NEW HORIZONS IN BIOTERRORISM

WORKSHOP REPORT

Arlington, VA
11-12 August 2008

September 17, 2008

PREPARED FOR:
Office of the Secretary of Defense: Defense Research and Engineering (DDRE) & Rapid Reaction Technology Office (RRTO)

US Strategic Command (STRATCOM): Global Innovation and Strategy Center (GISC)

United States Special Operations Command (SOCOM)

Department of Homeland Security, Science and Technology Directorate

PREPARED BY:
National Security Innovations, Inc.
8 Faneuil Hall Marketplace, 3rd floor
Boston, MA 02109
scanna@natlsec.com

&

National Consortium for the Study of Terrorism and Responses to Terrorism (START)
University of Maryland
gackerman@start.umd.edu

Executive Summary

The objective of the *New Horizons in Bioterrorism* workshop, held on 11-12 August 2008 in Arlington, Virginia, was to explore existing and future developments in bioterrorism through the elicitation and generation of adversary courses of action (ACOAs) and associated indicators. Ten bioterrorism subject matter experts (SMEs) were invited to explore bioterrorism indicators, plots, and capabilities through 2015. The workshop addressed both existing and future developments in biological terrorism through the elicitation and generation of bioterrorism ACOAs, as well as indicators associated with those activities. Through the exploration of both existing and potential paradigms, the workshop participants sought to provide the sponsors with a better understanding of the processes and procedures preceding a biological terrorism attack.

The unclassified workshop was the first step in a three-phase program supported by the U.S. Special Operations Command for the Joint Intelligence Preparation of the Operational Environment (JIPOE) and the Strategic Multilayer Assessment (SMA) programs. The goal of the WMD-T (Weapons of Mass Destruction – Terrorism) JIPOE is to develop a national-level combating WMD-Terrorism forecasting or inferential strategic assessment capability covering full threat spectrum from intent to act, to preparation, and all the way downstream to deployment by non-state actors (i.e. far left of "boom" to just left of "boom"). This requires a decidedly new adaptive and dynamic forecasting and alerting approach. SMA will provide concepts and tactics, techniques, and procedures (TT&Ps) for establishment of a national, federated WMD-T JIPOE enterprise to provide shared understanding and action orientation to the WMD-T threat domain.

The second phase of the program will employ a Bayes Net Risk Analysis model and an Automated Behavioral Analysis model to generate priority threat scenarios. The third phase will integrate the ACOAs from Phase I, risk estimates from Phase II, and a historical analysis in a classified session to evaluate and prioritize ACOAs. Intelligence or knowledge gaps will be identified and a top ten list of threats will be generated.

Results

The workshop participants generated 38 ACOAs, 25 of which fell in the "likely" (i.e., >1% probability) category and 13 of which fell in the "extreme" or "black swan"[1] category (<1% but incomputable probability). Participants ranked the likelihood of the 25 "likely" ACOAs occurring by 2015. The results are listed below (using brief descriptive labels), from most to least likely.

Table 0-1. ACOAs listed in order of subjective likelihood by 2015.

ACOA Description
Salmonella poisoning of food, such as tomatoes and multiple foodstuffs
Al-Qa 'ida anthrax attack on sporting venue
Anthrax attacks on transportation hubs
Jihadist cell releasing ricin using a nebulizer in subway system
Mixture of placebo/true agent multiple dissemination strategy using anthrax overwhelming first responders
Right-wing terrorist attack using anthrax from natural source in US; distribution by agricultural sprayer in slurry form
Al-Qa 'ida penetration of university laboratory to produce anthrax
FMD Al-Qa 'ida attack on US soil from Indian cow drool source
Ricin turkey attack
Disgruntled Individual, botulism poisoning of bottles in beverage plant
Disgruntled individual spraying anthrax in grocery store
Long-term Al-Qa 'ida infiltration of food and water supplies to induce botulism poisoning
Weaponized anthrax attack on foreign city when American diplomats attend -- theaters or public places -- aimed at teaching the populace to spurn diplomacy with the US
LTTE anthrax attack through mail system
Christian-Identity group FMD attack against US agriculture
Al-Qa 'ida creation of pandemic avian flu outbreak using suicide operatives
Long-term synthesis of 1918 flu virus
Disgruntled scientist Camel pox modification and dissemination.
Smallpox release and targeting of transportation nodes
Isolation and dissemination of Flesh-eating bacteria
Pneumonic plague using Cats as a vector
Hamas: typhoid US water supply contamination

[1] A black swan is a rare and unpredictable event as defined by Nassim Nicholas Taleb in his book The Black Swan.

Participants were also asked to separately rank their ten most likely perpetrators, modes of attack (agent + delivery method) and targets. These rankings are presented below, from most to least likely.

Perpetrator Type	Cumulative Score
Religious	220
Personal / Idiosyncratic	134
Single Issue	21
Right-wing	12
State Sponsored	12
Criminal	11
Ethnonationalist	9
Left-wing	8
Unspecified	***9***

Bioagent	Cumulative Score
B. anthracis	142
S. Typhi	58
FMD	47
Botulinum toxin	39
Y. pestis	39
Ricin	33
Viral Hemorrhagic Fever	22
Influenza	21
Variola major	17
E. Coli	10
African Swine Fever	7
Shigella	5
HIV	4
Hepatitus B	3
Other	3
B. cereus	1
Unspecified	***59***

Target Category	Cumulative Score
Transportation (vehicles or hubs)	77
Government (General)	71
Unspecified public space	71
Food supply	68
Sports / Entertainment Venue	67
Agriculture	39
Business	22
Mail system	18
Educational Institution	15
Consumer products	11
Water supply	9
Utilities	8
Government (Diplomatic)	6
Tourists	5

Delivery Method	Cumulative Score
Aerosol	155
Contamination - Food	132
Contagion	56
Contamination - Other	56
Direct Contact	38
Explosion	6
Other	4
Unspecified	***63***

Most Likely Perpetrator

As is widely recognized, the foreign-based threat is centered on jihadists, including al-Qa`ida and its offshoots - which is featured prominently in both the ACOAs and the rankings. However, the largest bioterrorism threat facing the United States in the next ten years does not originate solely from extremist groups abroad. A similar threat stems from the knowledgeable individual, such as the disgruntled scientist working in a lab with select agents or clever individuals with access to the internet. Their ability to also inflict a bioterrorism attack against U.S. targets is reflected in both the rankings and ACOAs. Many individuals might seek bioweapons because of the inordinately asymmetric nature of these weapons – they can have large-scale effects but compared to several other high-impact weapons, the scale of operation required to successfully perpetrate a bioterror attack is relatively low.

One output of the participants' discussion was the opinion that one of the chief dangers is that of a scientist with access to a laboratory who may either become disgruntled or may be co-opted by a group to use his/her knowledge and access to agents and laboratory facilities to facilitate a biological attack. Scientists working in laboratories often experience very little oversight (especially in non-U.S. contexts) and can use the agents and facilities available to them to surreptitiously grow and/or weaponize harmful agents. Another concern is the burgeoning number of laboratory facilities in the United States that handle the most dangerous pathogens – especially those dealing with select agents. Laboratory scientists in the United States have not historically been rigorously vetted or monitored, making laboratories vulnerable to infiltration by a group with a long time horizon. The participants concluded that they are less worried about terrorists becoming biologists and more worried about biologists becoming terrorists.

At the same time, bioterrorism by recognized terrorist groups (especially foreign-based organizations), is still very much a possibility. Intelligent individuals with access to instructions derived from the internet could make large quantities of crude agents over time in an improvised laboratory, located in such nondescript facilities as a residential basement. These individuals could purchase, without much difficulty, second-hand dual-use fermenters from online vendors. The key element here is time - lethal bioagents can be produced in relatively crude facilities with few resources and a lot of time. Law enforcement has already responded to many such cases, most of which have involved ricin or anthrax.

Most Likely Attack Mode

It is difficult to isolate the greatest threat facing the United States according to attack mode. The most popular types of agent presented in the ACOAs were bacteria and viruses. The most common agents were anthrax, ricin, and strains of the influenza virus - 1918 Spanish and Avian. In the ACOAs, the agents were generally obtained from thefts from laboratories pointing towards the need for vigorous security efforts. However, the fact that many of the perpetrators in the ACOAs obtained the bioagents from the environment is perhaps more troubling, since it vastly complicates the ability to observe acquisition attempts. In the uncontextualized participant rankings (shown above), the three highest-ranked bioagents were anthrax, salmonella and foot-and-mouth disease.

The most likely attack delivery mode varies widely by organization. A home-grown, small organization will face different options from a large, well resourced, organization with a long time horizon like al-Qa`ida. A small organization is more likely to use easily accessible agents against easily accessible targets such as sprinkling salmonella on salad bars, which has already been successfully attempted.[2] Certain

[2] Jonathon Tucker, ed. Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons, Chapter 8, the Rajneeshees by W. Seth Carus. MIT Press: Cambridge, MA, 2001.

organizations have technical fetishes that make them more likely to pursue advanced technologies. An apocalyptic group may be one of the few organizations willing to use a viral contagion against a target since the spread of many such contagions, for instance a potentially aerosolized HIV, can be difficult to control and such an attack would thus have the potential to infect and kill a significant proportion of the human race. The particular ideological profile or organizational make-up of a group is an important indicator in its potential threat level. This being said, two of the attack modes that appeared prominently during the workshop and in participant rankings were the contamination of food supplies with relatively less-lethal bioagents and the aerosol release of *B. anthracis* spores to infect large numbers of people.

Most Likely Targets

While the exact targets varied considerably by type and location, the target types most heavily represented in the collection of ACOAs supplied were private citizens / public places, the food and water supply and transportation hubs and vehicles. The transportation infrastructure and general gathering places of private citizens are attractive targets for most forms of terrorism, but biological agents are especially apt for contaminating food supplies.

Black Swans

The pace of scientific advancement over the last ten years has been greater than almost anyone anticipated. Therefore, the United States should anticipate novel advances in biotechnology that open new and terrible possibilities in bioterrorism. Scientists have reached the point in their understanding the human genome where they can potentially create targeted bioweapons against a particular population or engineer virulence and infectiousness into novel organisms. Advances with respect to biopeptides, viral vectors and nanotechnology all presented possibilities for new forms of bioterrorism. It is difficult to predict precisely how these potentially disruptive technologies will manifest themselves in the future, but the workshop provided several illustrative possibilities when it described "black swan" scenarios.

Resources Necessary for a Bioterrorism Attack

The barrier to creating effective bioterrorism weapons is relatively low compared to other weapons of mass destruction. In one exercise, the participants were split into three groups and each group was given a different terrorist group profile. Resources provided in the profiles ranged from $15,000 to $100,000 and the groups as given possessed generally low levels of technical expertise. All groups were able to plan high-casualty bioterrorism attacks given their limited resources – both financial and intellectual. The participants concluded that high-consequence bioterrorism attacks are possible to carry out with limited resources, depending on a group's social network and patience. With an excellent social network, accessing additional resources such as bioagent seed cultures becomes far easier. However, additional time is also sufficient to amass adequate agents to conduct an attack. In simple terms, time, knowledge and commitment can compensate for a lack of material resources and even expertise. The participants concluded that "brains - not money" are the most important resource for bioterrorism.

Contents

1 Introduction

The goal of the *New Horizons in Bioterrorism* workshop on 11-12 August 2008 was to explore existing and future developments in bioterrorism through the elicitation and generation of adversary courses of action (ACOAs) and associated indicators.

The workshop supports the ongoing work of the Strategic Multilayer Assessment (SMA) and the Weapons of Mass Destruction and Terrorism (WMD-T) Joint Intelligence Preparation of the Operational Environment (JIPOE) funded by the United States Special Operations Command (U.S. SOCOM). JIPOE is a systematic approach used by intelligence personnel to analyze the adversary and other relevant aspects of the operational environment.[3] The JIPOE process is used to define the operational environment, describe the impact of the operational environment on adversary and friendly COAs, evaluate the capabilities of adversary forces operating in the operational environment, and determine and describe potential adversary COAs and civilian activities that might impact military operations. SMA is a program charged with finding new ways of analyzing and solving problems facing today's warfighter. Within the SMA, each problem is approached from multiple perspectives, including quantitative, qualitative, historical and cognitive views. The *New Horizons in Bioterrorism* workshop gathered several of the leading non-governmental subject matter experts in bioterrorism to formulate a qualitative perspective regarding adversary courses of actions (ACOAs) in bioterrorism from the present until 2015.

In the context of this workshop, bioterrorism was defined as the use of biological agents (or their derivatives) by non-state actors in order to cause harm. The definition provided was deliberately broad and included microorganisms and biological toxins, as well as synthetic versions of these. The issue of states directly engaging in biological attacks was not addressed.

ACOAs in the context of the workshop can be described as structured representations of the behaviors and activities preceding and associated with bioterrorism attacks. All ACOAs depicted high-consequence scenarios. The facilitator did not provide participants with a definition of "high consequence," instead letting participants offer their own perceptions of high consequence events. Ultimately, high consequence was broadly defined by the participants to extend beyond casualties to large-scale disruptions, including physical/medical, economic, political, and psycho-social well being, recognizing that even scenarios that do not lead to high casualties may have devastating effects in these other areas.

Additionally, the workshop focused on human-centered attacks. Although agroterrorism scenarios were discussed and determined to be an area of vulnerability to the United States, the facilitator asked the SMEs to focus on high consequences of attacks directed against human beings.

The remainder of this report first discusses the methodological parameters of the workshop, and then briefly outlines the workshop structure. Next, the report provides preliminary analysis of the ACOAs generated, based upon the Bioterrorism ACOA Database, developed specifically for this project and presented as an accompanying product. A section describing certain of the indicators that could be generalized is included and the report concludes with a section outlining major findings, and the next phases of the research.

[3] Joint Publication 2-0, *Joint Intelligence*, 22 June 2007, http://www.dtic.mil/doctrine/jel/new_pubs/jp2_0.pdf.

1.1 Workshop Participants

The ten academic participants consisted of terrorism experts who study the decision to use weapons of mass destruction (3), scientists with experience dealing with bio-weapons (2 microbiologists, 1 biochemist), an operational counterterrorism expert with bioterror investigation experience (1), and “all-rounders” knowledgeable in both the science and policy aspects (3). See Appendix A for biographies for the ten participants.

- **Dr. Victor Asal**, Political Science Department of the State University of New York at Albany
- **Dr. Ronald Atlas**, Center for Health Hazards Preparedness at the University of Louisville
- **Dr. Jeffrey Bale**, Monterey Terrorism Research and Education Program at the Monterey Institute of International Studies
- **Dr. Seth Carus**, Center for the Study of Weapons of Mass Destruction at the National Defense University
- **Dr. Leonard Cole**, Political Science Department of Rutgers University
- **Mr. Al Gomez**, National Technical Nuclear Forensics program at the Defense Threat Reduction Agency
- **Dr. Jeffrey (Randy) Good**, NOBLIS, Inc.
- **Mr. Barry Kellman**, International Weapons Control Center at the DePaul University College of Law
- **Dr. Jonathan Tucker**, Center for Nonproliferation Studies (CNS) of the Monterey Institute of International Studies
- **Dr. Raymond Zilinskas**, Chemical and Biological Weapons Nonproliferation Program at the Center for Nonproliferation Studies, Monterey Institute of International Studies

Gary Ackerman, Assistant Director for Research and Communication of the National Consortium for the Study of Terrorism and Responses to Terrorism (START), facilitated the workshop.

2 Methodology

The one-and-a-half-day workshop format was designed to formally elicit the opinions of bioterrorism experts regarding the most likely and the most high consequence threats facing the United States between now and 2015. Through moderated, directed sessions, the facilitator assisted the diverse group to explore both existing and new paradigms of bioterrorism. The formal elicitation process has been shown to help participants break out of normal heuristic pathways and think more creatively. A diversity of opinion among the workshop participants was encouraged with the ultimate goal of gaining some convergence (or at least structured divergence) in key areas. Elicitation techniques were primarily qualitative, based on a combination of traditional “brainstorming-type” elicitation methods and several proprietary pattern-disruption techniques. More traditional elicitation (basic ranking activities) was also carried out and enabled preliminary quantitative analysis, but the focus was on developing detailed, contextual ACOAs.

A groupware website, Mercury Grove,[4] was employed to elicit and record participants' opinions. The site allowed users to post messages to each other, upload or download relevant documents, and to share potential ACOAs. The collaborative environment made it easier to capture the group's ideas over the limited time span of one-and-a-half days.

The ACOAS were designed to be the workshop's primary output. ACOAs are a particular type of scenario; they comprise a defined sequence of adversary activities, and incorporate variables that are of analytic significance. Workshop organizers selected ACOAs as the primary output of the Phase I meeting because of their analytic utility; the formalized structure of ACOAs is advantageous relative to the vagueness and inconsistent utility of generic attack scenarios or notional plots.

The expert panelists were asked to focus on exploration of both high-probability ("most likely") and low-probability/high-consequence ("black swan") ACOAs. As a result, the elicitation was not directed towards exploration of intermediate-probability bio-attacks.

To build the ACOAs fully, participants were asked to supply information that would satisfy the following questions:

- o **Who** is likely to execute the ACOA?
- o **Why** the ACOA might be executed?
- o **What** would occur?
- o **Where** the ACOA will develop and materialize?
- o **When** the ACOA will progress through distinct stages and result in a bioterrorism event?
- o **How** the ACOA will be executed?

Tier 1 variables (determined by the workshop sponsors), as listed below, were the essential focus of the ACOA. Tier 2 variables were important elements of the ACOA that were specified and described where time allowed.

Tier 1 Variables:

- Precursor activities: identify and sequentially describe activities and associated signatures
- Bio-agent used in attack: description to include type (bacterial, viral, etc.), form (dry aerosol, liquid slurry, etc.), and characteristics (concentration, additives, encapsulation etc.)

Tier 2 Variables:

- Target of attack
- Means of procurement/production of bio-weapon
- Delivery method used
- Intended scale of attack
- Sophistication of attack (consistent with bio-agent description above)
- Effects:
  - o Psycho-social
  - o Political
  - o Economic
  - o Physical/Medical

[4] To view a demo of the information sharing tool, please go to http://www.mercurygrove.com/.

The ACOAs include both a narrative component and a coded set of up to forty variables (for a complete listing of variables covered, see Appendix D). This dual structure is believed to maximize the descriptive utility of the ACOA and improve its analytic value. The panelists were instructed to identify and describe any indicators associated with each ACOA. As the identification of precursor activities and other "signatures" of a pending bio-event were among the primary objectives of the Phase I meeting, the collective expertise of the panels was focused on this task.

