2010-09-00

Homeland Insecurity Thinking about CBRN Terrorism

Mauroni, Albert J.

Monterey, California. Naval Postgraduate School

Homeland Security Affairs (September 2010), v.6 no.3

Homeland Insecurity: Thinking About CBRN Terrorism

Albert J. Mauroni

As the U.S. government has seen a change of administrations, there is an opportunity for a constructive review of how the Department of Homeland Security (DHS) has addressed the threat of chemical, biological, radiological, and nuclear (CBRN) terrorism in terms of policy development and execution to date. Our current homeland security approach to CBRN terrorism seems to have its basis in the incidents of 9/11 and the U.S. anthrax attacks in October-November 2001. However, our history of homeland defense goes back to 1941 (at least); to understand from a policy perspective how the government ought to address domestic CBRN terrorism, we need to put it all in context.

This essay examines the issues of how DHS has prepared for chemical, biological, radiological, and nuclear terrorism incidents. DHS should address these threats in a consistent and holistic manner, but instead the federal government has developed singular hazard-based approaches to each threat. DHS has not assessed its efforts to address CBRN terrorism or identified where DHS could improve, and as a result we see merely the continuation of previous initiatives. The essay concludes with some recommendations on how DHS could improve this area with better policy practices.

Words Are Important

The term "WMD" was the word of the year in 2002, but quickly fell into abuse as a term of political rhetoric and comedic punch lines. It was originally developed in 1948 by the United Nations as an accepted arms control term to describe the nation-state use of nuclear, biological, and chemical weapons. But today, the term means different things to different people and agencies. For that purpose, I'm going to take some time to define my terminology.

The military defines WMD as nuclear, biological, or chemical weapons that can cause a "high order of destruction." I would add to this definition that the intentional use of these weapons needs to cause mass casualties, defined as more than one thousand injured or dead, during a single incident. I disagree with the FBI's use of the Title 18 U.S. Code definition of WMD because of its deliberate lack of reference to the scale of the incident. To the Department of Justice (DoJ) lawyers, any amount of CBRN or explosives, no matter how small, constitutes a WMD. Even innate devices or hoaxes can have WMD aspects.

The presence of mass casualties is a key aspect of the WMD incident, but "mass casualties" is an undefined and nebulous phrase. In general, people use the term to describe a situation in which there is one more casualty than the number of available

hospital beds in the local area. Because we want to focus on the federal response, we need to quantify that number to understand what federal actions are adequate. The Department of Health and Human Services (DHHS) chose the number of 1,000 injured or dead people for the trigger for its Metropolitan Medical Response Forces.

In my mind, the term "WMD" is only useful as an arms control term. It is often used by international agencies and government officials to discuss a particular class of unconventional weapons. However, the United Nations wanted to keep the term open to other forms of technology that might equal nuclear weapons in the scope of their destructive force, so I'm not against consideration of high-yield explosives, directed energy lasers, or other weapons that could *realistically* cause mass casualties. Ricin and botolinum toxin, often used in small amounts for assassinations, are not WMD. Airplanes used to cause mass casualty events are not WMD. Pipebombs and grenades are not WMD.

There is a distinction between nuclear, biological, and chemical (NBC) weapons and CBRN hazards. This is probably more of an issue for specialists than for laypersons, but again, words are important. The term "NBC weapons" should cause one to take into consideration that a nation funded its top scientists and engineers with millions of dollars and built numerous facilities to develop and test special weapons that had definable characteristics and expected outcomes. The military developed operational specialists who could use these weapons on the battlefield for the purpose of causing measurable operational effects. This is where we got our nerve agents, our anthrax and smallpox weapons, and nuclear missiles and bombs.

These weapons were not developed casually, nor are they "immoral." They were developed because they could, in fact, kill large amounts of people or disrupt operations, causing an advantage for the side using them. That's what military forces do. The immorality comes in when the weapons are causally used and noncombatants suffer as a result, just as with any weapon system. Nonetheless, the world community has developed arms control treaties to regulate the use of these unconventional weapons, and the U.S. government has agreed to comply with these treaties.

One needs to be careful about how we use the term "chemical weapons." The military has always been careful to note the difference between munitions with chemical components, such as riot control agents, herbicides, and incendiaries like napalm, and toxic chemical munitions, like sarin nerve agent and mustard agent. Again, this is because of arms control agreements intended to guide nation-states during wartime. It is not against international law to use tear gas, herbicides, or flame munitions.

CBRN hazards, on the other hand, reflect a more general threat in which certain physical compounds could harm individuals through direct exposure, whether inadvertent or deliberate. The key here is that CBRN hazards do not have to be used in great quantity or to result in mass casualty events to be a concern to the public. It

benefits us, however, to narrow down the definition of what CBRN hazards are. There are literally tens of thousands of potential chemicals that could harm an individual through direct exposure. Even water has a material safety data sheet. The serious threats include toxic inhalation hazards like chlorine and phosgene, not chemicals like mercury or sulfuric acid. Anti-plant or anti-animal diseases are not so much a concern as are a limited number of pathogens and toxins that are particularly contagious or lethal to people. There is a short list of radioactive material, such as highly-enriched uranium, plutonium, and cobalt that cause people significant concern.

