDs are not normally thought of as weapons of mass destruction (WMD). [47] It would probably be preferable to refer to them as either weapons of mass disruption, dislocation, or as weapons of mass hysteria (WMH). [14] This problem is addressed in assessment of events involving RDDs. [36] On an international basis the IAEA has developed procedures for the handling, conditioning, and storage of SRSs. [37] The Government Accounting Office has reported on the international assistance efforts to control SRSs. [38]

The fission or fusion nuclear device is the ultimate terrorist weapon. The reality is, that even in cruder forms, it is a lethal and devastating device. Mining the available scientific data and website sources (e.g., the Wisconsin Project), it is possible to gain a good concept of either the construction of a tubular Hiroshima gun-type or a soccer ball implosion-type device. This has been driven home by the recent revelations coming out of the abandonment of Libya's nuclear Program and the discovery of a complete design, reported too heavy for a scud, but O.K. for a family-size car. The source of this black market design would appear to be from Pakistanian A. A. Khan's infamous nuclear "Walmart" operation. The extent of the damage done by this individual's organization is yet to be determined. [39]

Assuming that a device can be constructed, what is the potential damage? The estimate of casualties for a 10-kiloton device exploded in Times Square would be 1 million; even for a 1-kiloton device there would be 250,000 casualties. [36] Once you had the device, how do you deliver it? It is possible to deliver it by airfreight to the some 430 commercial airports. The most logical way would be by containerized sea-land freight that today forms the bulk of movement by national and international transport. It is not reassuring to know that a reporter last year sent 15 pounds of depleted uranium encased in a steel lead-lined pipe from Jakarta, Indonesia, to the Los Angeles Convention Center. [39] Add to this mix the porous American land borders. They are some 7500 miles long, with entrances from Canada and Mexico controlled by 300 border crossings. Native American reservations with margins on the international border are not patrolled. If you want to get into the country from the outside, all that is necessary is to follow the paths of the drug traffickers. The 12,400 miles of the American seacoasts with their some 300 deepwater seaports presents a further problem. [39]

The saving grace in this system is the need for highly enriched uranium (HEU) (+20% U-235), weapons grade uranium (+90% U-235), and Pu-239. Natural uranium consists of roughly 99.7% U-238, 0.7% U-235, and a trace of U-239. The ore has to be mined and processed to yellow cake form. It is then converted to uranium hexafloride gas at 133^{o}F. At this point, U-235 is concentrated, normally by a cascade of 1500 gaseous ultra centrifuges, from the U-238 by using the difference in their masses. One year is normally the time needed to collect enough U-235 to produce a bomb. Thirty-five pounds of weapons grade uranium with a beryllium reflector makes a bomb; without the reflector, it requires 100 pounds. Pu-239, formed in reactors when an additional neutron is melded onto the nucleus of U-238, is obtained from the recycling of reactor fuel rods. Only 9 pounds of weapons grade plutonium is necessary to construct a bomb; without the reflector, 33 pounds are necessary. [39] The only real non-nation state source of material is that from abandoned or stolen from a facility. Otherwise, it has to be supplied by one of the nation states.

The option to use nuclear devices cannot be hidden. [52] Nation states supplying terrorists cannot escape their responsibility, as they are the only possible source of weapons grade materials. However, the ultimate global control of these devices is only possible through an internationally rigorously enforced system of nonproliferation and safeguards.

The 28 page Annex on Nuclear/Radiological Incident of the National Response Plan (NRP) records 6 coordinating agencies (DoD, DOE, DHS, EPA, NASA, and NRC) and an additional 17 cooperating agencies. Response coordination to INS and other incidents includes: technical data

management and protective action recommendation, as well as Public Information, Congressional, White House, and International data coordination. The Annex has provisions for such areas as victim decontamination and population monitoring and recovery. It has an imbedded advisory team for environment, food, and health. The concluding section of this Annex provides a chart listing the responsibilities of the 22 directly affected entities.

RISK ANALYSIS

Unconventional terrorist threats are basically developed in four modes with reference to the security of our national infrastructure: cyber-, biological, chemical, and nuclear terrorism. Assuming a successful scenario develops in any one of these modes, what would the consequences to the populace and the infrastructure be? Given the fact that there are limited resources available for protection and reaction, where should they be expended? The responsibility for determining the risks and the allocation of monies rests squarely on the appropriate legislative and executive branches of the government.