Based on parameters provided by SOCOM, the threat horizon covered extended seven years into the future (2015) and allowed for probable scientific advances and potential time for adversary training and development. ACOAs could include all feasible (not necessarily realized) technological and motivational possibilities. ACOAs were designed to be developed by the expert panelists in an organic manner, an approach aimed at encouraging creativity that might otherwise be hindered by more traditional Cartesian attempts to cover the entire threat space. This encouraged panelists to step outside traditional thinking, disrupt existing heuristics, and generate non-linear recommendations.

As a consequence of the limited duration of the workshop, the discussions were based on a single world analysis, assuming no major distortions to the current global order or any other geo-political variables that might affect scenario development. Additionally, the workshop assumed that vulnerability levels will change only according to current expectations, i.e., that there will be only linear/marginal development in response plans, vaccines, detection systems, etc. These guidelines helped constrain the group to generate ACOAs without having to worry about "blue sky" defensive advances. This assumption is also consistent with the goals of the meeting and the established threat horizon.

Consistent with the informational objectives of SOCOM, the temporal scope of the ACOAs begins as early as practicable in the "threat chain" and progresses through to the operational deployment of biological agents. The basic operational timeline of ACOAs is depicted below:

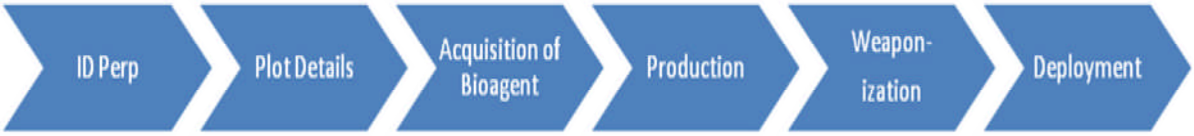


Figure 2-1. Notional Operational Timeline of an ACOA.

This notional representation in Figure 2-1 breaks down the aspects of interest within an ACOA and organizes them sequentially. The framework used at the workshop divided an ACOA into six parts: identification of the perpetrator, description of the plot details, acquisition of the bio-agent, production of sufficient quantities to perpetrate a terrorist event, the process of weaponization of that agent, and the method of deployment of the bio-agent in the attack. Whenever possible, the workshop participants were guided to provide detailed information about these aspects of the ACOAs, although not all ACOAs necessarily incorporated all six steps. Indicators of precursor activities were collected to enable the analysts to look as far "left of boom" as possible. Precursor activities were defined as anything that the adversary does prior to the attack, such as the theft of seed stocks or the purchase of equipment.

2.1 Workshop Exercises and Elicitation Techniques

This section provides a summary of the workshop format. A detailed script of the workshop, including the roles and activities of participants and staff is attached as Appendix C. Over the course of the first day of the workshop, and after introductory activities designed to "galvanize" creativity, participants brainstormed examples of potential terrorist attacks (both in response to facilitator prompts and in rapid-fire mode). The first exercise was *Exploring "Likely" Scenarios*. The objective was to elicit a set of scenarios that represent what participants believe to be at least somewhat likely, to accustom participants to the brainstorming process, to extract "low-hanging fruit", and to enable greater creativity. "Likely" scenarios were defined as those that participants believed have a greater than one percent chance of occurring by 2015. Throughout the course of the day, participants were asked to refine their scenarios to include the who, why, where, when, and how questions, as well as listing precursor activities. This brainstorming session resulted in over 20 initial ACOAs. Each participant described two of their most likely ACOAs to the group, before individually writing up their scenarios. Given all the ACOAs brainstormed to that point, each participant then ranked the top twenty most likely (see Table 3-5. Cumulative Ranking of Day 1 ACOAs.). The top ten were discussed in further detail and indicators for those ACOAs were collected. At the close of the day's activities, participants were given homework and asked to rank separately their opinions as to the top ten most likely perpetrators, modes of attack (bio-agent and deployment), and targets of attack.

On the second day, which focused on black swans – unlikely but high consequence events – the participants were asked to create, write down, and share orally an individual story using the "future backwards" technique, creating a reverse history of a catastrophic bio-terror event. The future backwards technique is used to interrupt the availability heuristic[5] and help participants think outside the box. This session emphasized new and advanced technologies.

The second exercise of the day was called *"Button Soup" red teaming*. In this exercise, the participants were broken up into three groups; each group was given a profile with information about their aims and organization, but restricted to a relatively low level of resources in order to focus attention on adversary improvisation and tactical innovation. Based on their profiles, the groups were asked to create a high casualty attack on the United States or its interests abroad. As the exercise continued, the groups were given the option of adding additional resources. This exercise generated three scenarios. The resulting plots were discussed in the larger group, and then submitted electronically by the participants.

Following this, positive and negative indicators were collected for the new ACOAs generated that day, and the types of attacks and targets that had not been discussed previously were directly addressed. Finally, future technologies were explored in more detail.

[5] The availability heuristic is a phenomenon (which can result in a cognitive bias) in which people base their prediction of the frequency of an event or the proportion within a population based on how easily an example can be brought to mind.

The primary output of the workshop was the generation of ACOAs, which are described in the following section. The ACOAs are neither comprehensive nor representative, but rather illustrate the range of bioterrorist threats faced by the United States over the next seven years.

3 Analysis of ACOAs

3.1 Overview

The Workshop resulted in the elicitation of 38 ACOAs in total, with 25 representing those scenarios which participants viewed as relatively more likely to occur by 2015 (i.e., with a subjective probability of occurrence greater than one percent), and 13 scenarios that were viewed as extreme events (i.e., with a probability of occurrence of less than 1 percent, often referred to as "black swans" or discontinuities). Of the 25 ACOAs in the "likely" category, only 17 were characterized somewhat comprehensively, with the remaining 8 ACOAs perhaps being more accurately described as "partial ACOAs." Nonetheless, even the less-than-complete ACOAs often reflected important details provided by the SMEs and were thus included in the following analysis in order to include any relevant information. A complete list of ACOAs generated by the participants is listed in Appendix B.

Each ACOA was coded into a database that represented the ACOA through forty variables, many of which can be analyzed cumulatively. The variables broadly reflected the ACOA process and were grouped under seven categories, viz. Perpetrator, Plot Details (including agent, target and motive), Acquisition of Bioagent, Production, Weaponization, Deployment, and ACOA Narrative (for a full list of variables used, see Appendix D).

The following sections present a basic descriptive analysis for those variables where there was sufficient data to draw at least preliminary inferences. One note of caution: since the participants were guided in some of the activities towards consideration of certain kinds of attacks, and since the number of ACOAs that could be elicited in the short time frame was limited, the ACOAs collected should not be viewed as a comprehensive or even representative sample upon which to append frequencies and probabilities. Rather, they are meant to illustrate the diversity of responses and in some cases (such as the selection of bioagents involved in the ACOA) are moderately suggestive of the relative emphasis that the SMEs place on specific features.

Perpetrator Identity

Of the 38 ACOAs provided, the SMEs did not specify a particular perpetrator for six ACOAs and three more were excluded from the analysis because they were provided by the organizers to the SMEs as part of the red-teaming elicitation exercise (see the Workshop Script in Appendix C). Figure 3-1 below represents the distribution of the remaining 29 ACOAs by perpetrator category.

It is apparent that the most common perpetrator type described by the SMEs were Jihadists, followed by Right-wing and Personal/Idiosyncratic (mostly used to describe lone perpetrators not linked to any specific ideological category; many were disgruntled or deranged scientists). While no firm conclusions can be drawn from this distribution (which may have been influenced by such factors as the availability bias), it is clear that religious motives seem to be associated closely with the use of biological weapons by non-state actors (especially if one adds together the 13 Jihadist, 2 Apocalyptic cult and 1 Christian Identity perpetrators). The SMEs' opinions thus accord closely with much of the literature on CBRN terrorism[6] as well as similar previous studies.[7] It should be noted, however, that perpetrators driven by religious motives were not the only perpetrators associated with possible bioattacks: a range of other actors, from right-wing militias to ethno-nationalists and radical environmentalists were also included.

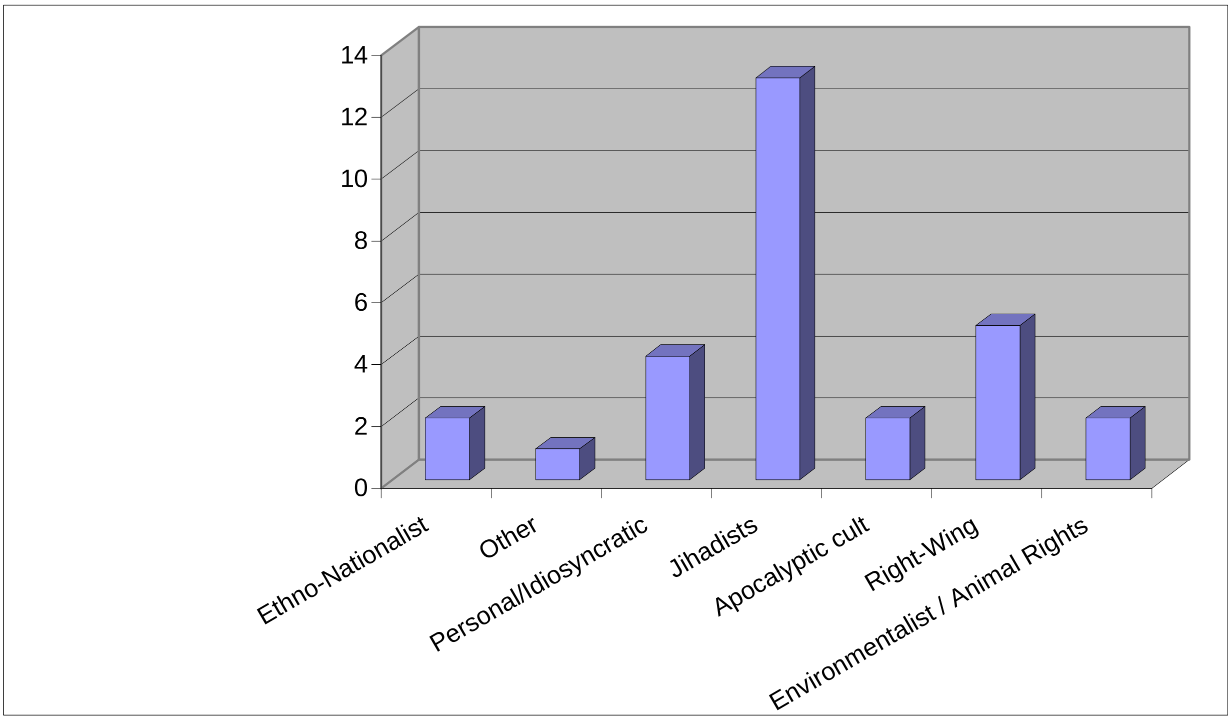


Figure 3-1. Distribution of Perpetrator Type in ACOAs

Intended Effects

High-consequence biological events are likely to have multiple, potentially-cascading effects on society, irrespective of the intent of the perpetrators. However, the SMEs were asked to speculate on the intended effects of each ACOA from the perpetrator's point of view. This included a variety of detailed motives (see the database for details), but also four general categories of effects that the perpetrators might hope to achieve:

- Mass casualties;
- High-level psycho-social disruption;
- High-level economic harm; and
- Large-scale political instability.

Discounting the 8 ACOAs where these effects were not specified, it is interesting to note that the perpetrators in 12 of the remaining 30 cases were viewed by the SMEs as seeking all four types of effect

[6] See, *inter alia*, Bruce Hoffman, *Inside Terrorism* (New York: Columbia University, 1998), p. 94; Gavin Cameron, "WMD Terrorism in the United States," *Nonproliferation Review*, 7:1 (2000), pp. 169-70; Nadine Gurr and Benjamin Cole, *The New Face of Terrorism: Threats from Weapons of Mass Destruction* (London: I. B. Tauris, 2002).

[7] Gary Ackerman, "The Future of Jihadists and WMD: Trends and Emerging Threats" in Gary Ackerman and Jeremy Tamsett (eds.), *Jihadists and Weapons of Mass Destruction*, (CRC Press, forthcoming 2008).

through their attacks, perhaps reflecting the opinion that biological weapons may generally be attractive to perpetrators who seek to achieve multiple objectives. Table 3-1 lists the number of ACOAs that contained each type of intended effect.

Table 3-1. Intended Effects of Perpetrators in Elicited ACOA.

Intended Effect of Bioattack	No. of ACOAs
Mass casualties	19
High-level psycho-social disruption	22
High-level economic harm	22
Large-scale political instability	18
Unspecified	8

In addition, in 22 of the 38 provided ACOAs, the perpetrators intended to deploy their biological weapon indiscriminately, not attempting to limit the harm to any particular person or small group.

Target

While the exact targets varied considerably by type and location, the target types most heavily represented in the collection of ACOAs supplied were private citizens / public places, the food and water supply, and transportation hubs and vehicles (see Figure 3-2).[8] The transportation infrastructure and general gatherings of private citizens are attractive targets for most forms of terrorism, but biological agents are especially apt for contaminating food supplies and products.

[8] The number of targets listed exceeds the total number of ACOAs because several ACOAs mentioned more than one type of target.

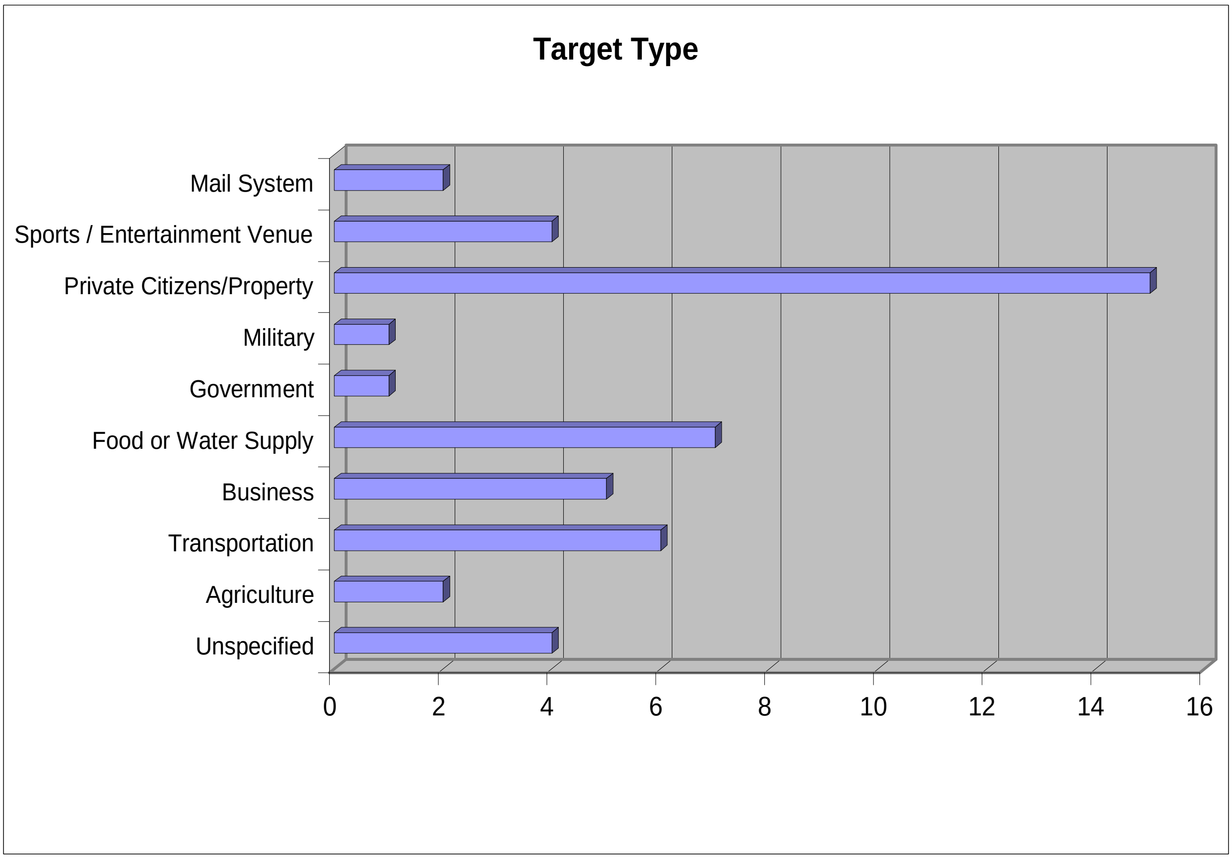


Figure 3-2. Target type, with heavy representation of private citizens / public places, the food and water supply and transportation hubs and vehicles.

Biological Agent

The SMEs proffered at least 19 different types of agents in the ACOAs, eight of which currently appear on the CDC's select agents list. Figure 3-3 shows a breakdown by class of agent and Table 3-2 shows the frequency of ACOAs in which specific agents appear.[9]

[9] Again, the total exceeds 38 since several ACOAs involved more than one bioagent.

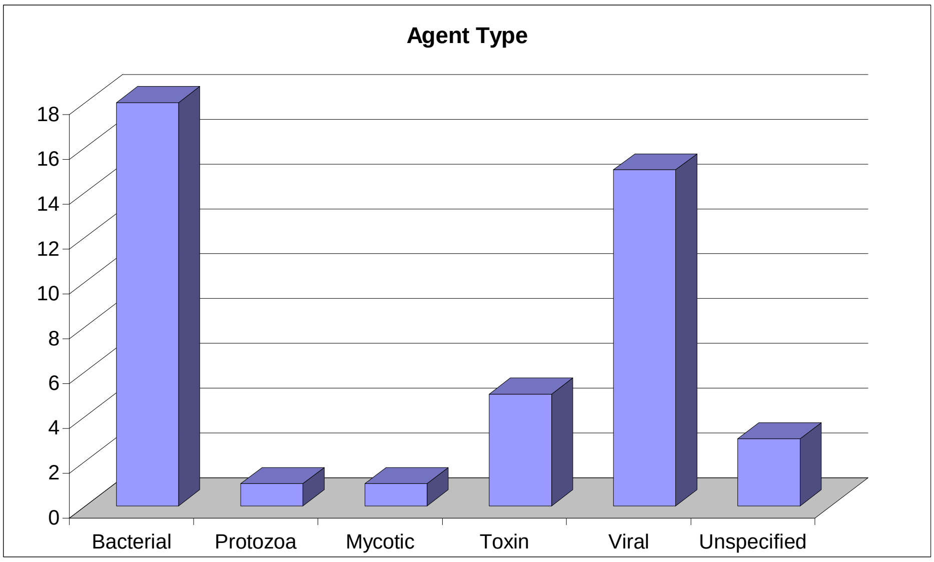


Figure 3-3. Agent type; bacterial and viral agents predominate.