I don't like the term "CBRNE" because that's an antiterrorism term, not a WMD term. The military police and emergency responders within the DOD antiterrorism community started using "CBRNE" in the late 1990s because of numerous terrorist incidents such as the bombing at Khobar Towers, the Oklahoma City bombing, and the Aum Shinrikyo's Tokyo subway incident. But the antiterrorism community really doesn't worry about the "CBRN" as much as they do the "E." When it comes to assigning resources and time to the most credible threats, the more probable threat of explosives wins over CBRN hazards every time.

THE EVOLUTION OF HOMELAND SECURITY

There's a good publication within DHS that describes the history of civil defense and its morphing into what we now know as homeland security.[1] I don't intend to go through the long linage of that effort, except to note two things. First of all, it's not a static history. Different administrations viewed civil defense/homeland defense in different ways, and they moved around the responsibilities from office to office. This is a natural part of policy development and maturation, where people can assess how the programs are going and where they need to be. That's something that I've hoped would happen more within DHS since its inception in 2003, and I'm not sure that this assessment has really taken place.

Second, there has been a change in the focus as to what the federal government's responsibilities are with respect to addressing civil defense/homeland defense roles. Initially, the federal government saw its role strictly as providing a response to the intentional use of military weapons against U.S. cities and noncombatants. First it was the fear of German and Japanese bombers and missiles hitting U.S. cities on the coast. Then it was the threat of Soviet bombers and missiles. But the congressional response was not to spend great deals of money on this threat. Over time, the state and local officials were not as concerned about the possibility of external attack as they were the power of Mother Nature. Congress, influenced by those state and local officials, decided it was more important for the federal government to respond to states and locals

affected by natural disasters and accidents rather than external threats. That balance was rudely jarred after 9/11, and we have yet to re-establish a more balanced view.

Using Public Policy Methodologies

There are policy analysts, such as Charles O. Jones, who have developed methodologies to examine how the federal government addresses specific issues, whether these functions are appropriate, whether they are being adequately executed, and whether the people in charge are addressing the challenges that are presented. Homeland security and national defense are two important public policy issues, and yet it seems rare to see any honest, intellectual assessment of the particular projects the government is executing.

Using the Jones model outlined in "An Introduction to the Study of Public Policy,"[2] there are four specific players involved in any public policy issue. There are the decision-makers at the top ranks of executive agencies who are responsible for developing rational policy for areas under their mandate, such as the DHS under secretaries and assistant secretaries. There are the technical agencies that have to implement an aspect of these public policies, such as FEMA or the Coast Guard or Fire Services. The state and federal politicians are never quite comfortable with wide, sweeping actions, so they implement policies in small increments rather than addressing reforms in bold strokes. Finally, there are the reformists who demand immediate actions despite legal or financial challenges. The activists for homeland security exist on both the right and the left, especially on issues such as missile defense and border control.

This model can assist in identifying the challenges in how DHS is executing its responsibilities for addressing CBRN terrorism. For instance, on occasion, one might find the policy-makers (rationalists) directing agencies (technicians) on how to do their jobs in great detail rather than developing policy issues (which is hard). And because those policy issues need to be laid out before the challenges are addressed, the subordinate agencies end up making policy directives that are ineffective because the technicians don't have a view of the entire policy issue from a higher level. Congress ends up being influenced by activists and create grand initiatives, but only incrementally fund them. And the challenges pile up.

Seeking National Guidance

The recently released *National Security Strategy* defines its homeland security approach as addressing a number of significant challenges.[3] There are the generic "threats" to American interests, the emphasis over maintaining our borders and to stopping the transit of "hostile actors" who are either bringing illegal trade into our country or who are intent on causing harm. The ever-present focus on terrorism is plain, but less so the emphasis on natural disasters and whatever "other hazards" entails. The

National Security Strategy provides the basis for developing public policy for homeland security.

We can argue about what homeland security is and isn't, but it should be clear that it is a broad area covering multiple issues and overlapping concerns where the public might expect the federal government to play a role. In responding to natural disasters and catastrophic incidents, there was the Federal Response Plan to explain how the federal response will address state and local emergencies. This was followed by the National Response Plan, and now we have the National Response Framework and National Incident Management System. Deliberate CBRN hazards and WMD incidents are one subset of the overall national response framework, but we do spend an awful lot of energy discussing these very low-probability, high-consequence events.

There are a number of national strategy documents that address CBRN terrorism concerns. I don't intend to go into each one, but these documents have been the basis for explaining how our nation will execute its plans and develop capabilities for particular aspects of CBRN terrorism response. The federal government does not often distinguish between the approaches of how the military addresses adversarial use of NBC weapons on the battlefield from how terrorists use CBRN hazards against noncombatants. This is a serious flaw. We don't lack for top-level guidance, but determining what one can do given unclear guidance, budgetary limits, and limited areas of responsibility, can be challenging.