The concept of risk has different meanings dependent on context and the individual(s) that are evaluating it. As an example these risks could easily be classified as extreme events in that they are rare, severe, and outside the normal range of experience and thus require the probability approaches of Bier and others. [40] Risk, normal and extreme, can also be split into four broad areas. [41, 44] Risk Assessment is the area of science and hard risk data, with some scientific judgments to be given by expert witnesses to bridge the gaps in our knowledge. Risk Management deals with such areas as the regulatory issues and requirements, technical feasibility, social values, and economic impacts. Comparative (Relative) Risk is what has to be done to set priorities on ranking the impacts to the infrastructure, public health, environment, societal framework, and economics in order to formulate policy. Risk Communication is easily mishandled, often times by the politicians and the media, resulting in risk exaggeration, emphasizing drama over scientific fact, and politicizing issues. [42]

Edwards-Winslow [42] observes that the public perception of risk and its consequence fears often are not correlatable to technical assessment. Public reactions to natural versus artificial (man-made) risks are quite different. Natural disasters (e.g., earthquakes, volcanic eruptions, etc.) are acceptable. In the case of an artificial disaster, there is a scapegoat, and it is an outrage. Attitude hardening of the public is easier with natural risks; it is unforgivable with regards to artificial risk. Risk is also a function of familiarity, exotic risk is of higher concern. It is like comparing the levels of fear in the general public to Sarin gas (exotic) versus chlorine gas (familiar). [42]

Risk may be considered to be a function of three variables: Threat (likelihood and scenarios), vulnerability (potential targets), and consequences (public health, safety, economic impacts, etc.). [43] System vulnerability and consequences are more reasonably estimated than the evaluation of likelihood and scenarios. Vulnerabilities and consequences for each target scenario incident can be estimated and ranked. Each of numerous scenarios with requisite likelihood of development, however, would require the use of experts from a broad spectrum of disciplines. [43] It would seem that it is necessary to develop a series of estimates based on individual potential scenarios in order to arrive at a numerical solution. The numerical solution giving us a ranking number which will enable us to build a model for reaction. As in the case of all models, the question of the validity of the assumptions made in development of the model is always open to critique and reevaluation. Even in light of the tenuous assumptions being made herein, the risk model assessment does provide a platform for the formulation of a hopefully more reasonable series of policies.

CONCLUSIONS

The identification of threats and the determination of the consequent vulnerabilities will most likely require a policy of immediate reaction and continued vigilance. Therefore, the advancement of four terrorism incident reaction plans will be required to meet this challenge, plans that are now, in part, addressed by the NRP. These plans include the issuance of both a general or mission statement and a more specific reaction policy statement for each of the four terror mode areas. The reaction policy statements need to reflect such areas as: potential utilization and deployment of first responders, governmental and private resources, and, if needed, the military assets. Transparency of these operations is absolutely necessary to prevent inadvertent chaos and hysteria produced by irresponsible media and others. Properly applied, any risk analysis is a work in progress that varies as more data become available and as perceptions change.

Cyber-terrorism is separated into a special category as it is not one of those modes that requires a mobile response body, as do the others. The impact of future disasters, as always, will fall directly upon local first responders. The use and overall adoption of the National Guard program on development of chemical, biological, radiological, nuclear, high-yield explosive (CBRNE) response units would seem to be an excellent approach on the state level. [2] On the national level the best model would seem to be specialist groups in each terror mode in regional offices to assist, evaluate and advise local and state personnel. The organizational structure of specialist groups could follow the most efficient model developed by Public Health.

Informally categorized on the basis of impact to the infrastructure, the ranking would seem to be: cyber-, biological, nuclear, and chemical. In relation to lethality, the ranking would be: nuclear, biological, chemical, and cyber. The solution to the problem of terrorism would seem to be the development of a global policy wherein the nations of the world outlaw terror in the same manner as piracy on the high seas: no safe haven and an automatic death sentence upon conviction.

REFERENCES

[1] D. Erton, "Black Ice: The Invisible Threat of Cyber-Terrorism," McGraw-Hill Companies/Osborne, Emeryville, CA, 273 p. (2003)

[2] T. X. Hamme, "The Sling and the Stone: On War in the 21st Century," Zenith Press, 321 p. (2004)

[3] C. D. Ferguson, T. Kazi, And J. Perera, "Commercial Radioactive Sources: Surveying the Security Risks," Monterrey Institute for International Studies, Center for Nonproliferation Studies, Occasional Paper no. 11, 55 p. (2003)

[4] C. Weldon, "Overview: Preparing America for the 21st Century," in S.K. Majumdar, et al. (eds.) Science, Technology, and National Security, Pennsylvania Academy of Science, p. 1-9 (2002)