Table 3-2. Specific Bioagents; eight agents currently appear on the CDC's select agents list. Bacterial and viral agents predominate.

Bioagent	**No. of ACOAs**
Anthrax (*B. anthracis*)	11
Ricin	4
Influenza (reconstituted 1918 or modified H5N1 strains)	4
Viral Hemorrhagic Fever	3
Foot and Mouth Disease	3
Typhoid fever (*S. Typhi*)	2
Smallpox (*Variola major*)	2
Modified orthopoxvirus (other than V. major)	2
Modified HIV	2
Rabies	1
Plague (*Y. Pestis*)	1
Novel agent: "Inflax" hybrid	1
Necrotizing fasciitis (*S. pyogenes*)	1
Measles	1
E. Coli O157:H7	1
Cryptospridium	1
Cholera (*V. Cholerae*)	1
Botulinum toxin	1
Amanita phlaoudes toxin	1
Unspecified	***3***

While all types of bioagents are represented, bacterial and viral agents predominate. In terms of specific agents, *B. anthracis* is far and away the most common agent used by the SMEs in constructing their ACOAs.

Acquisition

In terms of routes of acquisition of bioagent, Figure 3-4 summarizes the ACOAs. While the large number of thefts from laboratories points towards the need for vigorous security efforts, the fact that many of the perpetrators in the ACOAs obtained the bioagents from the environment is more troubling, since it vastly complicates the ability to observe acquisition attempts. Of the sixteen cases where an SME specified what form of the bioagent was acquired, only two ACOAs involved the acquisition of an intact weapon, while the remainder involved the acquisition of seed stocks which required further production and processing. In terms of the location of the acquisition, for the twelve ACOAs where this was specified, all but two acquisitions occurred in the same country as the perpetrator's intended target, obviating the need for shipping across international borders.

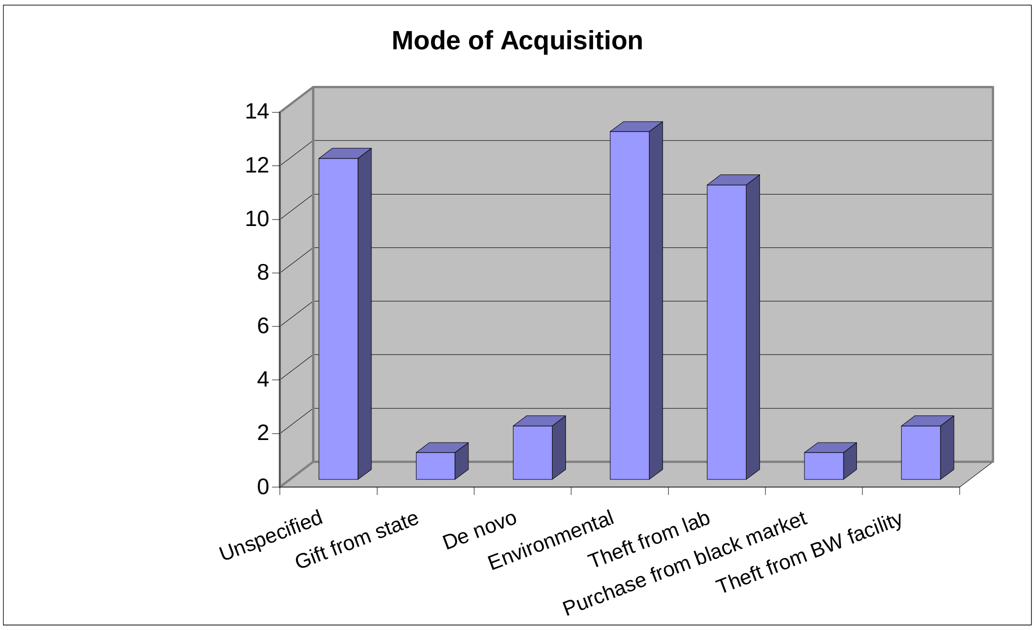


Figure 3-4. Mode of acquisition. Theft from laboratories point towards the need for vigorous security efforts, but environmental acquisition is more troubling.

Agent Enhancement

In 27 of the 38 ACOAs, there was no enhancement of the naturally-occurring form of the agent. However in 11 cases, the perpetrators enhanced or altered the naturally-occurring organism or toxin in some way. Table 3-3 displays the number of ACOAs in which one or more of several different types of enhancement appear. The relatively large number of ACOAs with enhancements stems at least partially from the "future backwards" elicitation exercise in which participants were instructed to focus on high-technology applications of biological attacks.

Table 3-3. Frequency of Agent Enhancement.

Number of ACOAs	Enhanced Survivability	Enhanced Lethality	Enhanced Infectiousness / Contagiousness	Inhibition of Immune Response or Treatment
2	X			
1	X	X	X	
2		X	X	X
2		X		X
1			X	X
2			X	
1				X

Production

Of the twelve ACOAs that noted the location of bioweapon production, in eight cases production occurred within the target country and in four cases, it occurred outside. Of the fourteen ACOAs where technical personnel were involved in production, there was one case of coercion, three of hiring external assistance and ten cases in which production occurred within the perpetrator group. However, since the participants did not seem to place too much emphasis on this aspect of production, such figures should not be viewed as being representative of their preferences. One interesting point is that in none of the twelve ACOAs where the number of technical personnel was mentioned, were more than 6 personnel required, and the modal number of personnel given as required was one. The number of ACOAs in which a specific level of equipment was described as necessary is given in Table 3-4.

Table 3-4. Level of Equipment Required for Production / Weaponization.

Level of Equipment	Number of ACOAs
Unspecified	***13***
Basic	10
Moderate	7
Sophisticated	8

Weaponization

Although several ACOAs described some of the details surrounding the process of agent weaponization, there were insufficient data points to discuss such factors as location, cost, or duration. Four ACOAs did however mention testing of the biological weapons, including on dogs, guinea pigs, and non-Caucasian people, which might have provided some tangible indicators.

Deployment

The only deployment-related variable for which sufficient data was provided was the method of bioagent delivery. Figure 3-5 shows the breakdown of delivery methods. As a general category, aerosol dispersal predominates, but contagion (by human vectors) and contamination also feature prominently.

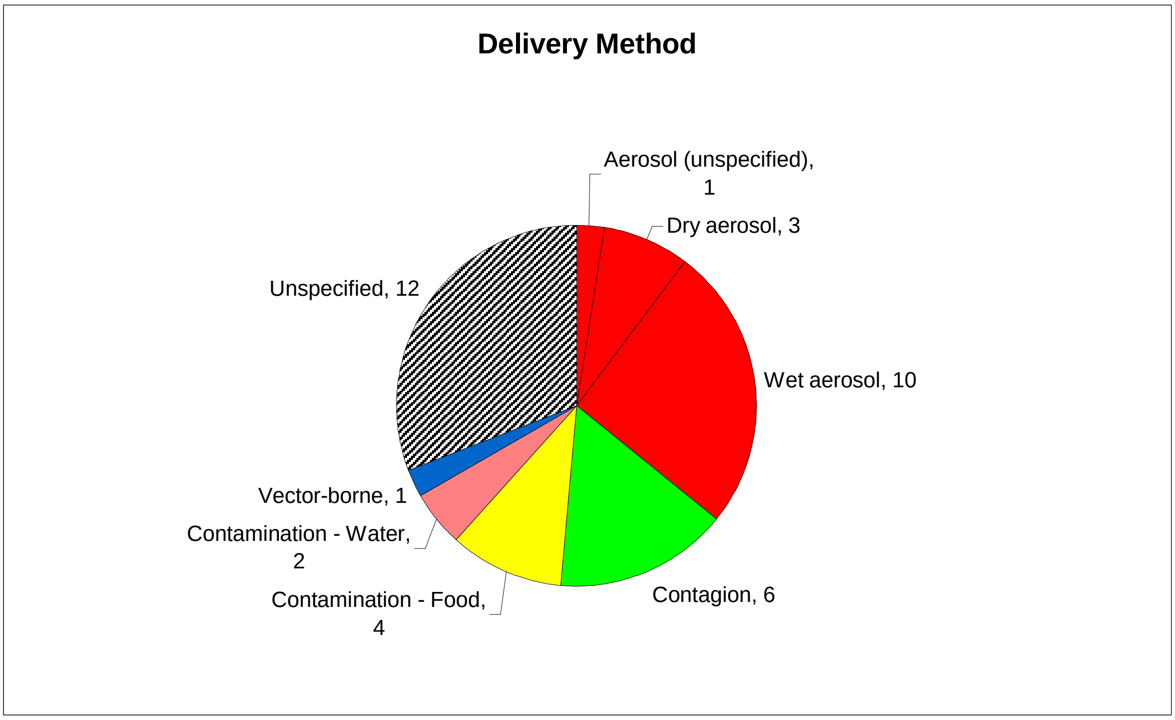


Figure 3-5. Bioagent delivery method. Aerosol dispersal predominates, but contagion (by human vectors) and contamination also feature prominently.

3.2 Ranking of ACOAs

While the frequency distributions of certain elements of the provided ACOAs detailed above can be suggestive of the relative importance attached to them by the SMEs, they do not substitute for a formal ranking. During Day 1 of the workshop, therefore, participants were asked to rank their top 20 ACOAs from those which they had provided under the "likely" category.[10] Each participant's ranking was then converted into a refined score[11] which was summed across participants. A cursory labeling of the 22 ACOAs from Day 1, ranked by their cumulative scores, is depicted in Table 3-5. Since the ACOAs are described only cursorily here, we recommended that the full ACOA be consulted, as listed in Appendix A.

Table 3-5. Cumulative Ranking of Day 1 ACOAs.

Brief ACOA Description	Cumulative Score
Salmonella poisoning of food, such as tomatoes and multiple foodstuffs	166
Al-Qa 'ida anthrax attack on sporting venue	131
Anthrax attacks on transportation hubs	122
Jihadist cell releasing ricin using a nebulizer in subway system	119
Mixture of placebo/true agent multiple dissemination strategy using anthrax overwhelming first responders	118
Right-wing terrorist attack using anthrax from natural source in US; distribution by agricultural sprayer in slurry form	113
Al-Qa 'ida penetration of university laboratory to produce anthrax	111
FMD Al-Qa 'ida attack on US soil from Indian cow drool source	110
Ricin turkey attack	109
Disgruntled Individual, botulism poisoning of bottles in beverage plant	100
Disgruntled individual spraying anthrax in grocery store	97
Long-term Al-Qa 'ida infiltration of food and water supplies to induce botulism poisoning	91
Weaponized anthrax attack on foreign city when American diplomats attend -- theaters or public places -- aimed at teaching the populace to spurn diplomacy with the US	89
LTTE anthrax attack through mail system	83
Christian-Identity group FMD attack against US agriculture	82
Al-Qa 'ida creation of pandemic avian flu outbreak using suicide operatives	63
Long-term synthesis of 1918 flu virus	60
Disgruntled scientist Camel pox modification and dissemination.	53
Smallpox release and targeting of transportation nodes	45
Isolation and dissemination of Flesh-eating bacteria	45
Pneumonic plague using Cats as a vector	37
Hamas: typhoid US water supply contamination	24

[10] Participants were not asked to rank the 13 "extreme" ACOAs, since these, by definition, were taken to have small but incomputable probabilities associated with them, see Nassim Nicholas Taleb (2007), *The Black Swan: The Impact of the Highly Improbable*, Random House (New York).

[11] The ranking was subtracted from 21, while leaving all zeros intact.

It is apparent from Table 3-5 that the ACOAs regarded as most likely by the participants were those involving contamination of food and beverages with toxins and fairly common microbes, in addition to the aerosol dispersal of *Bacillus anthracis* spores. However, participants argued that several of the ACOAs had not been specified in sufficient detail to allow for a direct comparison between them[12] and also that they did not have the opportunity to list all the elements they would have liked. Therefore, the workshop organizers distributed a ranking sheet on which the SMEs could rank separately what they regarded as the ten most likely perpetrators, attack modes and targets. SMEs were able to describe these as they saw fit and their raw answers were subsequently coded into categories similar to those used for the ACOAs. The resultant rankings provide a counterpoint to the above "whole ACOA" rankings. The summary results (with cumulative scores) are displayed below.

Table 3-6. Perpetrator Type Rankings.

Perpetrator Type	Cumulative Score
Religious	220
Personal / Idiosyncratic	134
Single Issue	21
Right-wing	12
State Sponsored	12
Criminal	11
Ethnonationalist	9
Left-wing	8
Unspecified	***9***

As is apparent, the Religious and Personal / Idiosyncratic categories were ranked highest by far, in large part mirroring the distribution found in the ACOAs (see above). These two categories can be broken down further into subcategories.

Table 3-7. Perpetrator Type Rankings – Detailed Breakdown.

Religious Perpetrators	Cumulative Score
Islamist (Sunni)	162
Apocalyptic Cult	22
Christian	15
Islamist (Shi'i)	11
Other	10

[12] For example, since some ACOAs included a named perpetrator (such as al-Qa`ida) while others involved only a generic type of attack, participants felt that a formal ranking to some extent would be like "comparing apples and oranges."

Personal / Idiosyncratic	Cumulative Score
Scientist	66
Student	15
Doctor	2
Unspecified	***51***

Al-Qa`ida and related jihadists lead the religious category, and disgruntled scientists lead the Personal / Idiosyncratic category. Overall, groups received a higher ranking than individuals, although individual perpetrators were still rated relatively highly. In terms of the origin of the perpetrators (relative to the U.S.), overall, foreign- based perpetrators were viewed as being twice as likely to launch high-consequence bioattacks as domestic perpetrators, although when viewed on their own, Personal / Idiosyncratic and Individual perpetrators were regarded as more likely to be domestic in nature than foreign-based.

Table 3-8. Group vs. Individual Rankings.

Structure	Cumulative Score
Group	277
Individual	159

Table 3-9. Domestic vs. Foreign Perpetrator Rankings.

Origin	Cumulative Score
Foreign	180
Domestic	90
Unspecified	***166***

In terms of the mode of attack employed, the tables below represent the cumulative rankings for agent and delivery method respectively.

Table 3-10. Bioagent Rankings.

Bioagent	Cumulative Score
B. anthracis	142
S. Typhi	58
FMD	47
Botulinum toxin	39
Y. pestis	39
Ricin	33
Viral Hemorrhagic Fever	22
Influenza	21
Variola major	17
E. Coli	10
African Swine Fever	7
Shigella	5
HIV	4
Hepatitus B	3
Other	3
B. cereus	1
Unspecified	***59***

Table 3-11. Delivery Method Rankings.

Delivery Method	Cumulative Score
Aerosol	155
Contamination – Food	132
Contagion	56
Contamination – Other	56
Direct Contact	38
Explosion	6
Other	4
Unspecified	***63***

These rankings compare favorably to those derived from the frequency of ACOAs (Figures 3-2 and 3-5), with anthrax heading the agents list by a large margin, and aerosol, food contamination and contagion leading the delivery method rankings.

Last, the SMEs ranked the most likely targets. As shown in the table below, transportation-related targets, public spaces and the food supply all ranked highly, similar to the distribution reflected in the ACOAs. The one somewhat anomalous inclusion is the high ranking that government-related targets received, since during the workshop the SMEs did not produce many ACOAs related to this type of target.

Table 3-12. Target Type Rankings.

Target Category	Cumulative Score
Transportation (vehicles or hubs)	77
Government (General)	71
Unspecified public space	71
Food supply	68
Sports / Entertainment Venue	67
Agriculture	39
Business	22
Mail system	18
Educational Institution	15
Consumer products	11
Water supply	9
Utilities	8
Government (Diplomatic)	6
Tourists	5

One can also separate the delivery method and target rankings, where applicable, into those attack modes utilizing enclosed versus open spaces as the locus of attack. Enclosed spaces are thought to be more likely (a score of 89 versus 26 for non-enclosed spaces in terms of delivery, and a score of 218 versus 20 for non-enclosed in terms of target).

In sum, it appears that, at least in terms of agents, attack modes and targets, the elements that the SMEs ranked most highly were reflected to a large extent in the ACOAs that they produced during the workshop. This provides some validation that the SMEs were providing consistent input and that the results of the workshop do indeed reflect their understanding and opinions of the threat of bioterrorism.

3.3 Indicators associated with ACOAs

During the workshop, there was sufficient time for the SMEs to supply indicators for 22 of the 38 ACOAs. While many of these indicators were specific to particular ACOAs, several of the indicators potentially have wider, more general application. While discussing indicators for specific attack modes, the participants realized that there were a set of general indicators that apply to many ACOAs. These are listed below.