As an example, Presidential Policy Directive 2, a national strategy to "counter biological threats" just came out in January 2010. It purports to address all biological threats, whether natural or deliberate, under a sweeping architecture of efforts. At a recent meeting, one person stated that the only difference between naturally-occurring infectious diseases and biological warfare agents was "intent." Such a statement could quickly lead to miscommunications as to who's in charge of what and whose funds ought to be used to address the problem. This casual approach doesn't help to identify the roles and responsibilities for responding to bioterrorism within the federal government.

U.S. GOVERNMENT STRATEGIES TO ADDRESS CBRN TERRORISM

When we examine federal responses to CBRN terrorism, there is a tendency to confuse what the DOD does to protect its forces from NBC weapons and what DHS does to support state and local responses to CBRN incidents. This hasn't been helped by the confusing, high-level guidance in the *National Strategy to Combat WMD*, which was released in 2002.[4]

We've seen a deliberate change of philosophy in how the federal government addresses CBRN terrorism before and after 9/11. Before 9/11, it was a law enforcement exercise that DOD supported as requested. After 9/11, it became a military responsibility

to pre-empt the terrorists, with less attention as to the adequacy of civilian response. But due to a lack of clarity over roles, missions, and responsibilities, we see a continued debate over who's supposed to do what to whom in both areas. We talk about using a "whole of government" approach to CBRN terrorism, often focusing on the efforts of DOD, DHS, and DHHS (and other federal agencies). But this also commits the sin of blurring the difference between military operations and homeland security.

Overall, there are many responsibilities across the government when it comes to addressing domestic CBRN terrorism. No one should be surprised by the long list of involved federal agencies. The broad responsibilities are pretty well known – it's the inter-agency coordination and actual implementation that's the challenging part. There are a lot of people doing different things, and it's sometimes hard to put the pieces all together. This article will focus on the DHS responsibilities and programs, but certainly, the discussion could continue as to other federal agencies that are involved in CBRN terrorism response.

Counterproliferation versus Counterterrorism

There is a National Counterterrorism Center (NCTC) and a National Counterproliferation Center (NCPC). Both address WMD issues, but from differing perspectives. The counterproliferation community largely focuses on nation-states and the means of producing WMD materials and technology, and works long-term policy initiatives. The counterterrorism community focuses on tracking violent extremist groups who may be seeking WMD materials and technology and their activities operating outside of nation-states. Both communities are looking for similar hazards, but from different perspectives, using different agencies and different funding. They don't work as well together as they probably should, but that's because they have different agendas. There is a gap.

There are those people who believe we should force the two communities to work more closely together – that we ought to eliminate the gap between the agencies. I don't agree. While the two communities use similar intelligence sources and may be looking at similar regions in the world, they are fundamentally different. I don't believe in the popular assumption that terrorists are actively working with "rogue nations" to exploit WMD materials and technology. The evidence isn't there. Nation states invest heavy amounts of people and funds to develop specific unconventional weapons, and if they were to give or sell them to terrorists, one of two things could happen – either the weapons would be traced back to them, or the weapons might get used someplace where the nation state regrets.

Terrorists get their material and technology where they can, from the local economy. They don't have the time, funds, or interests to get exotic. That's what we see, over and over again. The NCTC noted that, in 2008, there were approximately 11,800 terrorist

attacks resulting in more than 54,000 deaths, injuries, and kidnappings. Nearly all were caused by armed assaults, bombings, suicide attacks, kidnappings, and other conventional forms of assault.[5]

Early Efforts to Address CBRN Terrorism

In 2003, DHS began developing its CBRN terrorism response efforts by basically copying the DOD's CBRN defense concept. This included recommending the use of plastic sheets and duct tape for homes and businesses to provide "shelter in place" collective protection and the use of point detectors to identify lethal levels of chemical, biological, and radiological hazards. There were two major problems with this approach. First, the threat of CBRN hazard exposure to people at home (or even businesses) was about near zero, and second, the low probability of a CBRN hazard being used on any one day during the year at any one particular site within the United States was practically zero. It was not a sustainable strategy if one demanded eternal vigilance at all locations with the goal of eliminating all threats. And of course, the U.S. government wasn't protecting all potential terrorist targets.

The Homeland Security Planning Scenarios are ridiculously unrealistic in portraying the expected threats to the homeland. Of the fifteen scenarios, eleven are CBRN-focused, and not just typical CBRN hazards but significant quantities of military warfare agents such as anthrax, smallpox, sarin nerve agent, and mustard agent. They are "worst-case" scenarios, which are good for leadership exercises where you want to encourage interagency communications or to identify whether policies or resources are a limiting factor, but they are lousy for making resourcing decisions. Worst-case scenarios rely on movie-theater plots that maximize the threat only because that's the best way to get a maximum number of senior leaders within multiple agencies at the federal level involved to play in a short, annual national exercise. The 10-kiloton nuclear scenario is particularly ridiculous, but let's wait on that discussion.

As a result of these plans, we've inflated the stature of foreign terrorists into twelve-foot *ubermensch*. The term "non-state actor," a phrase that is routinely used around Washington, DC, applies to a larger cast of villains, including private militias, insurgents, criminals and drug smugglers, anyone who is basically working outside the government and conducting illegal activities. The concern focuses on those foreign (transnational) violent extremist organizations who generally receive some kind of basic military training so that they can use automatic rifles and grenades.