[5] W. Laqueur (ed.), Voices of Terror, Reed Press, New York, 520 p. (2004)

[6] W. Laqueur, The Geography of Terror, National Geographic, vol. 206, p. 72-81 (2004)

[7] L. Qiao, and X. Wang, "Unrestricted Warfare: China's Master Plan to Destroy America, NewsMax.com, West Palm Beach, Florida (2002)

[8] W. S. Mossberg, "Personal Technology," Wall Street Journal, p. B1, 12/2/04 (2004)

[9] D. Bank,, "Bush is Pressed to Boost Security on Information–Technology Front," Wall Street Journal, p. A3, A10 12/7/04, (2004)

[10] D. Bank, "Keeping Information Safe," Wall Street Journal, p. B1, B6, 11/11/04 (2004)

[11] C. Bryan-Low and L. Rousek, "Police Target Sensitive 29A' Virus Creators," Wall Street J0ournal, B1, B7, 12/2/04 (2004)

[12] W. M. Buckeley, " Wireless Mischief," Wall Street Journal, p. B1, B6 (2004)

[13] D. Nasow, "Command Centered Launched to Fight Instant-Message Viruses," Wall Street Journal, page D8, 12/7/04, (2004)

[14] D. V. LeMone, "Sealed Radioactive Sources and Greater than Class C Low-Level Wastes (GTCC): Potential Radioactive Dispersal Devices (RDD) Resources," Waste Management 2004, Session 55, Paper 2 (4525), Management of Spent and Disused Radioactive Sealed Sources, 15 p., published on CD-ROM, (2004)

[15] J. Omura, J. Spilker, Jr., and P. Baran, "The Evolution of Modern Digital Communications Security Technologies," in S.K. Majumdar, et al. (eds.) Science, Technology, and National Security, Pennsylvania Academy of Science, Chapter 15, p. 160-185 (2002)

[16] J. Chirillo and S. Blaul, "Implementing Biometric Security," Wiley Technological Publishing, Indianapolis, IN, 414 p. (2003)

[17] F. Bolz, Jr., K.J. Dudonis, and D.P. Schulz, The Counterterrorism Handbook: Tactics, Procedures and Techniques, CRC Press, 278 p.

[18] Y. Seto, "Sarin Gas Attacks in Japan and Forensic Investigations - A case Report" in S.K. Majumdar, et al. (eds.) Science, Technology, and National Security, Pennsylvania Academy of Science, Chapter 5, p. 62-73 (2002).

[19] Wickipedia, http://en.wickipedia.org/wiki/Nerve_gas

[20] R. F. Knouss, Inside and Outside the Loop: Defining Population at Risk in Bioterrorism, in J. N. Kayyem and R. L. Pangi (eds.) First to Arrive, MIT Press, Cambridge, p. 121-134 (2003)

[21] M.F. Rieders, "Issues in Homeland Security: Forensic Evidence in Real or Perceived Exposure to Chemical substances," in S.K. Majundar, et al. (eds.) Science, Technology, and National Security, Pennsylvania Academy of Science, chapter 4, p. 47-61 (2002).

[22] J. Lemley and A. Whitworth, "Homeland Security Perspectives, Radwaste, v. 32, no. 1, p. 31-33 (2004)

[23] J.J. Regens, "The Nature of the Bioterrorism Threat," Session 19-Panel: Alliances, Fear Factors, or Weakest Links - Surviving Global Energy Challenges in Uncertain Times, WM 03, 7 p. (2003)

[24] R. K. Chaduri, D. C. Pal, and I. Chaduri, "Plants and Toxins as Biowarfare Weapons," in S. K. Majumdar, et al. (eds.), Science, Technology and National Security, Pennsylvania Academy of Science, p. 30-46 (2002)

[25] S. K. Majumbar, J. H. Tchaicha, A. C. Donaghy, and C. M. Marc, "Biotechnology and Biological Warfare: A Review with Special Reference to the Anthrax Attack in the U.S.," in S. K. Majumbar et al. (eds.) Science, Technology and National Security, Pennsylvania Academy of Science, 10-29 (2002)

[26] R.S. Bray, "Armies of Pestilence," Barnes and Noble Books, 258 p. (2000)

[27] K. Brown, "Up in the Air," Science; v. 305, 27 August 2004, p. 1228-1229 (2000)

[28] A. Sarkar, "Marine Toxins and Their Toxicological Significance: An Overview," in S. K. Majumdar, et al. (eds.), Science, Technology and National Security, Pennsylvania Academy of Science, 47-61 (2002)

[29] W. Tsou, "Putting it together: Bioterrorism and Public Health," in S. K. Majumdar, et al. (eds.), Science, Technology and National Security, Pennsylvania Academy of Science, 113-121 (2002)

[30] T. Burr, K. Apt, K Budlong-Sylvester, W.D. Stanbro, and C.A. Wells, Institute for Nuclear Materials Management, In Transactions, LA-UR-02-3204, 7 p.