General Indicators for a Particular Perpetrator Plotting a Biological Attack

- Ethno-nationalist groups interested in any biological agents or involved with biotechnology facilities.
- Intelligence "chatter" that a group is interested in biological agents
- Bioscientist (microbiologist, geneticist, veterinarian, etc.) humiliated, fired, demoted, underappreciated
- Attempts to buy antibiotics or vaccines
- Discussion on group websites concerning poisoning in general / theological justification of poisoning
- Visit to area of disease outbreak by group operatives (e.g., FMD outbreak site)
- Technological fetish of a religious cult
- High levels of resources
- Connections between states with biological weapons (BW) programs and terrorist groups
- Ideology oriented towards science / technology
- Acceptance of the use of mass murder as a tactic
- High-level education in microbiology, science
- Joining of a known terrorist / extremist organization by a capable person in biosciences
- Recruitment of scientists and technical personnel
- Attempts to hire scientists
- Known extremists embarking on bioscience degrees
- "Sponsorships, scholarships, fellowships" set up by terrorists
- Undeclared laboratory of any kind
- Explicit rationalization for harming livestock
- Veterinarian associated with radical group
- Criticism of foreign agribusiness
- "Humanitarian missions" by groups not normally involved in humanitarian activities to areas where a disease outbreak is occurring

General Indicators that a Perpetrator is Interested in a Particular Agent

- Research on viral aerosolization
- Resynthesis of any H5N1 or any other influenza viruses
- Counterfeit drug activities or production activities
- Diversion of anthrax sample from lab
- Attempts to buy antibiotics or vaccines
- Anaerobic fermentation
- Increase in abnormal production media to clandestine bioproduction facility
- Unpleasant odor
- Sampling of birds
- "Humanitarian missions" by groups not normally involved in humanitarian activities to areas where a disease outbreak is occurring
- Interest in HIV community / research
- Attempt to genetically engineer a virulence factor of one organism into another agent
- Indications of research on increasing the virulence of any organism
- Multiple purchases of castor beans or castor bean plants

- Asking of guides where to find dead animals who have died of anthrax
- Evidence of prolonged collection of poisonous mushrooms
- Solving the problem of requiring life to survive without water

General Indicators that a Perpetrator is Interested in a Particular Target

- Acquisition of mailing lists, phone books
- Surveillance of particular target (e.g., transportation hubs, beverage bottling plant)
- Buying stock in substitute products
- Attempts to infiltrate food/beverage processing plants by employment or other means
- Religious reference to destroying crops and animals
- Explicit rationalization for harming livestock
- Human testing on non-whites

General Indicators of Attempts to Acquire Bioagent

- Formal or informal reporting of missing material / components / cultures from laboratory or culture collection
- Reports of attempts to collect environmental samples
- Buying DNA fragments separately from synthesis labs
- Collecting of samples from disease (e.g., FMD) outbreak sites or where certain diseases (e.g., anthrax) are endemic
- Searching and monitoring of disease outbreak stories based in media, ProMed, OIE bulletins, etc.
- Unusual frequency or location of travel, e.g., traveling for first time to area where anthrax is endemic
- Sampling of birds
- Research on inhibiting human immune response
- Lack of security at foreign BW facilities
- Nexus between international crime and weapons of mass destruction (WMD) terrorism
- Anomalous behavior of former Soviet scientists
- Attempts to buy antibiotics or vaccines
- Break-in at a university laboratory

General Indicators that Biological Weapons Production is Occurring

- Establishment of covert laboratory (i.e., movement of materials / equipment to location where laboratory not established)
- Environmental footprint around production facility (e.g., reports by neighbors of strange smell or substances)
- Strange patterns of illness around production facilities
- Illness among known extremists
- Alert from screening software of production equipment in genetic synthesis facility
- Moving of a group of biological scientists (former biological weapons scientists) en masse to undesirable areas
- Purchase of DNA synthesizer
- Purchase of large, anaerobic fermenter

- Acquisition of protective equipment
- Any work being done on aerosolizing viruses
- Resynthesis of any H5N1 or any other influenza viruses
- Pursuing/being drawn into apocalyptic literature by a research scientist
- Seeking of lab equipment, technicians by a known extremist group

General Indicators of Weaponization of Bioagent

- Acquisition of trucks with water tanks, agricultural sprayers, foggers, nebulizers, etc.
- Purchase of lyophilizers
- Evidence of precipitating biological substances out of solutions
- Dead Guinea pigs or other test animals
- Human testing and associated activities, e.g., kidnapping or coercion of test subjects
- Testing contained in laboratory setting

General Indicators of Deployment of Biological Weapon

- Coordinated movement of multiple individuals of concern
- Specific intelligence "chatter"
- Observation of dumping substances into water sources
- Attempts to gain access to HVAC system
- Abnormal smell or taste of food / beverage / consumer product
- Abnormal behavior of employee at food / beverage processing facility
- Unauthorized persons in feedlots
- Customization of vehicles with sprayers
- Sick people walking through airports or other areas of concentration of persons
- Ill terrorists
- Extermination vehicles spraying and in operation together with an absence of known infestation
- "Sprucing up" salad bar or grocery aisle by non-employee

4 Additional Participant Insights

This section captures the kernels of knowledge expressed by the participants, which have not been captured by the analysis or the ACOAs. These insights may not apply to mainstream bioterrorism threats, but help the reader understand the greater context of the bioterrorism threat.

While foreign extremists operating abroad will likely continue to pose a bioterrorism threat, the participants emphasized that a comparable level of threat is presented by the knowledgeable individual insider. Participants discussed that one of the chief dangers is that of a scientist with access to a laboratory who may either become disgruntled or may be co-opted by a group to use his/her knowledge, access to agents, and laboratory facilities to facilitate a biological attack. Scientists working in laboratories often experience very little oversight (especially in non-U.S. contexts) and can use the agents and facilities available to them to surreptitiously grow and/or weaponize harmful agents. Another concern is the burgeoning number of laboratory facilities in the United States that handle the most dangerous pathogens – especially those dealing with select agents. Laboratory scientists in the United States have not historically been rigorously vetted, making laboratories vulnerable to infiltration by a group with a long time horizon. The participants concluded that they are less worried about terrorists becoming biologists and more worried about biologists becoming terrorists. This concern was reflected in both the rankings and ACOAs.

It is even possible for intelligent individuals with access to instructions on the internet to make large quantities of crude agents over time in an improvised laboratory - located in such nondescript facilities as a residential basement. These individuals could purchase, without much difficulty, second-hand dual-use fermenters from online vendors. The key element here is time – lethal bioagents can be produced in relatively crude facilities with few resources and a lot of time.

At the more advanced end of the spectrum, the pace of scientific advancement over the last ten years has been greater than most observers had foreseen. Therefore, the Unites States should anticipate novel advances in biotechnology that open new and terrible possibilities for bioterrorism. Scientists have reached the point of understanding the human genome where they can potentially create targeted bioweapons against a particular population or engineer virulence and infectiousness into novel organisms. Biopeptides, viral vectors, and nanotechnology advances all present potential dangers.

An unforeseeable but potentially devastating black swan is the emergence of a new naturally-occurring pathogen in the next seven years. Severe Acute Respiratory Syndrome (SARS) and avian flu are reminders that a natural or augmented disease could easily emerge reminiscent of the 1918 Spanish flu, which killed 20-100 million people worldwide. While a naturally occurring pandemic virus is not an act of bioterrorism, if a group claims credit for the attack, the response may still result in panic, economic disruption, and terror.

The following observations were made by participants as part of the discussion of potential events, participants made the following observations which, while not formally developed into or intended to be complete scenarios, engendered a fair amount of discussion. The first is **Salmonella** is an agent of concern. Sprinkling salmonella on food, as the Rajneeshees did with salad bars,[13] could put hundreds in a hospital. Salmonella is easy to grow and could have a large impact. The only technical barrier is growing sufficient quantities. A group intending to cause large casualties would likely attempt to conduct multiple attacks. The second observation involved an attack with anthrax spores on a stadium, entertainment venues, and office buildings (elevators, HVAC). One participant mentioned that this could involve a large group who could put 50 people in a stadium (or other area) with the aim of releasing **anthrax spores** during a sporting or other entertainment event and potentially killing more than 100,000 people.

5 Conclusion

The *New Horizons in Bioterrorism* workshop represents the first of three phases that will seek to better understand the nature of a bioterrorism attack and the indicators preceding a bioterrorism attack. To accomplish this goal all participants were directed to focus as far “left of boom” as possible. Taking into account the time and personnel constraints, the workshop yielded an impressive array of ACOAs that spanned the threat spectrum, all of which were captured in a database. In addition, the workshop recorded a wealth of insights from a diverse group of experts on the contemporary and near future threat of bioterrorism.

This report completes the Phase I objective of identifying the greatest bioterrorism threat ACOAs and their indicators by leading experts in the field. The second phase of the program will employ a Bayes Net Risk Analysis model and an Automated Behavioral Analysis model to generate priority threat scenarios. The third phase will integrate the ACOAs from Phase I, the risk estimates from Phase II, and a historical analysis in a classified session to evaluate and prioritize ACOAs. Intelligence or knowledge gaps will be identified and a top ten list of threats will be generated.

[13] Jonathon Tucker, ed. Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons, Chapter 8, the Rajneeshees by W. Seth Carus. MIT Press: Cambridge, MA, 2001.

A. Adversary Course of Action Narratives

The narratives below are presented in the approximate order in which they were elicited from the subject matter experts and do not reflect likelihood of occurrence (see the Analysis section above for a full discussion of the ACOAs).

The ACOAS listed below are the output of workshop participants. Some ACOAs are brief ideas expressed by individual participants as part of a brainstorming sessions, while others have been shaped and revised by the group. These ACOAs were generated to elicit key tactics, perpetrators, attack modes, and targets from workshop participants, which were studied in the main section of the report. The ACOAs are listed here to illustrate the breadth and depth of the participants' input over one and a half days.

A.1. "Likely" ACOAs

1: Botulinum Toxin in Coca-Cola Bottling Plant

A jihadist sleeper cell in New York City, seeking to attack an iconic symbol of U.S. imperialism and decadent Western culture, decides to poison a Coca-Cola bottling plant in the United States. The group receives authorization from al-Qa`ida central to proceed with the plan. Drawing on the expertise of a member who has a master's degree in microbiology, the group produces a liter of botulinum toxin by anaerobic fermentation over a period of two weeks. They then infiltrate an operative into a Coca-Cola bottling plant in northern New Jersey that supplies the New York City metropolitan area. The operative is hired as a worker on the bottling line and volunteers to work the night shift, when the intensity of surveillance is reduced. During the production of several batches, he injects the solution of toxin into the cola syrup before it is mixed with carbonated water on the assembly line. Cans and bottles containing the contaminated beverage are then widely distributed throughout the New York City area, causing dozens of fatalities. Within weeks, the FDA traces the outbreak to Coca-Cola, causing a dramatic drop in consumption of the beverage world-wide and the collapse of the company's stock price. The jihadist group later claims credit for the attack, claiming a symbolic victory over the "Great Satan."

Group discussion followed the creation of the scenario. One participant stated that this was an interpretation of the botulinum in milk supply article.[14] Almost anyone can acquire enough botulinum toxin to result in at least 1,000 deaths because the toxin would likely to be widely dispersed to the consumer end of the supply chain before it could be recalled. Participants were of the opinion that the perpetrator could even be a high school student who might or might not realize how dangerous the agent is. Additionally, improving the toxin slightly would not be out of the question, since information is available on the internet or one might accomplish it accidentally.

There was some debate regarding whether a well-established group would take the somewhat higher risk of getting caught in order to attempt this attack. A group may not want to target a very large corporation like Coca-Cola which probably has fairly high levels of security. On the other hand, many

[14] Lawrence Wein and Yifan Liu. "Analyzing a Bioterror Attack on the Food Supply: The Case of Botulinum Toxin in Milk." *Proceedings of the National Academy of Science*s. 12 July 2005. http://www.pnas.org/content/102/28/9984.full.pdf+html?maxtoshow=&HITS=10&hits=10&RESULTFORMAT=&fulltext=milk&searchid=1119981811614_5834&stored_search=&FIRSTINDEX=0&journalcode=pnas

groups might be willing to take the risk, either by not being concerned if members are caught or detected or by taking credit as part of their strategy.

Attacking the food supply from within the industry would likely require a group with a long operational time horizon, such as al Qa`ida. It might take several years for operatives to penetrate a facility to a degree where they have moments of unsupervised access to sensitive parts of the bottling/packing/distribution process. However, even contaminating one day's distribution of food or beverage could result in many illnesses.

Some indicators of this kind of attack include:

- discussion on jihadists web sites about poisoning;
- consideration of the theological correctness of poisoning;
- source information from informants;
- surveillance of bottling plants;
- buying stock in Pepsi;
- coworkers noticing suspicious activities;
- stolen supply of botulinum toxin or *C. botulinum*;
- acquisition of large anaerobic fermenter or other distinctive aspects of anaerobic fermentation;
- someone with a masters in microbiology linked to al Qa`ida traveling to Pakistan;
- awful taste.[15]

2: Tamil Tiger Anthrax Mailing

In this scenario, the United States government does something to upset the Tamil Tigers. The LTTE, a highly organized, technical, and well-connected organization decides to teach the U.S. a lesson. They gather together some bright people to grow and mill anthrax. They use their diaspora in Canada to distribute 10,000 letters to various cities around Christmas with no prior warning. The LTTE would need to produce a gram of anthrax per letter with an estimated 100kg required in all. The logistics of making 100kg of anthrax is technically challenging and would require an industrial scale facility unless the organization is willing to wait a couple of years. The LTTE decides to build a medium scale facility with 50 gallon fermenters. The organization can produce anthrax over a long period of time since the spores do not die. The LTTE followed a corporate strategy to either find anthrax naturally (elephants in Namibia) or buy it. It will take the organization about one year to produce 100 kilograms of anthrax.

In the discussion that ensued, most participants agreed that the odds of an organization producing 100kg of anthrax in the jungle are not very likely, nor is it likely to ship such large quantities of anthrax abroad for distribution. An organization is more likely to set up a facility in the country that it plans to attack, perhaps co-opting a scientist at a research lab to assist them. The organization could easily buy a 20-liter fermenter on eBay, especially since second-hand dual use equipment is not tracked in the United States. The fermenter could be set up in a lab or basement. Within less than a year, it would be possible to produce 100kg of anthrax using a 20-liter fermenter. The group could then mill the anthrax outside using a gas mask. The acquisition of a virulent anthrax strain is the most difficult part of this scenario.

[15] The medium for growing an anaerobe such as botulinum toxin has an awful taste. Quality control will have an instant recall based on taste alone, but the contamination might not be detected immediately.

Indicators for this event might include:

- the mobilization of resources to build a jungle lab;
- the acquisition of a large mailing list;
- statements by the LTTE expressing anger at the U.S.

Group Discussion: Use of a large lab facility to grow B. anthracis (anthrax spores)

It would be relatively easy to obtain or grow bioagents in commercial, university or research laboratories in the United States and abroad. A group could co-opt someone who already works there or plant someone there, even a student. The poor oversight of research in the labs makes them an ideal location for surreptitiously growing bioagents. An organization could also rent out lab space or fermenters and many labs would not ask what they were growing. In that case, an organization could produce a lot of material in one week. *Bacillus anthracis* is the logical choice but biosafety level two or three labs are not likely to have large scale facilities.

3: Contaminate tomatoes/jalapenos

Salmonella (S. typhimurium) could also be used to attack the food supply early in the food chain since produce is not normally treated to eliminate pathogens. Contaminating fields of tomatoes and peppers in a foreign country with salmonella would result in high-level consequences. The group can mimic a natural occurrence of food-borne illness by adding bacteria to the irrigation water. Perpetrators could also use certain strains of E. coli, such as E. coli O157:H7. The group could apply the agent at different sites on various days. The group could even apply the agent to various types of food so it was not apparent where it was coming from. This would eliminate confidence in the safety of the food supply and the ability of the government to protect the American public. A variation of the attack might include apples with the intent of impacting baby food and causing more panic. If the FDA (or the perpetrators) announced that the event was an act of terrorism, there would be a much greater impact. Perpetrators could be an anti-globalization or Nativist group.

Some potential indicators of an attack include

- the recruitment of microbiologists, lab equipment, etc., into a group with no a priori scientific experience;
- public criticism of NAFTA / globalization;
- specific criticism of importing cheap food;
- anger directed toward illegal immigrants;
- anger toward "imperialistic" corporate monopolies;
- criticism of agribusiness (more than imperialist monopoly);
- buying laboratory equipment;
- renting short-term laboratory space;
- collection or purchase of salmonella or E. coli;
- detection: outbreak in two different places that cannot naturally be coming from the same place.

4: Anthrax Diplomacy

In this ACOA, an organization obtains high-quality refined *B. anthracis* spores or seed cultures from a poorly-secured laboratory. At the group's own covert facility where they have assembled rudimentary but effective equipment for propagating, refining, and milling *B. anthracis* spores, the group produces

enough agent to commit multiple widespread attacks. Using a small team of operatives, all of whom are immunized against anthrax, the group identifies the Secretary of State's (or other senior diplomat's) international meetings. At the time of each such meeting, the group has one of its operatives release a quantity of anthrax spores in an enclosed entertainment or sports venue, using unsophisticated dissemination devices. The idea is not mass casualties at any one particular event but to convey the message: "Meet with U.S. diplomats and political leaders or establish supportive mutual relationships, and your people will get sick."

Indicators of this event might include:

- chatter about a particular diplomatic event or chatter about a high profile person's schedule.

5: Christian Identity Foot and Mouth Disease

A Christian extremist group decides to spread foot and mouth disease to several animal species through seven or eight states to seriously undermine the U.S. agricultural industry. The group obtains the agent naturally and grows it in their own lab. Another possible perpetrator of this attack could be an animal rights group.

Some indicators of this attack may include:

- non-authorized people loitering around infected cattle sites;
- explicit rationalization for harming livestock.

6: Toxic Turkeys

A few days before Thanksgiving, the Animal Liberation Front (ALF), seeking to protect animal welfare and deter the consumption of meat, contaminates pre-cooked turkeys in five different supermarkets across the U.S. with a crude solution of ricin prepared from castor beans using a recipe downloaded from the Internet. After a dozen people die, the ALF distributes a press release to the news media claiming credit for the attack and threatening follow-on poisonings unless the consumption of meat in the United States stops immediately.

7: Anthrax Slurry

A white supremacist group based in the northern tier states obtains anthracis from a downer animal. They isolated the organism, which was grown using a production lab bought from eBay. The anthracis was disseminated as a liquid slurry using an agricultural sprayer. The group targeted large eastern metropolitan area(s). The group intended to cause collapse of the U.S. government. This event requires moderate technical sophistication and good organizational skills.

8: Toxin Trains

A small cell of jihadists produces some ricin and disseminates it in subway cars in New York City and Chicago with a nebulizer, killing and sickening several people.

9: Infectious Agent Spread at Transportation Centers

Operatives carrying an infectious disease (smallpox, hemorrhagic fever) travel through various transportation centers. A related scenario would be to attack a transportation hub--actually multiple hubs--with aerosolized anthrax. This would have the impact of causing multiple outbreaks across the country. It likely would lead to a massive flood of worry that would overwhelm the healthcare system as well as causing actual casualties.

Participants agreed that the above scenario is low tech and would not require highly trained scientists. If a scientist wanted to demonstrate how clever he or she was, however, it could result in a scenario involving genetic engineering or synthetic biology. One participant mentioned that the FBI initiated an event where a person on a flight had simulated hemorrhagic fever. Although everyone was aware that it was a simulation, the scenario became so realistic that people panicked. One person tried to escape the plane and the FBI drew guns and tackled him.

10: FMD Drool Collection

A sympathetic scientist has been retained as a microbiological consultant to an al-Qa`ida front organization to cause enormous economic damage to the U.S. By consulting ProMed, he learns about a sizeable outbreak of Foot and Mouth disease (FMD) in India. He travels to the site of the outbreak and collects drool from affected cattle and places it in a plastic tube with appropriate holding media. Passing through customs easily, he suspends the drool in sterile saline, places the saline in a spray bottle, and travels up and down highway 101 in California dispersing the solution by spray over the snouts of cattle, cows, sheep, and horses. Two weeks later, the damage to the U.S. economy is likely to be greater than $30 billion.