The basic approach used by terrorists and insurgents is to seek out and use low-risk, easily-acquired weapon systems. Any weapon that can be improvised using available and accessible materials is good; any weapon that can be bought on the open market and easily used is good. CBRN materials don't fit that niche. The reason why terrorists are interested in CBRN hazards is because so many senior leaders keep vocalizing how

afraid they are of this particular threat. Before 9/11, the interest was not as strong (and the senior leader rhetoric about "WMD threats" wasn't, either).

While terrorists are interested in CBRN hazards, they can't get the dangerous precursor materials, they don't have any training in handling or dispersing these hazards, and they don't understand the particular effects on their targets. So we see some scattered use of industrial chemicals, some production of ricin toxin from castor beans, a few grams of radioactive material stolen from a facility – not exactly mass casualty threats. As terrorists attempt to develop more sophisticated weapons in an effort to create mass casualties, their machinations become more public and it actually becomes easier to catch them.

Chemical Terrorism

Chemical terrorism has been downplayed recently, ironically because it doesn't cause enough casualties for high-consequence scenarios. Chemical terrorism remains the most likely form of CBRN terrorism, if one looks at the relative ease of obtaining industrial chemicals from the economy and low threshold of training and equipment required. Still, people focus on the nerve agents as the "likely" threat, not because they're available, but because they're the most lethal. Actual cases show terrorists seeking available industrial chemicals rather than making nerve agents, with one exception. Aum Shinrikyo had millions of dollars, facilities, trained chemists, and years of practice to make its sarin nerve agent. Most terrorist groups lack those resources.

I'm not a proponent of the DHS Chemical Facility Antiterrorism Standards, where the department looks to identify all chemical storage facilities and to make their owners assess the security of their chemicals. All this does is cause incentives to industry to move the chemicals somewhere else. Instead of focusing on the major producers, DHS diminishes its efforts by trying to cover tens of thousands of small facilities and anyone using a chemistry kit. It becomes a paperwork drill where no one addresses the really tough problems.

The toxic inhalation hazards, such as chlorine and phosgene, represent the most challenging terrorist threat, but that doesn't stop DHS from listing sixteen pages of "chemicals of interest."[6] Even then, getting cylinders of chlorine gas in the United States is not as easy as it used to be. Many water treatment plants have converted to alternatives to chlorine gas. Most toxic chemicals have colors or smells that cause people to take preventive measures prior to succumbing to their effects. But in the end, we know how to address hazardous material incidents, right? So why is this so difficult to address?

The railcar discussions are particularly amusing, in that there is so much concern about a hazmat derailment within a major city. So the answer is to divert hazardous materials around a city, right? There are two things wrong with that – the secondary

rails are less well maintained, and so represent a greater safety risk. And legal issues with regulation of interstate rail transport get in the way.

We're driven in the chemical industry to use this mentality of limiting exposure to the general public to "as low as reasonably achievable" or ALARA. This approach results in promoting "worst-case" EPA plume analyses that use minimum levels of incapacitating exposure as guidance for area effects, overestimating the actual impact of such incidents. We need to be serious about the probability of "high-consequence" events and what can be done to address them. DHS should focus on providing installation security assessments and identify ways to assist industry rather than being watchdogs.

Biological Terrorism

Bioterrorism is the flavor of the year, thanks to a recently-released government report titled "World At Risk" by former senators Bob Graham and Jim Talent.[7] Hollywood and fiction novels have done their best to ensure we all believe that a contagious virus without any cure is being secretly developed in a government lab and will wipe out civilization as we know it. We have a very long history on the treatment of natural diseases, and with the rise of biological warfare the difference between addressing deliberate and natural disease outbreaks gets very blurry. Some people say that, merely because there is greater access to information and technology related to natural biological diseases, there is a corresponding increasing chance of a bioterrorist incident. This isn't necessarily so.

One requires a large amount of biological warfare (BW) agent to successfully cause mass casualties, and these agents can't be made in a bathtub. You can't go to Wal-Mart stores to obtain dangerous biological assays or to Home Depot for equipment to grow biological material. Bruce Ivins was successful because he had a full laboratory suite and starter material available to him, plus decades of experience in handling anthrax.[8] But while the dangerous agents are hard to make, the diversity of the biological threat complicates the development of particular solutions. That isn't to say that we haven't made a good faith effort.

There are at least a dozen top BW threats, but under Project Bioshield, we have vaccines for only two of them. Maybe in another ten years, we'll have a few more vaccines, but certainly not twelve. For the 270 cities in the United States with a population of more than 100,000, only thirty-odd cities have Project Biowatch detectors. It's a very expensive project to sustain against a wide variety of potential threats. But this isn't just a medical issue, although the medics have assumed the spokesperson role.

Let's look at the "whole of government" approach to public health. DHS coordinates the Biowatch effort and the National Biosurveillance Integration Center effort. It's not a lot of money. DHHS has more than $80 billion a year invested into public health (not

including nondiscretionary spending). This includes the work at CDC. The DOD has its Defense Health Program funded at $40 billion a year. This includes all the military hospitals and TRICARE program, in addition to medical surveillance and treatment on the battlefield. The Department of Veterans Affairs department handles the health care of former military and is slightly bigger than the active duty health affairs efforts at $41 billion a year, but that's not a big surprise.