[31] P. Dehne, "Preparing for and responding to conventional and unconventional warfare," in S. K. Majumdar, et al. (eds.), Science, Technology and National Security, Pennsylvania Academy of Science, p. 97-112 (2002)

[32] C.E. Mathur, "Vaccines and Civilian Security against Biological Weapons," in S. K. Majumdar, et al. (eds.), Science, Technology and National Security, Pennsylvania Academy of Science, 89-96 (2002)

[33] G. Molina, "Lessons learned during the recovery operations in the Cuidad Juarez accident," IAEASM-316/53 (1986)

[34] International Atomic Energy Agency, "Management for the prevention of accidents from disused radioactive sources," IAEA-TECDOC-1205, Vienna (2001)

[35] International Atomic Energy Agency, "Dosimetric and medical aspects of the radiological accident in Goiania in 1987," IAEA-TECDOC-1009, Vienna (1998)
[36] American Nuclear Society, "The scientific basis for communication about events involving radioactive disposal devices," Report to Homeland Security, 158 p. (2003)
[37] International Atomic Energy, "Handling, conditioning, and storage of sealed radioactive sources," AGENCY IAEA-TECDOC-1145, Vienna (2001)
[38] Government Accounting Office, "Nuclear Nonproliferation, U. S. and International
[39] G. T. Allison, "Nuclear Terrorism: The Ultimate Preventable Catastrophe," Henry Holt and Company, New York, 263 p. (2004)
[40] V. M. Bier, Y. Y. Haimes, J. H. Lambert, N. C. Natalas, and R. Zimmerman, "A survey of approaches for assessing and managing the risk of extremes," Risk Analysis, 19 (1): 83-94 (1999)
[41] L. Goldman, "Statement on Risk Assessment," given 11/17/93 before Subcommittee on Transportation and Hazardous Materials of the Committee of Energy and Commerce, House of Representatives (1993)
[42] F. Edwards-Winslow, "Telling it like it is: The Role of Media in Terrorism Response and Recovery," in J. N. Kayyem and R. L. Pangl (eds.), First to Arrive: State and Local Responses to Terrorism, M.I.T. Press, Cambridge, Mass., p.59-76.
[43] J. P. Indusi, "A Relative Risk Assessment approach to Homeland Security System Planning," Proceeding of the 44th Annual Meeting of the Institute of Nuclear Materials Management, 4 p. (2003)
[44] National Academy of Science/National Research Council, "Risk Assessment in the Federal Government: Managing the Process Report," Report to Congress (1983)
[45] M. Campagna and W. Sawruk, "Protection of Nuclear Plants against Vehicular Bombs via Full Spectrum Risk Analysis," 44th Annual Institute of Nuclear Materials Management, 8 p. (2003)
[46] S. Y. Chen and A. Kapoor, "The Resource Handbook on DOE Transportation Risk Assessment," Session 63, Special Topics in the Packaging and Transportation of Radioactive Materials, WM'03, 8 p. (2003)
[47] International Atomic Energy Agency, "Categorization of radiation sources," IAEA-TECDOC-1191, Vienna (2000)
[48] K. Koizumi, "AAAS Co-sponsors Biodefense Research Talks," (December 2003) www.scienceonline.org (2003)
[49] J. C. Moltz, "New Challenges in Missile Proliferation, Missile Defense, and Space Security," Monterrey Institute for International Studies, Center for Nonproliferation Studies, Occasional Paper No. 12, 72 p. (2003)
[50] J. L. Ford, "Radiological Dispersal Devices: Assessing the Transnational Threat," Center for Counterproliferation Research, Number 136, March (1998) Assistance Efforts to Control Sealed Radioactive Sources Needs Strengthening, GAO-03- 638, 104 p. (2003)
[51] Department of Homeland Security, "National Response Plan," 417 p. (December 2004)
[52] Charleton, W. S., et al., "Nuclear Forensics Technique for Attributing Material used in a Radiological Dispersal Device Event," 45th Proceeding of INMM, 8 p. (2004)