Possible indicators include:

- visit to area by al-Qa`ida operatives to FMD outbreak site or lab;
- jihadist religious reference to destroying crops and animals;
- anyone collecting samples from FMD outbreak sites;
- searching and monitoring of FMD stories based in media, especially OIE;
- unauthorized persons in feedlots.

11: Overwhelm Response Capability

From a perspective of complicating response, the most likely bioagent is *B. anthracis*. It could be delivered by either an individual or group with the behavioral resolve and the technical feasibility to develop, transport, and disseminate the agent despite any technical or logistical obstacles. The emphasis would be on an overall strategy to maximize dissemination and achieve the maximum consequence, both in terms of U.S. infrastructure and human casualties, domestically and/or internationally. The objective would be to fully understand the response capability of the local, state, and federal entities. Further, the group could identify and attack multiple locations with multiple frequencies over a substantial period of time, which could be weeks, months, years, but also introducing false positives to distract and overwhelm different aspects of the response capability.

12: B. Anthracis and Disgruntled Employee

A disgruntled employee isolates a pathogen from the environment that will likely make people ill. He takes his time and waits for an anthrax outbreak somewhere so he knows it is a virulent strain. He grows this environmental sample in his home in a makeshift growth culture that he can easily learn about online. Periodically he takes samples to the local grocery store, food markets, restaurants, etc. and spreads it around on food, table, and other surfaces. Much of it will not be effective, but some will be effective. Additionally, this process is cheap, easy, and has a very low chance of discovery, so he can do it for a long time and take credit for all of it.

13: Avian Flu

An organization connected to al-Qa`ida will get samples of the current H5N1 Avian Flu virus. Consulting with a very sophisticated bioscientist, the group will work on culturing variants of that

virus that are highly person-to-person contagious. Once a variant is identified that is stable, lethal, and contagious, the group will infect, perhaps surreptitiously, a group of “suicide bombers” and instruct them to circulate through densely populated areas (entertainment venues, airports and train stations), spreading the virus through touch, sneezing, coughing, etc. The motivation here is to put an end to the corruptive influences of modern civilization by causing an apocalypse. Once the pandemic has gathered steam, the group will augment its health consequences by spreading rumors of other imminent disasters.

Indicators for this kind of attack may include:

- a disgruntled or recently-fired scientist;
- acquisition or use of a gene synthesizer.

14: Typhoid in Water Supply

HAMAS releases typhoid (S. typhimurium) in non-chlorinated water supplies in areas like Albany, NY. In 1939, there was a case of the Japanese successfully contaminating Russian water supplies.

15: Here Kitty…

Pets can be used as a vector of disease. An organization can spread the plague among outdoor cats and dogs. People are infected through contact with their pets.

16: Flesh-Eating Bacteria

A sociopathic hospital worker collects samples of the "flesh-eating" strep bacteria (S. pyogenes), and then sprays it in public places where it can infect those with open sores or wounds. This could cause a large psychological impact on the U.S. population if even some of the victims develop necrotizing fasciitis.

17: 1918 Spanish Flu

A disgruntled scientist resynthesizes the 1918 Spanish Flu. Only a nihilistic individual or an apocalyptic group would attempt this because there is no way to protect themselves from the disease.

Possible indicators include:

- scientist being humiliated, fired, demoted, or underappreciated;
- buying DNA fragments separately from synthesis labs;
- buying a DNA synthesizer or the unauthorized use of one.

18: New Smallpox Threat

After having gained expertise on orthopox viruses, a scientist studies camel pox as a surrogate for smallpox virus. As a side project to his regular work, he genetically engineers the camel pox virus (which is genetically the closest of all orthopox virus to the smallpox virus) so it becomes essentially the same as the smallpox virus. He then sells his creation to an apocalyptic or environmental terrorist group for economic gain.

19: Biological Unabomber

A PhD microbiologist takes isolate of organism with which he is familiar (could be moderate to low virulence). He then cultures it and uses it in any appropriate means to cause moderate to high casualties. The attack could be food contamination if the individual has no dissemination skills, but also could be aerosolized depending on the agent and the dissemination skills of the perpetrator.

20: Pathogens on Public Surfaces

An organization co-opts a student in a lab who has access to a pathogen that is not readily available in nature. This would make it clear that this was a terrorist event. Growing the agent at home or in the lab from which it is isolated would be the easiest option. The group would take the agent to local population centers (malls) and place it on surfaces that people will be touching. This will likely result in some numbers of casualties for which the group can take responsibility.

21: Anthrax Attack

A scientist sympathetic to Islamist extremism provides a group with access to anthrax from his laboratory. After procuring the seed bacteria, the group conducts a long-term growing and processing effort in a private hidden laboratory. The group's objective is to kill/sicken some and cause anxiety and negative economic effects. The attack causes widespread anxiety. The attack is carried out at multiple points included mail (with no threat message) and in shopping malls. The agent is released when recipients opened the contaminated envelopes, as well as near HVAC vents in enclosed public facilities. The group claims credit by phone after the attacks.

22. Aryan Nation Ricin Release

A small group of political / ideological "Aryan Nations-type" extremists release ricin to strike fear into "corrupt" and "nefarious" highly visible American cultural and political locations. The goal is not so much to kill as to cause anxiety. The group surreptitiously releases powder in theaters, local government offices (e.g., social security, motor vehicle, post offices) and later reveals the cause by phone as well as the locations where the powder was released. The attack is planned to coincide with a major event such as elections, World Series, etc. The attack is carried out by individuals dropping powder without notice or attention, near vents or lightly blowing fans.

Day 2: Extreme ACOAs ("Future Backwards")

On the second day, which focused on black swans – unlikely but high consequence events – the participants were asked to create, write down, and share orally an individual story using the "future backwards" technique, creating a reverse history of a catastrophic bio-terror event. The future backwards technique is used to interrupt the availability heuristic[16] and help participants think outside the box. This session emphasized new and advanced technologies.

1: Ethnic Group Virus

Over the course of five years, 35 percent of the human race was wiped out by a virulent disease designed to focus on particular ethnic group. In the winter of November 2015, outbreaks in Boston targeted the African American community. People left Boston in droves. Over 144 people were infected intentionally. They traveled around the world to major travel hubs, moving with the seasons. The agent was prepared starting with a scientist (a skilled microbiologist) that joined a doomsday cult offshoot of the Creativity movement. Production was facilitated by other members of the doomsday cult. The group used a pox virus acquired from a university laboratory and modified it to be highly lethal, highly communicable, and highly resistant to treatment. The agent was created so that it would

[16] The availability heuristic is a phenomenon (which can result in a cognitive bias) in which people base their prediction of the frequency of an event or the proportion within a population based on how easily an example can be brought to mind.

infect everybody, but the lethality is variable according to certain genetic features/ markers posited by the group as being "non-white". The motive was to purify the world for the Aryan race. The key perpetrator was a highly skilled microbiologist who worked with group over long time to create this disease and come up with plan to spread it throughout world.

Potential indicators may include:

- Aryan identity movement with a twist of apocalyptic nature;
- research scientist pursuing / being drawn into apocalyptic literature;
- research into ethnic specific bioagents;
- modification of a relatively non-virulent strain of pox to make it more virulent in humans through genetic modification;
- break-in at university laboratory;
- formal or informal reporting of missing material / components / cultures;
- establishment of covert laboratory (i.e., movement of materials / equipment to location where laboratory not established);
- screening software of production equipment in genetic synthesis facility sounds an alert;
- environmental footprint around production facility (e.g., reports by neighbors of strange smell or substances);
- strange patterns of illness around production facilities;
- human testing (on-non whites) and associated activities, e.g., kidnapping or coercion of test subjects.

2: Infectious Pandemic

In multiple incidents worldwide, thousands of people were injured and killed in what has been initially defined as potentially-related infectious pandemics. Health care facilities have been overwhelmed in these locations. Medical and first responder personnel have been affected, which has diminished these capabilities and resources and exacerbated the crisis. Transportation means have created bottlenecks for injured and others to move. Government facilities and officials are confused and attempting to calm public and maintain continuity of government. Many key government officials and functions have been affected. Private industry has also been affected and there is greatly diminished output of goods and services due to infected employees and transportation obstacles. A highly virulent form of anthrax, with high resistance to prophylactics, was identified that was disseminated in a bioterrorist act in multiple locations worldwide. Dispersal was accomplished by highly effective mobile, vehicle-borne, aerosol dispersal methods enhancing inhalation. This occurred in the spring months of 2012 during a pattern of mild weather that was predetermined by the strategic plan of the attackers. The attack was carried out on Western democratic governments and allies in New York, Los Angeles, Washington DC, London, Madrid, Sydney, Canberra, and Paris. The attack originated with an Iranian state sponsored program to develop this agent in conjunction with a unified group(s) of Islamic Jihadist fundamentalists, who conspired on this attack over several years and planned simultaneous attacks. The anthrax was developed and designed by a covert biological program and by recruiting sympathetic, highly educated Islamic scientists to support the attack. The intended motive was to continue threatened attacks on the U.S. and its allies to discredit and diminish Western democratic government and economic influence.

Potential indicators of this event include:

- connections between states with BW programs and terrorists;

- indications of research on increasing virulence of anthrax;
- purchase of sprayers.

3: Aerosolized HIV

The contagiousness of HIV increased drastically throughout the world, which also meant that the mortality rate of AIDS increased dramatically. By 2015, the number of persons dying from AIDS was over 100 million and the direct costs relevant to treating affected persons have destroyed the economies of many nations; the United States experienced the 2011 Depression. The HIV was originally altered by induced mutation to be spreadable by aerosol. In the event, unexpected mutations occurred, making human-to-human transmission possible. The new strain also proved to be more virulent than the wild form and brought about AIDS many years sooner than to speed to which the world had been accustomed. The mutations occurred accidentally when scientists in a laboratory tried to alter the HIV virus so it would be useful as a terrorist weapon and spreadable by aerosol; i.e.; by having such a pathogen, its owner could blackmail a nation by threatening to depopulate it. It was the intent of these scientists to simultaneously develop a vaccine to protect favored populations, but the accidentally-induced mutation occurred so unexpectedly that no vaccine had been perfected. The synthesis of the virus occurred in winter 2010 in a laboratory in Japan. The new virus escaped the laboratory, carried by one of its developers to a basketball game where it was spread further by aerosol. The propagation of the new mutation of continued as it had in the 1990s. As noted above, the original intent of the developers was to develop and produce a strain of HIV that would be perfect for political blackmail. It was meant to be spread by aerosol but was not to be contagious. Specifically, the strain was to be used to force the Japanese government to pardon and release all surviving members of the Aum Shinrikyo, especially its jailed leader Asahara. The original strain was natural, but the mutated strain was accidentally produced in the laboratory. The original perpetrators were scientists who had been converted by members of the Aleph (which is the reincarnation of the Aum).

Potential indicators include:

- hiring of scientists[17] ;
- interest in HIV community / research;
- work done on aerosolizing viruses;
- environmental footprint;
- undeclared lab.

4: The Great Inflax Epidemic

Between 2012 and 2014, one million people in the U.S. became critically ill, of whom more than 30 percent died. A previously unknown hybrid microorganism carried the communicability of an influenza virus and the virulence of Ames strain anthrax bacteria. The genetic structure of the organism seemed patterned after the 1918-19 Spanish flu virus, which also incorporated antigenic features of the three virulence factors of the anthrax bacterium. The organism and subsequent disease has come to be called "inflax." Cases began appearing in March-April 2012. After two months of confusion about the nature of the outbreak, in June it became understood that the epidemic originated from at least a half-dozen point sources: evidently aerosolized in a shopping mall in Columbus, Ohio, the metro in DC, the BART in San Francisco, the NYC subway, Houston Astrodome, and the Mirage Casino in Las Vegas. A few dozen people in each location became infected from the

[17] Groups which have previously done wrong should be monitored for the hiring of new scientists.

released organisms. During the incubation period of three to ten days, infected individuals going about normal routines further infected family members, friends, and others with whom they were in close proximity. These secondary carriers then infected others, creating a domino effect. No drug was able to counteract the effects, and the disease dissipated on its own in due course. The hybrid organism, some people recalled, was similar to one that Ken Alibek claimed was a goal in the old Soviet program. It was evidently developed in secret by a few veterans of the Soviet program. Working in Russian laboratories, the effort had been funded by the increasingly secretive Russian regime. The state's leadership, now all-but-completely subject to the will of Vladimir Putin, began to exhibit a resurgent authoritarian nature in 2008 following the absorption of Georgia into the expanding Russian orbit. The actual distribution of the inflax hybrid was carried out by Islamic jihadists. They had obtained it from one of the Russian scientists who were sympathetic to their anti-American doctrines. Releasing the organism would further encourage Americans to withdraw from international involvement, they believed.

Potential indicators for this event include:

- anyone trying to genetically engineer one virulence factor of one organism into another agent;
- lack of security of foreign BW activity;
- nexus between international crime and WMD terrorism;
- anomalous behavior of former Soviet scientists.

5: UFO Cult Engineers Avian Flu

Several million people were killed in North America by a virulent flu spread from Toronto. It was a genetically engineered variant of avian flu. The agent was intentionally released in an aerosol form in the western Toronto suburb of Mississauga using two vans equipped with sprayers. It was intentionally released in aerosolized form using two vans equipped with sprayers. It later emerged that the group had procured a sample of the avian flu virus and then subjected it to genetic engineering processes in its labs before actually deciding to "weaponize" it and release it in an aerosol form. The agent had been released in the wake of public threats by the Canadian government to ban certain dangerous "religious sects." This event began at 2 pm in the autumn of 2011, on a clear, sunny day in October. The group responsible had prepared the genetically-engineered strain of the avian flu in its own laboratory facilities in its headquarters outside Montreal. The perpetrators had hoped to prevent a government raid on their headquarters by creating a catastrophe that would divert the attention of the authorities in Ottawa, as well as warn them that it had the capacity to do even greater harm. The perpetrators were members of the high-tech Raelian UFO cult, whose leader had only arranged for the manufacturing of a genetically-engineered variant of the avian flu as a last resort, in the event that the Canadian government opted to ban the group.

Potential indicators for this event include:

- religious cult with a technological fetish;
- high-level education in microbiology, science;
- high levels of resources;
- previous threat issued by group promising retribution if government takes action against them;
- laboratory facilities (declared OR undeclared) owned by religious/utopian group;
- any undeclared laboratory;
- establishment of covert laboratory (i.e., movement of materials/ equipment to location where laboratory not established);

- environmental footprint around production facility (e.g., reports by neighbors of strange smell or substances);
- strange patterns of illness around production facilities;
- sampling of birds;
- acquisition of protective equipment;
- unusual frequency or location of travel;
- “humanitarian missions” by groups not normally involved in humanitarian activities OR to areas where outbreak is occurring;
- acquisition of sprayers;
- customization of vehicles with sprayers.

6: Water Contamination in Africa

Contamination of virtually all public water sources across Africa in 2011 killed millions who had no access to clean water for consumption or irrigation of food crops. It was caused by a mixture of food-borne and waterborne pathogens (Vibrio, Cryptosporidium, cholera, etc.). Each water source was contaminated by large scale inoculation by trucks or the placement of slow-leak barrels into the water supply. The attack was facilitated by mass migration from many civil wars that concentrate the populations across the continent. The attack started at the beginning of the growing season when food supplies were already low and new food production was not an option. Primary water supplies and rivers were targeted; the ongoing contamination of water supplies continued for months. Agents were produced and prepared in large-scale facilities on the continent set up in old industrial facilities in places like Somalia or Angola. These locations were used to develop large amounts of bioagents, without drawing much attention due to the low levels of oversight of activities. Many of these areas were controlled by gangs and militant groups. Initial attempts to acquire the agent from nature were used as test bed experiments, and proved to be of insufficient quality to kill on a large scale. Thus, later development was based on an organism that was acquired from a laboratory source that had been modified with additional antibiotic resistance. The goal of the event was to introduce political unrest and chaos across Africa, spurring mass migration, governmental instability, and terror across the world. Though the development of the organism was carried out by a gang/warlord in Africa, it was funded and facilitated by a group of former Soviet officials. The goal of the Soviet group was to impose costs on the Western world by exacerbating problems in the developing world.

Potential indicators may include:

- formal or informal reporting of missing material/ components/ cultures;
- reports of observers viewing attempts to collect environmental samples;
- covert setup of laboratory by scientists in Africa;
- establishment of covert laboratory (i.e., movement of materials/ equipment to location where laboratory not established);
- movement of former biological weapon scientists / experts to Africa;
- movement of group of biological scientists en masse to undesirable areas of developing world (bio-knowledge base moving from one area to anther);
- strange odors near laboratory facilities;
- illness around suspected laboratory facilities;
- sudden increase in construction activities, including trucks in the area;
- acquisition of barrels / trucks with water tanks;

- observation of dumping into water sources.

7: Doomsday Attack

Everyone in the world died. The devastation began in 2013. The attack was carried out by a radical splinter branch of a known Indian separatist group that previously had used civil disobedience to achieve its aims. The perpetrators wanted to destabilize the Indian government but the infection spread out of control. The infection began in India as a result of an attack by a radical separatist group and spreads worldwide. They used EITHER: 1) the smallpox virus - obtained from the Russian biological weapons program from a scientist who formally worked at the facility (the smallpox is genetically engineered to insert immunomodulators that crippled the immune system); OR 2) the influenza virus synthesized de novo in the laboratory from DNA sequences obtained from commercial sources (a mixture of influenza viruses synthesized to include virulent the 1918 strain and a H5N1 strain that had emerged in Indonesia); OR 3) modified HIV which was acquired from an infected individuals and modified to be transmissible via aerosols. The agent was produced at a facility within India that purportedly was a biotechnology company – the agent was genetically modified in the lab and grown in tissue culture, and since this was a highly infectious agent only small quantities were needed to be introduced to the target population. The devastation began during 2010. Simultaneous attacks occur in July in Mumbai at the railway station and the airport. Most people died between October and December of 2010 but significant disease outbreaks continued into January – March; by April the world order had been totally disrupted. Within a year a full third of the world population had died. Those not felled by the infection themselves starved because there were no food supplies. The entire social support system collapsed. The world went black as the electric grid failed.

Potential indicators for this event include:

- anyone researching HIV aerosolization;
- ethno-nationalist groups interested in any biological agents or involved with biotechnology facilities;
- counterfeit drug activities or production activities;
- surveillance of transportation hubs detected;
- resynthesis of any H5N1 or any other influenza viruses;
- strange patterns of illness around production facilities;
- Alert from screening software of production equipment in genetic synthesis facility.