Then there's the DoD combating WMD community. While two-thirds of its $15 billion annual budget is spent on missile defense and special operations efforts, there are some funds spent on medical countermeasures and responses to biological warfare agent use. And finally, the international community plays a role through numerous non-governmental agencies as well as international health organizations. There are lots of players addressing different aspects of this huge area we call "public health."

By the estimates of the Center for Biosecurity at the University of Pittsburgh, there is roughly $5-6 billion a year spent on "biological defense," depending on how one defines that project. The FY2011 budget calls for about $6.5 billion. The "whole of government" challenge is managing all these efforts without disrupting anyone's rice bowl and still keeping cognizant of the bioterrorism threat, in addition to other public health concerns of infectious diseases, drug safety, and other health concerns.

People like to quote the total federal investment of $58 billion in biodefense projects over the past ten years to discuss the efforts made in this one specific area of CBRN terrorism. It's a misleading number, since many of the projects address multiple or tangential goals, not just domestic bioterrorism. However, the question should not be, is this too much money, but rather, how well is the money spent toward achievable goals? And we don't really know, because no one has established the end state against which we ought to be planning.

In January 2009, I presented a paper on behalf of the Project for National Security Reform, examining the progress we've made since the "Biodefense Strategy for the 21st Century" was released in April 2004.[9] Overall, the framework of the strategy is good. It identifies all the aspects required to respond to domestic bioterrorism and assigns responsibilities to the right federal agencies. In fact, it is unique in that there is no equivalent chemical or rad/nuclear framework (and that ought to be a concern). The problem is that no one has assessed how well the agencies were performing, if they were going in the right direction or required rebalancing, or if the end state was achievable given the available resources and personnel.

My research revealed that there are significant limitations on the progress made over the past five years. In particular, it was not apparent that there was any direct day-to-day federal oversight of CBRN terrorism response measures. Both the National Security Council and Homeland Security Council were consumed with daily emergencies and

meetings, and there was little to no oversight of what executive agencies were doing and if more funds or guidance were needed.

The generic terrorist threat is often referenced without any specific understanding of specific group motivations or activities. Al Qaeda has stated intentions to use CBRN hazards, but this has not led to the actual development of any specific capabilities. While the Proliferation Security Initiative has equipment for rad/nuke interdiction, there are no technologies to support biological interdiction. We're blindly attacking the tools instead of the terrorists.

The lack of any effort to harden critical infrastructure, notably with collective protection filters and CB agent detectors, surprised me. While integrating improved collective protection systems into existing buildings can be done, it's not an area that you see implemented. It seems like a relatively easy solution, but it seems that people would rather spend the money on military intervention or medical response rather than general protection.

I already mentioned the lack of vaccines and medical countermeasures for biological agents. The challenge was, and continues to be, that Big Pharma has no incentive to get involved in researching these specialized medical countermeasures. It's too expensive, it's not profitable, and it could lead to lawsuits if the drugs are incorrectly used. The government's offer of indemnity isn't winning any friends.

Bioforensics remains a tough challenge, considering the number of different strains of biological organisms. I don't know how many anthrax strains there are, for instance, but information on specific biological organism strains was helpful in narrowing down the Amerithrax suspect to a domestic source. The Biowatch effort should not be acceptable to any serious analyst. False positives aside, we'll never get adequate coverage for the entire United States, or even a majority of the nation's major cities, because it is too expensive to run 24/7 and to test all the samples in a lab. Even with the proposed Gen 3 biowatch detector, which doesn't exist right now, DHS plans to roughly double its monitors to cover sixty cities. Using point detectors for national special security events makes sense. Biowatch doesn't.

DOD has an impressive amount of personnel standing by for responding to a CBRN incident. At last count, it was approaching fourteen to fifteen thousand people ready to respond to assist state and local emergency responders. Although they might be useful for addressing the consequences of a chemical or radiological terrorist incident, they're not much help for biological terrorist incidents – especially a "no-notice" attack – other than offering a presumptive identification that the "white powder" threats isn't anthrax.

Radiological and Nuclear Terrorism

Radiological terrorism gets people excited because, even though the nature of radiological hazards hasn't changed in more than six decades, there's something about

radiation that spooks us. The term "dirty bombs" has a sinister sound. But of all the terrorist CBRN hazards, radiological devices (RDD) are certainly not WMD. We have never had an RDD incident to date, and yet so many people like to worry about the loose or available radiological isotopes that could be grabbed up by terrorists.

I'm very critical about the approach to addressing radiological terrorism. It's no surprise that the easiest way to reduce our risk in this area is to secure all the radiological material that industry uses and to place it in one location that could be guarded. Instead, because of NIMBY politics, the decision was made to close down a $9 billion nuclear material repository and to maintain the status quo of storing nuclear material in "temporary" storage near more than 120 nuclear facilities across the nation.