8: Petroleum Bacteria

From 2013 to 2015, the worldwide spread of a genetically engineered bacterium caused an 80 percent decline in global GDP. Hundreds of thousands of people died from food shortages or froze to death from a lack of heating fuel. The disaster began when an environmental terrorist group called Earth First sought to sabotage the U.S. oil-based economy, halt the pollution of the biosphere, and force the rapid adoption of renewable energy technologies. In April 2013, Earth First stole a genetically engineered bacterial strain from a biotech research firm called Green Genes in Rockville, MD. The highly robust strain had been developed for the purpose of digesting petroleum products for the bioremediation of oil spills. It was designed not only to be highly efficient at digesting hydrocarbons, but also resistant to ultraviolet radiation and genetic mutation. Earth First infiltrated an operative into the firm, who was hired as a laboratory technician. Because he had an advanced degree in bacteriology, he was able to identify and divert a seed culture of the strain. The operatives cultivated the bacterium in crude fermentation tanks and used it to attack petroleum-based transportation and industrial sites and to degrade synthetic rubber products across the United States. Unexpectedly, the

bacterium turned out to be capable causing a sub-clinical infection in migratory birds, which carried the agent to other continents and dispersed it in their guano.

Potential indicators for this event include:

- diversion of genetically-engineered strain;
- contained testing in laboratory setting;
- solving the problem of requiring life to survive without water.

9: Measles Pandemic

With the intention of subverting modern governments and causing populations to lose faith in their governments' ability to keep them safe, an apocalyptic group of Islamic fanatics developed an immune-resistant and especially-lethal variant of measles. Their attack was preceded by isolated anthrax attacks which, although not optimally effective, caused worldwide panic about bioterrorism. Following those attacks, the perpetrators initiated an FMD outbreak in South America, further causing fear about bioterrorism. The measles outbreak was inflicted by intentionally-infected "suicide" terrorists (a few dozen) who spread it throughout the world's key transportation hubs, especially in countries having weak public health systems. Under the radar screen of the anthrax and FMD attacks, the virus picked up critical mass before it was recognized; by that time, it had circulated throughout most of the world. In the end, approximately 10 percent of the world's population was infected, and of that group approximately 20 percent died (about 150 million casualties). More devastating was the collapse of governments worldwide as popular confidence evaporated – the precise goal of the perpetrators. The pandemic, which started in Istanbul, Calcutta, and Sao Paulo, spread worldwide. There was substantial political and economic dislocation and instability that affected developing nations more heavily. Perpetrators infected a few dozen supporters (probably without full disclosure of consequences) and sent them to key transport hubs. The steps involved were: (1) gathering of measles strains from laboratories and supply houses (via diversion); (2) building of a covert laboratory in east Africa including equipment and materials; (3) genetic manipulation of the virus; growth of the virus. The motivation was de-stabilization of governments, social unrest worldwide; and massive migrations. The perpetrators were a wealthy apocalyptic sub-group of Islamic fanatics, primarily from south Asia and east Africa.

Potential indicators of this event include:

- intelligence that group is seeking widespread political destabilization;
- research on inhibiting human immune response;
- formal or informal reports of diversions from supply houses of samples;
- sick people walking through airports, train stations, etc.

10: Hemorrhagic Fever

In 2015, 500,000 people died in China from a disease outbreak. A viral hemorrhagic fever (VHF) known as the Shanghai virus caused the outbreak. Perpetrators disseminated the Shanghai virus as an aerosol in multiple releases in several major urban areas. It was released on several days in January 2015 in the evening – although it could have been released in the daytime because the air pollution might mask much of the UV that normally would kill the organisms. The agent was disseminated upwind of target cities with the intent to cover large areas. The agent was grown in cell cultures and the agent was placed in a slurry for dissemination in an agricultural sprayer. The Shanghai virus was stolen from a research facility in 2012 in China by a lab technician sympathetic to the perpetrators. The virus was originally discovered by a team of Chinese scientists working in the Congo in support of

the WHO. Perpetrators wanted to kill a lot of Chinese and disrupt the Chinese economy. The perpetrators were part of a Muslim separatist group based in Western China.

Potential indicators of this event include:

- acceptance of the use of mass murder as a tactic;
- formal or informal reporting of missing material/ components/ cultures;
- establishment of covert laboratory (i.e., movement of materials/ equipment to location where laboratory not established);
- environmental footprint around production facility (e.g., reports by neighbors of strange smell or substances);
- acquisition of protective equipment;
- purchase of agricultural sprayers[18].

Claiming Credit Where No Credit is Due

A smart group could wait for a natural outbreak of disease and then claim credit. It is hard to disprove responsibility, and would have a high psychological impact on the U.S.

[18] If the United States kept track of purchases of agricultural sprayers, this indicator would be easily noticed. However, tracking the sale of all agricultural sprayers would be an enormous undertaking.

A.2. High Casualty ACOAs with Limited Resources

The participants were split into three groups, which were given separate terror group profiles. Resources ranged from $15,000 to $100,000 and the groups had generally low levels of technical expertise. All groups were able to plan high-casualty bioterrorism attacks given their limited resources – both financial and intellectual.

Table A-5-1. Summary of Red-Teaming Group Attributes.

Variable	Group 1	Group 2	Group 3
Name	Church of the Heavenly Spires	Jaish al-Qiyama (Army of the End Days)	Purity Commandos
Ideology / Objectives (esp. relative to casualties).	UFO cult – believe can only ascend when humanity is cleansed of its tainted multitudes and demonstrate mastery over nature.	Homegrown cell intent on punishing the West, causing U.S. to withdraw from the ME politically and militarily and ushering in global Caliphate.	Right-wing supremacist militia group; seek to eliminate non-White threat and initiate race war.
$ Resources	$100,000	$45,000	$15,000
Number of members	12 members	6 members	23 members
Skill set	Internet proficiency; basic firearms and bombmaking skills.	Internet proficiency; basic firearms and bombmaking skills.	Internet proficiency; basic firearms and bombmaking skills.
Leadership / Decisionmaking structure	Authoritarian: “Vorlock”	Spiritual sanctioner and operational leader make decisions.	Consultative process.
Operational Experience	None	None	Armed gas-station robberies; infiltrated facilities in the past by posing as janitors, etc.
Popular support	None	None; virtual connections to other jihadist communities over internet.	Small pockets in local community.

11: Church of Heavenly Spires

The Church of Heavenly Spires has two college graduates with basic biochemistry background. They are modeled on Aum Shinrykio, but they want to do it “right”. The group buys ciprofloxacin and sends some of its members to Namibia. The organization spends a few thousand dollars collecting anthrax at Etosha National park. The member brings dirt samples back in a plastic bag. The group also spends $30-40,000 on lab equipment to culture anthrax including for an incubator, fermenter, lyophylizer, etc. The intended targets were evil aliens posing as humans. Attacks were to be concentrated in subways in San Francisco, New York City, Chicago, and DC – cities with large subway systems and where the group believes perverse behavior is most rampant. A second wave attack is planned for the casinos in Las Vegas.

The group receives additional resources. The first resource is a person who knows how to "weaponize" i.e., effectively aerosolize *B. anthracis*. The second resource is more equipment to help refine and weaponize. The revised plan calls for dispersing anthrax inside subway carts. Two operators will be used in each city with a possible third in San Francisco. Three to four operators are put on standby to conduct a second wave if the first set of operators are caught. The third new resource is a scientist from the University of Galveston from a biosafety level four lab who has access to a South American Hemorrhagic Fever virus. The group is able to grow stocks from seed stock provided by the Galveston scientist. This time the target is airports and passenger airliners.

Potential indicators of this event may include:

- recruitment of scientists;
- Ideology oriented towards science / technology;
- undeclared laboratory;
- novel travel to areas where anthrax is endemic;
- asking wildlife guides where to find dead elephants;
- surveillance of target destinations;
- buying Cipro;
- buying equipment;
- environmental footprint (for B. anthracis production);
- illnesses around production facility.

12: Jaish al-Qiyama: Ricin in Germany and Salmonella U.S.

Jaish al-Qiyama is a self-actualized cell of jihadists. Their goal is to punish the West in order to get the U.S. to withdraw from Iraq. The group sent a few of its members to take microbiology classes for free in Sweden. As a side project, the organization set up a lab in one of the member's basement to start growing bioagents. The group intends to grow large quantities of salmonella and ricin. The group has a two-stage plan that does not require much money or resources. Two members of the group will go to the U.S. while the rest will focus on Germany. The Germany team will obtain jobs in the food industry for companies that supply American bases. They will target their ricin efforts on American bases in Germany. In the U.S., members will get jobs and grow salmonella waiting for D-day. D-day is two weeks after the attacks in Germany. The group will set up a website to explain why they are taking these actions. One member is fluent in English and will record messages. Another member will be in charge of production. The group succeeds in killing lots of soldiers. Two weeks after the attack, American team will go into action. The U.S. team will take salmonella and contaminate salad bar in two different directions making their way across the U.S. All the salmonella created will be taken on the road, where the perpetrators will hit every fast-food or grocery salad bar until they run out. Then they will state that this is only the first wave. Starting in Philadelphia, they will drive north/south and west on two separate routes and use Google Maps to plan their attacks. The idea is to kill a thousand American troops, and send thousands of Americans to the hospital.
Added resource: An informant/operative inside American bases in Germany.

Indicators for this scenario might include:

- known extremists embarking on bioscience degrees;
- "sponsorships, scholarships, fellowships" sponsored by terrorists;
- multiple purchases of castor beans or castor bean plants;

- attempts to infiltrate U.S. bases;
- environmental footprint;
- illness around production facility;
- ill Jihadists.

13: Purity Commandos

The Purity Commandos are a white supremacist group in Idaho with poor capabilities and poor resources. They take a local resource – the Amanita phlaoudes mushroom, which is the most toxic mushroom in the world – and process it into a fine powder. The mushroom is easy to identify and grows abundantly in Idaho. They group tests the powder on dogs and estimates that one mushroom could kill five people. They sprinkle the powder over food supplies. People get sick. Three days later victims recover, but their livers are permanently damaged. The only hope is a liver transplant. The group used the powder to do directed sabotage of non-white markets. The group targets salad bars in San Francisco or targets Hispanic populations in agricultural towns. They leave literature behind.

Eventually, the group obtains more resources. They recruit a veterinarian who has access to anthrax. The group grows *B. anthracis* based on instructions from the internet. The additional resources allow them to buy sprayers they need to disseminate the *B. anthracis*. They spray the agent using a truck camouflaged as "Medfly extermination" in predominantly African American or Hispanic communities in Los Angeles, which has good inversion. Five or six days later, the outbreak kills 10,000. An additional resource that could be useful is a modern nebulizer that can be adjusted for particle size, and has GPS system for exact and precise spraying.

Potential indicators of this event may include:

- extensive collection of poisonous mushrooms;
- absence of Medfly infestation, but Medfly extermination vehicles spraying and in operation;
- environmental footprint of anthrax;
- illnesses around production facility;
- veterinarian associated with radical group.

B. Participant Biographies

Gary Ackerman

Gary Ackerman is Assistant Director for Research and Communication of the National Consortium for the Study of Terrorism and Responses to Terrorism (START), and is responsible for managing START research projects, exploring new avenues for research, and establishing collaborative research relationships with other institutions. Mr. Ackerman previously held the post of Director of the Center for Terrorism and Intelligence Studies, a private research and analysis institute. Prior to taking up his current position, Mr. Ackerman was Director of the Weapons of Mass Destruction Terrorism Research Program at the Center for Nonproliferation Studies in Monterey, California, and he earlier served as the Chief of Operations of the South Africa-based African-Asian Society. He received his M.A. in International Relations (Strategic Studies - Terrorism) from Yale University and his Bachelors (Law, Mathematics, International Relations) and Honors (International Relations) degrees from the University of the Witwatersrand in Johannesburg, South Africa. Originally hailing from South Africa, Mr. Ackerman possesses an eclectic academic background, including past studies in the fields of mathematics, history, law, and international relations, and has won numerous academic awards. His research encompasses various areas relating to terrorism and counterterrorism, including terrorist threat assessment, terrorist technologies and motivations, terrorism involving chemical, biological, radiological, and nuclear (CBRN) weapons, terrorist financing, environmental extremism, and the modeling and simulation of terrorist behavior.

Victor Asal

Victor Asal joined the faculty of the Political Science Department of the University at Albany-SUNY in fall 2003 (Ph.D., University of Maryland, 2003; M.A. Hebrew University, Israel, 1996). Asal is also the Director of the Public Security Certificate at Rockefeller College, SUNY, Albany. Asal is a specialist in Comparative Politics and International Relations with his research focusing on the interaction of international relations and domestic politics, notably how this interaction influences ethnic conflict and ethnic terrorism. Asal's current research looks at the impact of political discrimination on ethnic conflict and terrorism. Asal also is looking at the impact of organizational actors on terrorist behavior. In addition, Prof. Asal works with the Crisis and Negotiation Group in researching the impact of styles of mediation on crisis negotiation using both empirical and experimental methods.

Ronald Atlas

Ronald M. Atlas is Graduate Dean, Professor of Biology and Public Health, and Co-director of the Center for Health Hazards Preparedness at the University of Louisville. He received his BS degree from the State University at Stony Brook, his MS and PhD degrees from Rutgers the State University, and a DSc (honoris causa) from the University of Guelph. He was a postdoctoral fellow at the Jet Propulsion Laboratory where he worked on Mars Life Detection. He is chair of NASA's Planetary Protection Subcommittee, co-chair of the American Society for Microbiology (ASM) Task Force on Biodefense and co-chair of the sub-committee on Science of the National Academies of Science Committee on Science, Security and Prosperity in a Changing World. He is also a member of the Council of Graduate Schools' Government Relations Task Force as well as the FBI Scientific Working Group on Microbial Genetics and Forensics. He previously served as President of ASM, was a member of the NIH Recombinant Advisory committee, was on the Board of Governors of the Council of Graduate Schools (CGS), and was a member of the DHS Homeland Security Science and Technology Advisory Committee. His early research focused on oil spills and he discovered bioremediation as part of his doctoral studies. Later he turned to the molecular detection of pathogens in the environment which forms the basis for biosensors to detect biothreat agents. He is author of nearly 300 manuscripts and 20 books. He is a fellow in the American Academy of Microbiology and has received the ASM Award for Applied and Environmental Microbiology, the ASM Founders Award, and the Edmund Youde Lectureship Award in Hong Kong. He regularly advises the U.S. government on policy issues related to the deterrence of bioterrorism.

Jeffrey Bale

Jeffrey Bale is a Director of the Monterey Terrorism Research and Education Program at the Monterey Institute of International Studies. He obtained his B.A. in Middle Eastern and Central Asian history at the University of Michigan, his M.A. in social movements and political sociology at the University of California at Berkeley, and his Ph.D. in contemporary European history at Berkeley. He has taught at Berkeley, Columbia University, and the University of California at Irvine, and was the recipient of postdoctoral fellowships from the Society of Fellows in the Humanities at Columbia, the Office of Scholarly Programs at the Library of Congress, and the Center for German and European Studies at Berkeley. Dr. Bale has been studying extremist and terrorist groups for many years, and has published numerous articles on terrorism, right-wing extremism, Islamism, and covert operations. Dr. Bale has co-authored several texts on WMD terrorism and has participated in numerous government studies on the subject.

W. Seth Carus

Dr. Carus is the Deputy Director of the Center for the Study of Weapons of Mass Destruction and a Distinguished Research Fellow at the National Defense University. His research focuses on biological warfare threat assessment, biodefense, homeland security, and the role of the Department of Defense in responding to chemical and biological terrorism. He also is researching allegations of biological agent use by terrorists and criminals, and has written a working paper, “Bioterrorism and Biocrimes: The Illicit Use of Biological Agents in the 20th Century,” and several articles on that subject. He has been at NDU since 1997. From 2001 to 2003, Dr. Carus was detailed to the Office of the Vice President, where he was the Senior Advisor to the Vice President for Biodefense. Before assuming that position, he was on the staff of the National Preparedness Review, where he was commissioned to recommend changes in homeland security organization and supported the Office of Homeland Security while it was being established. Prior to joining NDU, Dr. Carus was a research analyst at the Center for Naval Analyses. He worked on studies for NAVCENT on naval forward presence and for the Office of the Secretary of Defense on the impact of nuclear, biological, and chemical weapons on the conduct of a major regional contingency in Korea. From 1991 to 1994, Dr. Carus was a member of the Policy Planning staff in the Undersecretary of Defense for Policy, Office of the Secretary of Defense. Before joining the government, he was a research fellow at the Washington Institute for Near East Policy. Dr. Carus has a Ph.D. from the Johns Hopkins University in Baltimore, Maryland.

Leonard A. Cole

Dr. Leonard A. Cole is an adjunct professor of political science at Rutgers University, Newark, New Jersey, where he teaches science and public policy. He is an expert on bioterrorism. Trained in the health sciences and public policy, he holds a Ph.D. in political science from Columbia University. Cole has written for professional journals as well as general publications including *The New York Times*, *The Washington Post*, *Los Angeles Times*, *Scientific American*, and *The Sciences*. He has testified before congressional committees and made invited presentations to several government agencies including the U.S. Department of Energy, the Department of Defense, the Centers for Disease Control and Prevention, and the Office of Technology Assessment. He has appeared frequently on network and public television and has been a regular on MSNBC. He is the author of six books including *The Eleventh Plague: The*

Politics of Biological and Chemical Warfare and, most recently, *The Anthrax Letters: A Medical Detective Story*.

Alan Gomez

Alan S. Gomez served as an FBI Special Agent in the FBI for 21 years and was assigned general investigative duties in criminal investigations of White Collar Crime, Violent Crime, Fugitive, and Drug related investigations for 15 years. During these responsibilities, Mr. Gomez also received extensive training in crime scene management and response while assigned to the FBI Evidence Response Team (ERT) program as a member and team leader. He received extensive training in forensic evidence recovery techniques, and the management and response to many crime scenes to conduct the recovery of evidence. Mr. Gomez also spent 6 1/2 years assigned as a Supervisory Special Agent assigned to the Hazardous Materials Response Unit (HMRU) of the FBI Laboratory. During these responsibilities, Mr. Gomez also received extensive training and experience in hazardous materials response. He participated in many WMD responses in support of FBI criminal investigations involving chemical, biological, and radiological incidents both domestically and internationally. These responses involved the administrative and operational management of a field operations program that consisted of 27 Hazardous Materials Response teams with over 350 operational response personnel located in various FBI field offices. He has also received training and actual event experience in the National Incident Management System (NIMS) and the Incident Command System (ICS). Mr. Gomez is currently assigned to work in the National Technical Nuclear Forensics program for the Defense Threat Reduction Agency (DTRA) to develop and prepare for operational response to a national level nuclear incident.