The idea of placing radiological monitors at every airport, sea port, and border crossing is, again, a concept that DHS adopted from the DOD. There's no question that the radiological dosimeters and monitors work when presented with an isotope. It's just that using these detectors at the thousands of possible entry points, considering the huge and constant flow of personnel and cargo, is a really stressful and expensive operation. We do not have reliable, cheap detectors that can be integrated into the process of screening people and cargo without negatively impacting our economy.

Getting past the actual implementation of such a vast network of detectors, let's look at the real 800-pound gorilla in the room. Some people fear that al Qaeda is going to somehow obtain a nuke from Pakistan, disable the safety mechanisms, and transport it to a U.S. city. Some fear that al Qaeda will build a crude nuclear bomb, using technical expertise and material through the global economy. The scenario of a 10-kiloton nuclear blast is what causes people to "lose sleep," allegedly. And yet, if you examine the facts, it's not likely at all that this is a credible scenario.

I strongly recommend Brian Jenkins' book *Will Terrorists Go Nuclear?*[10] and Michael Levi's book *On Nuclear Terrorism*[11] for anyone who's interested in an objective discussion on this topic. In short, nations with nuclear technology or materials need to consider whether the bomb will be traced back to them, and where the bomb might be used. It might not be in the United States, it might be in a neighboring country. The number of people who would need to be engaged to get/build a bomb and move it to the United States, let alone engineer a successful detonation, would make this a complex operation that would be visible to law enforcement and the intelligence community. We have no compelling evidence that any nation has provided a terrorist group with chemical or biological weapons – why on earth would they provide a terrorist group with nuclear weapons? It doesn't make sense.

The "high-altitude EMP blast" scenario is particularly outlandish, suggesting that a terrorist organization would be able to move a ballistic missile to the coast of the United States and set off a megaton nuke 200 miles over the country just to collapse the electronic infrastructure and turn America into a pre-industrial society. There are better

odds that an asteroid the size of Texas might collide with a major city within the United States. Resiliency is the answer – it would be simple to harden critical infrastructure points and maintain spares to stop this scenario from occurring. The argument here actually masks a separate debate over the continued development of a comprehensive (and very expensive) national missile defense effort.

Bottom line, we're already petrified that al Qaeda is going to nuke America, even lacking any evidence that it has one or could get a nuclear weapon. So why does al Qaeda need a nuclear bomb? It already has accomplished its purpose of terrifying the country. And yet, we see the unfolding of this massive "Global Nuclear Detection Architecture" that's designed to ensure our politicians can sleep well at night. We could cite the statistics – the hundreds of ports, the thousands of miles of border, the "second line of defense" – and ask is this the most effective way to address the challenge of a terrorist rad/nuke incident?

The scope of the global architecture keeps growing. In addition to the major air and sea ports and border crossings, the DHS Domestic Nuclear Detection Office has proposed going after all the smaller air and sea ports that cater to private vessels. And then there's the idea of populating the major cities and interstate roads between cities with radiological monitors. Is this a sustainable plan? Is it really effective, considering the limits of radiological detection technology? I would argue, no. The false alarms and cost of maintaining such a nation-wide system are prohibitive, considering the very low probability of occurrence and other options available to the national security community.

The GAO is actually very reserved in its criticism in this area.[12] It focuses on the lack of a strategic plan with measurable actions rather than on the feasibility of the concept itself, because the GAO strongly believes in strategic planning in any area of government. But let's be clear, this is a losing proposition. It is security theater, designed to make us feel good about doing something against a threat that people feel, in their gut, is an unacceptable challenge, despite the lack of any credible possibility of it occurring.

This is the least probable threat, granted one with an extremely high-consequence event if it is successful. Increasing the effort to focus on the origins of the rad/nuke material, in addition to good old-fashioned law enforcement and intelligence work, would be a far more effective solution than developing a network of detectors that focus on a particular hazard that could be easily shielded. To truly be effective, we need to develop a strategy that is guided by resources and that can be sustained throughout the year.

Let's assume that, worst case, a nuclear bomb is smuggled into a major U.S. city. Let's not pick New York City, that's been debated enough. But say a nuke goes off in Atlanta or Chicago or Seattle. Let's assume that the terrorists had a functional bomb that yielded

a 10-kiloton blast, not a crude device that resulted in a 1-2 kiloton fissile. Certainly thousands of Americans would die and a city would be irrevocably damaged. But would the United States stop, falter, collapse as a nation? No. A single nuclear terrorist event is not an existential threat to such a massive country. It can be managed, and given all the effort already in place to prevent such an incident, it's not what ought to be keeping us up at night.[13]

DOD Efforts to Respond to CBRN Terrorism

The DOD became involved in the discussion of federal response to CBRN terrorism in the late 1990s because Secretary of Defense William Cohen wanted his technical specialists to be involved in any federal response to a CBRN terrorist incident. Since everyone believed the threat was NBC weapons, DOD was of course the subject-matter expert. We already had a limited capability with the Army's Technical Escort Unit and the Marine Corp's Chemical-Biological Incident Response Force (CBIRF), the latter developed after the Aum Shinrikyo incident in 1995. So Cohen started with the concept of WMD Civil Support Teams to advise and assist state and local emergency responders. Congress really liked that idea, and now we have fifty-seven teams deployed across the U.S. states and territories.