Randy Good

Dr. J. Randall Good is a Senior Manager in the Center for National Security and Intelligence at Noblis. Dr. Good oversees programs in the biological/medical defense, bioinformatics, and critical infrastructure protection areas. Dr. Good has an extensive and multifaceted background in the bio-defense area with focus on medical defense. He has spent most of the last eight years with the Institute for Defense Analyses' (IDA's) Science and Technology Division where he provided scientific, technical, and programmatic support to the defense, national security, and intelligence communities in biological and chemical defense, technology assessment and development, bioinformatics, and the analysis of worldwide science and technology efforts and capabilities. While with IDA, Dr. Good supported the Strategic Technologies Office at the Defense Advanced Research Projects Office (STO/DARPA) in the acceleration of the operational deployment of novel technologies, and the Intelligence Community in the review of research and development portfolios in the biological sciences. Dr. Good also served as co-chair of the Biomedical and Biotechnology working groups for the Military Critical Technologies List (MCTL). Dr. Good helped create the new Science and Technology Policy Institute in the Executive Office of the President (EOP) (2003–2005). While with the Institute, he created and implemented a standard for the assessment of emerging pathogens, performed an assessment of medical countermeasures to chemical agents, performed an assessment of the requirements and cost of implementing the Select Agent Rule for laboratories performing research with identified pathogens, and identified programs and resources of interest to the intelligence and national security communities. As an Adjunct Professor at George Mason University (2001–2005), Dr. Good assisted in the development of a multidisciplinary degree program in Biological Defense, and developed and instructed graduate courses in bioinformatics. Dr. Good has a Ph.D. from Baylor College of Medicine and a B.S. from the University of North Carolina at Wilmington. He has extensive additional professional and technical training at the Sherman Kent School for Intelligence Analysis, the Army Institute for Professional Development, and the Defense Systems Management College, among others.

Barry Kellman

Barry Kellman is a Professor of international law and is Director of the International Weapons Control Center at the DePaul University College of Law. Professor Kellman's work for the past decade has focused primarily on biological terrorism. Professor Kellman has published widely on: weapons proliferation and smuggling, the laws of armed conflict, Middle East arms control, and nuclear non proliferation, including his most recent book, *BIOVIOLENCE: Preventing Biological Terror and Crime* (Cambridge University Press, August, 2007). Professor Kellman's professional work has long been concerned with weapons of mass destruction proliferation and terrorism. He worked for ratification and implementation of the Chemical Weapons Convention as lead author of the *Manual for National Implementation of the CWC* (1993; 2nd ed. 1998) and by testifying to Congress as to the constitutionality of its inspection scheme (1997). He was commissioned by the Memorial Institute for the Prevention of Terrorism (MIPT) to draft *Managing Terrorism's Consequences* (2003), which reviews legal authorities for responding to terror activity in the United States.

Jonathan B. Tucker

Jonathan B. Tucker is a Senior Fellow specializing in chemical and biological weapons issues in the Washington, D.C., office of the James Martin Center for Nonproliferation Studies (CNS) of the Monterey Institute of International Studies. Before joining CNS in 1996, he worked at the U.S. Department of State, the congressional Office of Technology Assessment, and the Arms Control & Disarmament Agency. From 1993 to 1995, he served on the U.S. delegation to the Chemical Weapons Convention Preparatory Commission in The Hague, and in February 1995 he was a United Nations biological weapons inspector in Iraq. Dr. Tucker holds a B.S. in biology from Yale University and a Ph.D. in political science from the Massachusetts Institute of Technology. He has been a visiting fellow at Stanford's Hoover Institution, the U.S. Institute of Peace, and the American Academy in Berlin, and a Fulbright Scholar at the German Institute for International and Security Affairs. He is a life member of the Council on Foreign Relations and serves on the board of the Arms Control Association. His books include *War of Nerves: Chemical Warfare from World War I to Al-Qaeda* (Pantheon, 2006); *Scourge: The Once and Future Threat of Smallpox* (Grove/Atlantic, 2001), and *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons* (MIT Press, 2000). Dr. Tucker's current research interests focus on emerging biotechnologies such as synthetic genomics and their implications for the chemical and biological control regimes.

Raymond Zilinskas

Dr. Zilinskas is the Director of the Chemical and Biological Weapons Nonproliferation Program at the Center for Nonproliferation Studies. After earning a Ph.D. in 1981, Dr. Zilinskas worked at the U.S. Office of Technology Assessment (1981 - 1982), the United Nations Industrial Development Organization (1982 - 1986), and the Center for Public Issues in Biotechnology, University of Maryland Biotechnology Institute. In addition, while at Maryland he was an Adjunct Associate Professor at the Department of International Health, School of Hygiene and Public Health, the Johns Hopkins University. In 1993, Dr. Zilinskas was appointed a William Foster Fellow at the U.S. Arms Control and Disarmament Agency (ACDA), where he worked on biological and toxin warfare issues. In April 1994, ACDA seconded Dr. Zilinskas to the United Nations Special Commission (UNSCOM) for seven months, during which time he participated in two biological warfare-related inspections in Iraq (June and October 1994) encompassing 61 biological research and production facilities. At UNSCOM headquarters, he set up a database containing data about key dual-use biological equipment in Iraq and developed a protocol to guide UNSCOM's on-going monitoring and verification program in the biological field. On September 1, 1998, Dr. Zilinskas began working as a Senior Scientist in Residence at the Center for Nonproliferation Studies, Monterey Institute of International Studies (MIIS), Monterey, CA. His research focuses on achieving effective biological arms control, the proliferation potential of the former Soviet Union's biological warfare program, and meeting the threat of bioterrorism. He also is a Research Professor at the Graduate School of International Politics at MIIS, where he teaches courses on biological and chemical weapons and arms control and emerging issues in international public health. Dr. Zilinskas' book *Biological Warfare: Modern Offense and Defense*, which provides a definitive account on how modern biotechnology has qualitatively changed developments related to biological weapons and defense, was published in 1999 by Lynne Rienner Publishers. He also is co-editor of the *Encyclopedia of Bioterrorism Defense,* which was published in summer 2005 by Wiley and Sons.

C. Workshop Elicitation Script

The workshop elicitation script was designed to aid the facilitator in encouraging participants to think broadly and unconventionally about the bioterrorism threat to the United States from now until 2015. The script may seem formulaic, but it was constructed to obtain the highest quantity and quality input from the participants as possible in a limited amount of time. The script describes the exercises, the facilitator's role, and the role of the note takers and other assistants. Please see the script below.

Bioterrorism Workshop
Elicitation Script

Time	#	Session Title	Session Goals	Session Details		Roles				
						Facilitator	*Participants*	*Ashley Arana*	*Pam Toman*	*Matthew Rhodes*
Mon, August 11										
10:30		***Staff Arrival***				Preparations and checks.	N/A	Preparations and checks.	Preparations and checks.	Preparations and checks.
12:00 - 12:30	**0**	**Arrival and registration**	Assemble participants for on-time start; create relaxed, isolated atmosphere; familiarize each participant with collaborative software.	Participants will be registered, given name-tents and shown to their places. Snacks and drinks (sandwiches???) will be available in case participants have not had lunch. Instrumental classical music in background. Participants will be shown how the collaborative software works.		Informal introductions, verifying that all particpants are present or on their way.	Leave outside world behind; get comfortable; test collaborative software.	Keep track of missing participants; any participants not present by 12:20 should be contacted by phone.	Registration	Assist with software familiarization.

12:30 - 13:00	**1**	**Kick-off**	Welcome and introduce participants; convey admin information; outline expectations and parameters; orient workshop in participant mental frames; "prime" participants for elicitation with breakout scenario.	Welcome (5 mins)		Introduces himself; Welcomes participants; Brief introductory speech: a) why we are here – select group of diverse, exceptional individuals to explore a pressing topic; b) who NSI and JIPOE are and what we seek to get out of the Workshop; b) sensitivity of information: stressing the importance of discretion in using or distributing the ideas generated during the Workshop.		[If needed: prepare printouts of kick-off scenario]		
				Introductions (10 mins)		Manages participant introductions.	Provide brief introductions.			
				Admin Info (3 mins)		Admin information (bathrooms, expense reporting, etc.)				
				Audio-visual breakout scenario (5 mins)				Ready with backup in case of technical difficulties.		
				Describe elicitation (7 mins)		Briefly describes elicitation process, stressing creativity, sober assessment, etc. and gives parameters (e.g. only interested in substantial effect attacks) - on display and handouts.		Distribute handouts.	Distribute handouts.	
13:00 - 13:45	**2**	**Exploring "Likely" Scenarios**	Elicit a set of scenarios that represent what participants believe to be at lest somewhat likely; accustom participants to brainstorming process; extract "low-hanging friut" (i.e. pet scenarios) so that greater	Introduce session (5 mins)		Describes the types of COAs that qualify in the "likely" category (any COAs that participants perceive as having a greater than 1% probability of occurring by 2015). Outline the format of COAs (Who, Why, Where, When, How) and emphasize the particular importance of precursor activities in the COA structure. Refer participants to "pathway" handout.				

			creativity can follow.		[redacted]					
				Structured Brainstorming: including prompts (40 mins)	[redacted]	Ask participants to verbally provide one or more COAs according to a set of prompts. Allow open offers and discussion (but not debate on likelihood). Ensure less directly participative people are also queried. Prompts are based on effects, e.g. "give me a bioterrorism COA that would result in > 1 million fatalities" (see associated documentation for detailed list of prompts). Each COA is quickly and briefly described.	Supply COAs according to prompts. Also permitted to submit COAs electronically or to Instant Chat with any other member.	Captures each COA together with discussion and who suggested it.	Semi-structured Backup - captures each COA in Excel spreadsheet template, but concentrates on detail as opposed to identity of SME.	Two-liner summaries of COA inserted into ranking template. Hands off to Pam Toman on memory stick. Can begin COA mapping.
13:45 - 13:50		**Break**		Snacks available.	[redacted]			Catch-up	Printout COA spreadsheet.	Begins mapping COAs into database.
13:50 - 14:30	**2**	**Exploring "Likely" Scenarios , cont.**	See above.	Free-form Brainstorming (Rapid-fire: 2 liners only) (15 mins)	[redacted]	Participants are now requested to verbally supply brief titles and 1-sentence descriptions of any likely bioterrorist attacks not already mentioned. Make rounds of anyone who has not offered a COA.	Provide brief COAs. Also permitted to submit COAs electronically or to Instant Chat with any other member.	Capture COA titles and sources.	Captures COA titles and descriptions.	Continues to map COAs into database.

				Free-form brainstorming detail + additional COAs (20 mins)		Participants are asked to use their virtual whiteboard / wiki to a) supply some detail to all COAs they suggested in rapid-fire round (i.e. write full, 1-paragraph descriptions of each COA); b) supply interesting variants of any other COAs they have seen thus far; and c) provide any additional COAs they think are important and have been missed.	Participants, working independently, submit electronic versions of COAs, which are displayed on the Whiteboard. Encouraged to IC with any of the experts.	Places COAs into Word doc.	Collates COAs as they arrive into Excel spreadsheet.	Continues to map COAs into database.
14:30 - 14:35		**Break**	Snacks					Print out ranking document.	Pastes titles + descriptions into ranking template. Upload to Collaborative website.	Continues to map COAs into database.
14:35 - 15:00	**3**	**Scenario Ranking**	Obtain a ranking of top 20 COAs judgedto be most likely by the SMEs.	Introduce ranking instrument.		Participants are instructed as to how to downlaod and rank COAs.				Continues to map COAs into database.
				COA ranking.			Participants, working independently, rank COAs using the computer system. Can proceed directly to break once they have uploaded their rankings.	Begin merging rankings as they are completed.		Continues to map COAs into database.
15:00 - 15:15		**Break**		Snacks available.				Merging of rankings and statistical distribution generating.	Merging of rankings and statistical distribution generating.	Adding rankings to DB and sorting so as to display highest ranked COAs.

15:15 - 16:15	4	**Identification of Positive Indicators**	Identify indicators associated with precursor activities, esp. those that enable differential analysis. Minimum goal - provide indicators for Top 10 ranked COAs.	Discussion of ranked scenarios (15 mins)	[redacted]	Displays top-ranked COAs. Initiates open discussion regarding aggregated ranking. Should any COAs be added? Should any be moved up or down the list?	Providing comments on ranking. Encouraged to IC with any of the other participants.	Capturing discussion.	Capturing discussion.	
				Elicitation of positive indicators (45 mins)	[redacted]	Starting with the COA ranked most likely, participants are polled as to indicators related to precursor activities. Indicators should be a) observable and b) preferably enabling differential analysis. Ensure that all participants are engaged and remind them that additional indicators can be sent subsequently. Session goal is deriving indicators for AT LEAST top 10 ranked COAs, preferably top 20.	Supplying indicators for each COA. Encouraged to IC with any of the other participants.	Capturing indicators and discussion surrounding them.	Capturing indicators and discussion surrounding them.	Adding indicators in real-time to overhead display.
16:15 - 16:30		**Break**		Snacks available.	[redacted]					
16:30 - 17:00	4	**Identification of Positive Indicators, cont.**		Elicitation of positive indicators (30 mins)	[redacted]	See above.	See above.	See above.	See above.	See above.

17:00 - 18:00	**5**	**Identification of Negative Indicators**	Identify indicators that would invalidate the hypothesis that a particular COA is occuring.	Elicitation of negative indicators (60 mins).		Starting with the COA ranked most likely, participants are polled as to indicators that would signal that a particular COA is NOT in play. Ensure that all participants are engaged and remind them that additional indicators can be sent subsequently. Session goal is deriving indicators for AT LEAST top 10 ranked COAs, preferably top 20.	Supplying indicators for each COA. Encouraged to IC with any of the other participants.	Capturing indicators and discussion surrounding them.	Capturing indicators and discussion surrounding them.	Adding indicators in real-time to overhead display.
18:00 - 18:15	**6**	**Wrap-up Day 1**	Elicit initial feedback on day 1.	Wrap-up (15 mins)		Elicit initial feedback on day's activities; introduce following day's activities; provide dinner suggestions; remind of Day 2 start time.	Supply feedback	Record feedback.	Begin constructing cartesian map.	Begin constructing cartesian map.
18:15		**Adjourn**								
18:30 - 19:30		***Dinner Break***								
19:30 - 21:30		***Cartesian Map Construction (staff only)***	Map Day 1 scenarios to identify threat regions covered / neglected	Cartesian Space Construction (90 mins)			N/A	Constructing cartesian map.	Constructing cartesian map.	Constructing cartesian map.
				Cartesian Space Analysis (30 mins)		Analyzing cartesian map.	N/A			
Tues, August 12										
8:15 - 9:00		***Staff Arrival***	Preparations and make printouts of Cartesian Space.	(45 mins)		General preparations.	N/A	Preparations and make printouts of Cartesian Space.	Preparations and make printouts of Cartesian Space.	Preparations and make printouts of Cartesian Space.

8:30 - 9:00		**Arrival of Participants**		Simple breakfast is provided (Fruit + danishes / bagels + coffee / juice) (30 mins)	[redacted]					
9:00 - 9:30	**7**	**Day 1 Recap and Cartesian Space Review**	Collectively examine "gaps" as a means of priming for extreme COAs.	Introduce Cartesian Space (10 mins)	[redacted]	Introduces Cartesian Space and analysis as means of recapping Day 1. Emphasizes that group is now going to focus on "extreme" COAs, i.e. terrorist attacks with high consequences but which have <1% probability of occurring. Mention "Black Swans".		Distribute handouts.	Distribute handouts.	
				Discussion (20 mins)	[redacted]	Encourages open discussion regarding potential gaps.	Provide feedback. Encouraged to IC with any of the other participants.	Record discussion.	Record discussion.	
9:30 - 11:00	**8**	**Exploring Extreme Scenarios I: Future Backwards**	Use pattern disruption to elicit initial set of extreme COAs; emphasis on new technology.	Introduce Future Backwards and Supply sample and "Future Tech" powerpoint (10 mins).	[redacted]	Introduces the technique of future backwards and explains why it is useful.	Read sample	Present "Future Tech" Powerpoint.		

				Facilitated future backwards elicitation (25 mins).		Guides participants through construction of disruptive narrative of COA using sequence of questions (see associated documentation for details).	Each participant enters his COA into his computer. The form of these responses is irrelevant (for example, participants can jot down their thoughts as bullet points or keywords or just maintain them mentally), as long as the participants remember their responses. Participants are instructed to phrase their responses (either written or mental) as if they were at a future time, say 2016, writing or thinking in the past tense, as if they were describing a real event that happened in the past, although obviously their responses will be fabricated.			

				Future backwards presentations and discussion. (45 mins).		Each participant is then asked, in turn, to tell their story about what happened. Select the most talkative / "on-target" person to present first. The story must be told in the past tense (this is difficult!) and in reverse chronological order (i.e. more or less following its construction). Storytellers are urged to give as much DETAIL as possible when they recount the stories. Although participants can use their answers to the above questions as a guide, they are also free to “ad-lib” and alter their stories as they tell them. In fact, elaboration should be encouraged. AFTER each story, the other participants are allowed to ask the storyteller questions ABOUT THE STORY, such as details about how something was actually accomplished or more information about the perpetrators. They are not allowed to comment (either positively or negatively) on the merits of the story itself (after all, it is a story).	Discussion. The participants are asked to jot down any thoughts they have while other participants recount their stories, which they think would make their own story more INTERESTING (not necessarily more realistic or accurate).	Capture discussion.	Capture discussion.	
				Modification of COAs (10 mins)		Participants are instructed to now write down their stories in as much detail as possible, either forwards or in reverse (taking into account any additions they may want to make after listening to the other stories and answering questions about their own story)	Each particpant can individually modify his story, and submits electronically to WCs. Encouraged to IC with any of the other participants. Can go to break immediately upon completion.	Collate stories and add to Word doc.		Take stories and convert to COAs.