That wasn't good enough, so DOD designed a Chemical-Biological Rapid Response Team, using various Army, Air Force, and Navy technical specialists, and later designed a "Guardian Brigade" in 2005. The National Guard decided to help with seventeen CBRNE Emergency Response Force Packages (CERF-P), which placed a CBIRF-type organization in every FEMA region (with some extra units for redundancy). The Bush administration pushed for a more robust capability using active duty forces, identifying the need for three large CBRNE Consequence Management Response Forces (CCMRF) to address multiple, simultaneous mass casualty events, but the strains of combat operations in the Middle East were significant, so that idea collapsed. As an alternative, the National Guard may provide additional response capability by creating ten Homeland Response Forces (HRF), one in each FEMA region.

The development of DOD response forces assumes that the states and local emergency responders will become overwhelmed by a high-consequence WMD event within forty-eight to seventy-two hours, and that gradual waves of federal troops are required to reinforce the response to that incident until it is concluded. So DOD comes in if a state governor requests federal support, if DOD is seen as necessary to that support, and if the DOD secretary approves it. However, if a high-consequence event never occurs, is this really a necessary capability? It is more likely that state and local emergency responders will be able to address the majority of CBRN terrorist incidents (short of that 10-kiloton event), given adequate training and preparation. It's an awful lot of manpower standing around, waiting for the firehouse alarm that may never ring.

As an example of DOD's own inherent challenges in addressing "homeland defense" with military chemical-biological (CB) detectors, let me offer this case study. Shortly after 9/11, DOD leadership was concerned that terrorists were going to attack U.S. military installations with CB warfare agents. There was no clear intelligence to support this, but it was a gut feeling based on the belief that terrorists liked mass casualties and domestic military installations were the top targets. It wasn't exactly a solid piece of analytical work.[14]

In 2002, DOD had more than 650 military bases and installations across the globe, but because of financial implications, the Office of the Secretary of Defense decided that it would provide funds to develop CB defensive measures for 200 of these bases, the majority of which were within the continental United States, at a cost of $5 million each. In addition to the one billion dollars for the project, there was another half-billion dollars allocated for training installation responders. This would provide a number of chem-bio detectors (no radiation detectors) tied into the emergency ops center, some protective gear and medical countermeasures, hazard plume software and warning sirens, and training and concept development. This was supposed to provide a basic level of protection for the installation.

The effort began in 2004, and within the first two years only one base received enough gear that might constitute an adequate antiterrorism capability. Most of the bases only received limited gear for the emergency responders, rather than receiving a full antiterrorism capability. In 2006, half of the billion dollars was funneled off for a new program aimed at developing "silver bullet" vaccine shots for "broad spectrum" biological threats. The main failure lay in the inability of the antiterrorism and CB defense communities to implement an integrated, all-hazard "CBRNE" operational concept for military installations and bases. The antiterrorism community didn't view CBRN hazards as a significant threat, and didn't appreciate having specialized equipment forced onto them.

CONCLUSIONS

Homeland security is not a new issue. It's encouraging that we have advanced education now and interagency discussions on how we all can address the threat of domestic CBRN incidents, from the state and local level through the federal level. But we need serious reviews of the policies that are in place and to use that "risk-based" management approach to ensure that we are spending our funds wisely. We continue to view WMD or CBRN hazards as the threat – that's a myopic focus. We need to look at the process by which terrorists develop their tools and understand that it is by defeating the terrorists that we can stop the CBRN threat. When you take a realistic look at the threat and what

terrorists can actually do – outside of a television show like *24* – it's not a difficult thing. We can do this more smartly.

There is a fundamentally better approach to developing a federal response to domestic CBRN incidents, but we need to start by stopping the loose use of the term "WMD." It only confuses the discussion and presents an unachievable goal that obstructs serious discussion. We need to clearly separate the concepts of how militaries defend against NBC weapons and how emergency responders address terrorist CBRN hazards. These are very different concepts. We should not act as if a terrorist group has the capability to do as much damage as a nation with an active WMD program. Although the military threat is similar to the terrorist threat in terms of physical composition, the scope of the incident and required concepts and equipment are entirely unique. We have to develop a sustainable, effective solution that can be employed throughout the year to protect untrained noncombatants.

We need to address the mass casualty definition to allow more informed discussions on possible approaches to realistic scenarios. My suggestion is to develop a three-part framework based on the expected number of casualties:

- Type A: 100 – 1,000 casualties (Oklahoma City bombing)
- Type B: 1,000 – 5,000 casualties (9/11 incident)
- Type C: 5,000 – 50,000 casualties (nuclear weapon incident)

By better defining the consequences of a terrorist incident, we can develop focused initiatives that can be measured against easily understood scenarios. Similarly, the Homeland Security Planning Scenarios have to be changed to reflect realistic and probable threats, not "worse-case" scenarios. By using the scenarios as the basis for national-level exercises, we risk the danger of overestimating the actual need for unique and specialized resources that may never be employed within our lifetimes. We should not lose sight of the fact that the majority of incidents requiring federal response to state and local emergency responders will be for natural disasters and industrial accidents rather than WMD.

In developing policies that try to protect everything, we protect nothing. We need to develop strategies that are guided by resources, recognizing that there are multiple homeland security threats that all have to be addressed. It actually is a question of "if, not when" we ever see a CBRN terrorist incident that results in mass casualties. We need a sustainable, effective approach, which requires us to stop overhyping the threat. It's not September 12, 2001, anymore. We need to realistically assess the challenge and all possible threats – natural and man-made – and calmly, rationally, develop a plan that doesn't bankrupt the annual operating budget. None of us have enough money to

provide perfect protection for everyone throughout the year, and there are better things to spend money on – like retirement plans.

Al Mauroni is a senior policy analyst with more than twenty-four years experience in Department of Defense chemical, biological, nuclear, and radiological (CBRN) defense policy and program development. He served as a U.S. Army chemical officer for seven years before leaving active duty in 1992. He holds a master's degree in administration from Central Michigan University and a bachelor's degree in chemistry from Carnegie-Mellon University. He is the author of six books (the latest of which is titled Where Are the WMDs?) *and more than two dozen articles. Mr. Mauroni can be contacted at mauronia@yahoo.com.*

---

[1] U.S. Department of Homeland Security (DHS), "Civil Defense and Homeland Security: A Short History of National Preparedness Efforts," (September 2006), http://training.fema.gov/EMIWeb/edu/docs/DHS%20Civil%20Defense-HS%20-%20Short%20History.pdf.
[2] Charles O. Jones, "An Introduction to the Study of Public Policy," (Harcourt, 1984).
[3] The White House, *National Security Strategy* (May 2010) http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.
[4] The White House, *National Strategy to Combat Weapons of Mass Destruction* (November 2002), http://www.state.gov/documents/organization/16092.pdf.
[5] National Counterterrorism Center (NCTC), *2009 Report on Terrorism* (Office of the Director of National Intelligence, April 20, 2010), http://www.nctc.gov/witsbanner/docs/2009_report_on_terrorism.pdf.
[6] See the DHS webpage on CFATS at http://www.dhs.gov/files/laws/gc_1166796969417.shtm.
[7] Bob Graham, et al, *World At Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism* (Vintage Books, 2008), http://www.preventwmd.gov/report/.
[8] Federal Bureau of Investigations (FBI), "Amerithrax Investigation," http://www.fbi.gov/anthrax/amerithraxlinks.htm.
[9] See Project on National Security Reform, "Progress of 'Biodefense for the 21st Century' – A Five-Year Evaluation," Project on National Security Reform (January 2009), http://otherwmds.blogspot.com/2009/03/biodefense-monograph.html.
[10] See http://willterroristsgonuclear.com/.
[11] See http://www.cfr.org/publication/13915/on_nuclear_terrorism.html.
[12] U.S. Government Accountability Office, "Nuclear Detection: Domestic Nuclear Detection Office Should Improve Planning to Better Address Gaps and Vulnerabilities," GAO-09-257 (January 2009), www.gao.gov/new.items/d09257.pdf.
[13] See also Robert C. Harney, "Inaccurate Prediction of Nuclear Weapons Effects and Possible Adverse Influences on Nuclear Terrorism Preparedness," *Homeland Security Affairs* V. No. 3 (September 2009), http://www.hsaj.org/?fullarticle=5.3.3.
[14] Al Mauroni, "CBRN Defense of U.S. Military Installations and Facilities," *Scribd.* (August 2005), http://www.scribd.com/share/upload/10460697/1d19xw96qz30iaqq48pw.

Homeland Insecurity is the debut album by Endwell. It was released on October 31, 2006 on Victory Records. "The End". "A Taste of Everest". "Single and Loving It". "Four Letter Words". "Homeland Insecurity". "Goodbyes Are Always Coldest in December". "Boy Meets World War III". "I'm Frozen and You're Dead". "Drowning (One Last Breath)". "Whine and Dine". "Fever White". "Zombies Never Think Twice". "Single And Loving It" was made into a music video. SUGGESTED CITATION: Mauroni, Al. â€œHomeland Insecurity: Thinking About CBRN Terrorism.â€ Homeland Security Affairs 6, Article 3 (September 2010). https://www.hsaj.org/articles/78.Â DHS has not assessed its efforts to address CBRN terrorism or identified where DHS could improve, and as a result we see merely the continuation of previous initiatives. The essay concludes with some recommendations on how DHS could improve this area with better policy practices. Words Are Important. HOMELAND SECURITY AND THE SEARCH FOR TERRORISTS A recently issued report from the U.S. General Accounting Office [8] notes that at least 52 agencies are using or are using or planning to use data mining, "factual data analysis," or "predictive analytics," in some 199 different efforts. Of these, at least 29 projects involve ana-lyzing intelligence and detecting terrorist activities, or detecting criminal activities or patterns.Â The first part of this paper will provide an historical outline of thinking about the distinction between security intelligence and evidence. The second part of this paper will outline some of the competing goals that should [Show full abstract] inform the relationship between security intelligence and evidence.