11:00 - 11:15		**Break**		Snacks available.	[redacted]					Take stories and convert to COAs.
11:15 - 12:30	**9**	**Exploring Extreme Scearios II: "Button Soup" Red-teaming**	Use red-teaming to generate extreme COAs; emphasis on improvisation and tactical innovation.	Group Assignment and Description (5 mins)	[redacted]	Participants are broken up into 3 groups, each with a facilitator. Facilitator hands out terrorist group profile (brief – newspaper article format) to each group, who read it.		Each WC assigned to a group to capture discussions.	Each WC assigned to a group to capture discussions.	Each WC assigned to a group to capture discussions.
				Instructions (5 mins)	[redacted]	Facilitator explains that this exercise gets us thinking about what can be done with scarce resources. Participants are instructed to devise a bioterrorism attack (one attack for the group, working as a team and IN ROLE). Explain that initially start out with no resources except: guns, Internet, X members and $Y (will vary by group). Also, high-consequence motive will vary by group (e.g. some to maximize casualties; others, disruption).				
				First Round (no resources) (20 mins)	[redacted]	Facilitator tracks the open discussions, trying to limit his or her role to scribe only, guiding participants only as necessary to ensure they stay realistic and stay in role. The attack should only be described in terms of its actions and consequences, not describing the response unless the response is part of the	Open discussion IN ROLE.	Capture discussion.	Capture discussion.	Capture discussion.

					[redacted]	attack strategy. As soon as one attack is devised, participants are instructed to plan a second attack.				
				Second Round (2 resources) (10 mins)	[redacted]	Whether or not participants succeed in this task, after 20 minutes the facilitator now asks the following question: if you could add any two other objects (and their associated skill-sets) to the existing set to increase the chances of success or the scope of the attack, what would this be? Discussion follows.	Open discussion IN ROLE.	Capture discussion.	Capture discussion.	Capture discussion.
				Third Round (4 resources) (10 mins)	[redacted]	This is procedure is repeated, except this time two further objects are added to the previous two.	Open discussion IN ROLE.	Capture discussion.	Capture discussion.	Capture discussion.
				Presentation and discussion (15 mins).	[redacted]	Participants are reconvened.	A representative from each group details their attack(s) IN ROLE. Participants discuss these and any variations OUT OF ROLE. Questions that could be asked include: is an attack with initial objects possible? To what extent do resources and technical capacity limit the scope of possible attacks?	Capture discussion.	Capture discussion.	Convert attacks to COAs and maps into DB.
				Additional COAs (10 mins.)	[redacted]	Partcipants are asked to (individually) add any new COAs through electronic system. Each participant encouraged to submit at least one.	Participants add new COAs and submit electronically.			Convert attacks to COAs and maps into DB.

12:30 - 13:15		**Lunch**			[redacted]			Download and add to word doc.	Download and add to excel spreadsheet.	Convert attacks to COAs and maps into DB.
13:15 - 13:45	**10**	**Clustering of Extreme Scenarios**	Elicit additional COAs; Derive representative set of approx. 10 extreme COAs through clustering.	Present accumulated COAs (5 mins).	[redacted]	Quickly run-through all extreme COAs produced thus far.				
				Elicit additional COAs (5 mins).	[redacted]	Request verbal or written additional COAs.	Discussion and optional submission of additional COAs.			
				Clustering (20 mins).	[redacted]	Leads participants in clustering exercise.	Discussion.	Capture discussion and clusters.	Capture discussion and seleted representative COAs.	
13:45 - 15:00	**11**	**Identification of Positive Indicators**	Identify indicators associated with precursor activities, esp. those that enable differential analysis. Minimum goal - provide indicators for 10 representative COAs.	Elicitation of positive indicators (75 mins)	[redacted]	Participants are polled as to indicators related to precursor activities. Indicators should be a) observable and b) preferably enabling differential analysis. Ensure that all participants are engaged and remind them that additional indicators can be sent subsequently. Session goal is deriving indicators for AT LEAST 10 repesentative extreme COAs, preferably all of them.	Supplying indicators for each COA. Encouraged to IC with any of the other participants.	Capturing indicators and discussion surrounding them.	Capturing indicators in detail.	Adding indicators in real-time to overhead display.
15:00 - 15:15		**Break**			[redacted]					
15:15 - 16:15	**12**	**Identification of Negative Indicators**	Identify indicators that would invalidate the hypothesis that a particular COA is	Elicitation of negative indicators (60 mins).	[redacted]	Participants are polled as to indicators that would signal that a particular COA is NOT in play. Ensure that all	Supplying indicators for each COA. Encouraged to IC with any of the other participants.	Capturing indicators and discussion surrounding them.	Capturing indicators in detail.	Adding indicators in real-time to overhead display.

			occuring.		participants are engaged and remind them that additional indicators can be sent subsequently. Session goal is deriving indicators for AT LEAST 10 representative COAs, preferably top 20.				
16:15 - 16:20		**Break**							
16:20 - 16:45	**13**	**Last Call and Participant Feedback**	Elicit further COAs and preliminary workshop feedback.	Last call for COAs	Invite participants to provide any last substantive ideas or thoughts before conference close.	Supply additional ideas in open forum.	Capture ideas and add to existing COAs.	Capture ideas and add to existing COAs in spreadsheet.	Map any additional COAs to database.
				Participant feedback.	Engage in informal discussion about the format and utility of the workshop.	Provide feedback on their perceptions of the workshop.	Capture discussion.	Capture discussion.	
16:45 - 17:00	**14**	**Workshop Wrap-up**	Maintain momentum post-conference.	Thank participants and explain next steps.					
17:00		**Close**							

D. Adversary Course of Action Variables

The ACOA variables coded into the database include:

- ID
- Perp Name
- Perp Category
- Motive
- Intended Effects
- Cause high-social disruption?
- Cause high-economic disruption?
- Cause high-political instability?
- Cause high-mass casualties?
- Target Category
- Exact target
- Indiscriminate?
- Type Bioagent Used
- Specific Agent Used
- Mode of Acquisition
- Cost of Acquisition (USD)
- Acquisition Duration (Months)
- Location of Acquisition
- Acquisition Type
- Bioagent Enhancement Characteristics
- Enhanced Survivability?
- Enhanced Lethality?
- Enhanced Infectiousness?
- Decreased Immunology?
- Production Details
- Technicians
- Number of Technicians
- Equipment
- Cost of Production (USD)
- Production Duration (Months)
- Location of Production
- Weaponization Details
- Cost of Weaponization (USD)
- Weaponization Duration (Months)
- Location of Weaponization
- Testing
- Test Details (if applicable)
- Delivery Method Details
- Intl Borders
- Border Crossing Details
- Delivery Method
- Delivery Vehicle
- Ranking
- Indicator Perp
- Indicator Agent
- Indicator Target
- Indicator Acquisition
- Indicator Production
- Indicator Weaponization
- Indicator Deployment
- ACOA Narrative

E. Bio-terrorism and Violent Non-State Actors

The Bio-terrorism violent non-state actors (VNSA) study was conducted by Drs. Victor Asal and Karl Rethelmeyer, both from the Rockefellar School of Public Affairs, State University of New York, Albany, and both recognized experts on terrorism.

The basic aim of this study was to identify the factors statistically associated with increased likelihood of a Violent Non-State Actor (VNSA) engaging in the use of biological agents for terrorism. The researchers conducted a "Hoax no hoax" analysis, to examine incidents and identify which incidents are likely to be "real" with real defined as efforts that go beyond hoaxes, plots, attempted acquisition and threats. Many hoaxes are done by lone individuals, so the researchers focused on incidents with actual possession of agents, or more attempts to use agents (possession plus).

The researchers compiled data on 395 terrorist organizations and coded organizational variables for the period 1998-2005. The data was compiled from the Monterey WMD Terrorism Database, Monterey Institute for International Studies, and the Tactical Terrorism Dataset, compiled by the Institute for the Study of Violent Groups (ISVG) at Sam Huston State University. The data was ultimately compiled into SUNY's Big, Allied and Deadly terror group data set.

The method of analysis used was multiple logistical regression, in which the logits, or the log of the odds ration (log (Probability Event / 1- Probability of Event)) of the dependent variable is predicted (Hanushek & Jackson, 1977). Logits are distributed linearly and therefore can be used in linear models. Once estimated, logits are easily transformed into predicted probabilities that the dependent variable would occur.

The study reached several conclusions, which are listed below:

1. Bioterrorism is a rare event. Only 2% of VNSA groups ever engaged in plotting and attempting it, and less than 0.5% ever gained possession of biological agents and/or attempted to use them.

2. Bacteriological agents are the most common bio agents sought, possessed or used by terrorist groups, but because of their involvement in hoaxes, they had a negative correlation with actual possession or use.

3. The majority of hoaxes are perpetrated by lone actors, and the majority of actual possession or attacks are perpetrated by religious cults, but not by fundamentalist religious organizations.

4. Religious groups and nationalist/separatist groups were the most likely to possess, plot and/or use biological agents than other groups.

5. Salmonella is the agent most often involved in actual plots.

6. A group's connectedness to other groups, its previous use of suicide attacks, high kill ratio, and weapons smuggling were statistically associated with a group's probability of actually plotting a bio-terror attack.

7. Even though suicide attacks and weapons smuggling were statistically related to bio-terror, they had a negligible influence on the probability that a group would carry out a bio terror attack within their range of values.

8. Groups with a history of high lethality and high connectedness to other groups were most likely to be involved in actual bio terror plots.

9. Groups that had a combination of suicide attack and weapons smuggling increased their probability of plotting an actual bio attack by 0.06%.

10. Fingerprinting exercise netted groups known to have engaged in bio agent possession plotting or use (7 groups), but also netted 3 (30% of groups) false positives in the top 10 groups predicted to be involved in bio terrorism.

11. Those groups predicted and known (open source) to have been engaged in nuclear smuggling include:
    - Jemaah Islamiya
    - Al Qaeda
    - PKK
    - Chechens
    - Hamas
    - Armed Islamic Group
    - Al Aqsa Martyrs Brigade

Dr. Victor Asal
Dr. Karl Rethelmeyer
Rockefellar School of Public Affairs
State University of New York, Albany

F. Automated Behavior Analysis Subject Matter Expert (ABA/SME) Application for Evaluating the Probability of Biological Attack Threat

Automated behavior analysis is the automation and extension of applied behavior analysis, a field in psychology. Applied behavior analysis stresses that behavior does not occur in a vacuum or occur spontaneously. Instead, behavior occurs in response to environmental precursors (antecedents) and is maintained by following events (consequences). ABA has been developed to automate the clinical applied behavior analysis process used to analyze target behaviors of individuals with problems for the purpose of altering behavior for the better. Although applied behavior analysis is used universally, it had to be extended to include prediction and automated to be useful in today's information-rich world. ABA is the only automated version of applied behavior analysis to date. To be predictive, ABA requires multiple examples of behavior and associated contexts to provide the antecedent-behavior-consequence sequences necessary for advanced pattern classification. However, in some situations, sufficient examples are not available. When data are sparse a hybrid ABA subject matter expert (ABA/SME) application has been developed and applied successfully. That is, if only a few examples of the behavioral phenomenon are available, then subject matter expertise must be added to augment the small number of cases. The developed ABA/SME methodology has proven to be successful and is different from expert rule-based applications.

Typical artificial intelligence (AI) knowledge capture applications are variants of an approach that begins with extensive interviews of experts and ends with the reduction of such knowledge to rules that specify "if-then" rules. Although proven to be useful in a variety of applications, typical rule-based applications may be brittle. That is, they can faithfully exhibit fairly straightforward decisions based on multiple if-then conditions, but are not capable of providing accurate decisions or outcomes when presented with unique combinations of input variables. ABA/SME was designed to replace the rule-based engine with the well-tested ABA pattern classification methodology using ABA tools. The advantage of this approach has been that the ABA/SME applications developed for specific domains are capable of providing specific decisions and projections when presented with clear input variables like any typical knowledge based application but can also provided "educated guesses" when presented with unique combinations of input variable not present previously. In other words, the ABA/SME methodology has been useful in identifying unique adversary attacks with no previous signatures, particularly within the domain of computer network intrusion.

Although the domain of biological agent attack is different than computer network intrusion, the basic principles are identical. That is, there are few examples of unique attacks, little useful data supporting the analysis of new signatures, and subject matter expertise is necessary to fill the significant "holes" in available data. The application described here was based on the methodology used to develop the predictive engine underlying the commercial off the shelf (COTS) Checkmate Intrusion Protection System (Checkmate^{TM}). This application has been independently validated to identify first time network attacks and was based on the development of knowledge using subject matter expertise, as opposed to past attack data.

F.1. ABA/SME Methdology for Biological Threat

Figure F-1 depicts the ABA/SME process used for this project. As a stage one application, ABA staff attended the New Horizons academic SME session to understand the bio threat scenario generation process. Using the New Horizons report, all scenarios with associated indicators were extracted and indicator duplicates were excluded. Following indicator extraction, a typical ABA data array was developed. This array was formatted to fit the requirements of ABA pattern classification. As part of the ABA methodology it has been determined that accurate prediction/forecasting must include examples of behavior and antecedent combinations not associated with attack. For this reason, "nons" were added and comprised of alternate versions of the provided attack scenarios. Once completed, the data array was then presented to the ABA pattern classification methodology to develop weights. The gradient decent pattern classification process returned likelihood, type of agent, and perpetrator type when the application was presented with indicators associated with a given scenario. This recall was 100% accurate. To test the capability of the application to generate outcomes with alternate combinations of indicators, indicators associated with the past TTX exercise were presented to the application. This test projected a low likelihood event with a viral agent and a religious perpetrator. Other combinations were presented to test for authenticity.

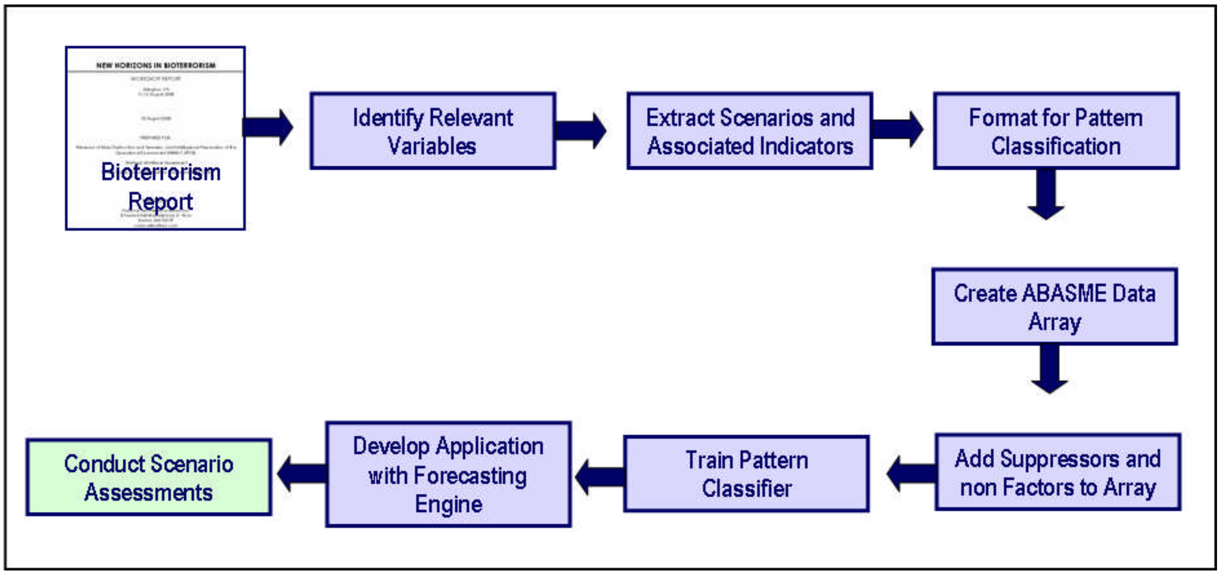
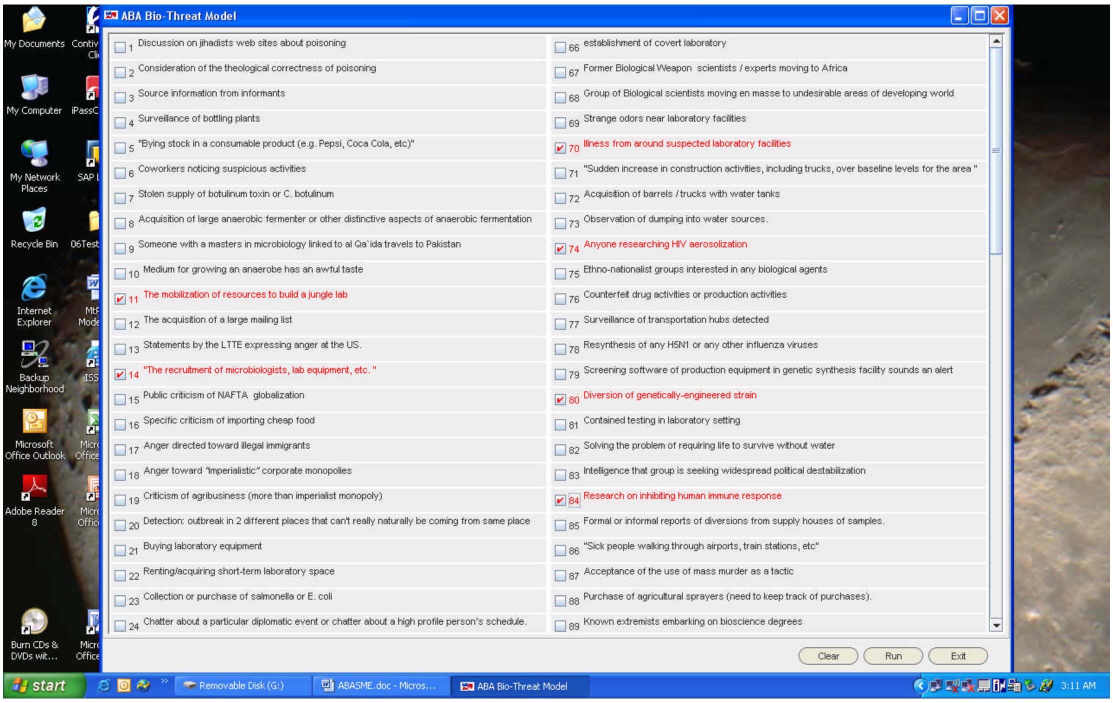

NEW HORIZONS IN BIOTERRORISM
Bioterrorism Report
Identify Relevant Variables
Extract Scenarios and Associated Indicators
Format for Pattern Classification
Create ABASME Data Array
Add Suppressors and non Factors to Array
Train Pattern Classifier
Develop Application with Forecasting Engine
Conduct Scenario Assessments

Figure F-1. The ABA/SME process as applied to biological threat.

Once all testing was completed, the ABA application was developed in C++ and JAVA code. The ABA/SME application consists of an input screen with all indicators presented with checkboxes. To operate the application, one checks the boxes of the indicators of a new scenario to test. By clicking on "run" the constellation of indicators are presented to the trained pattern classifier and likelihood of event, perpetrator type, and biological agent type is immediately returned. These outcomes are the "most likely" outcomes given the constellation of indicators presented. Results can be saved or printed.

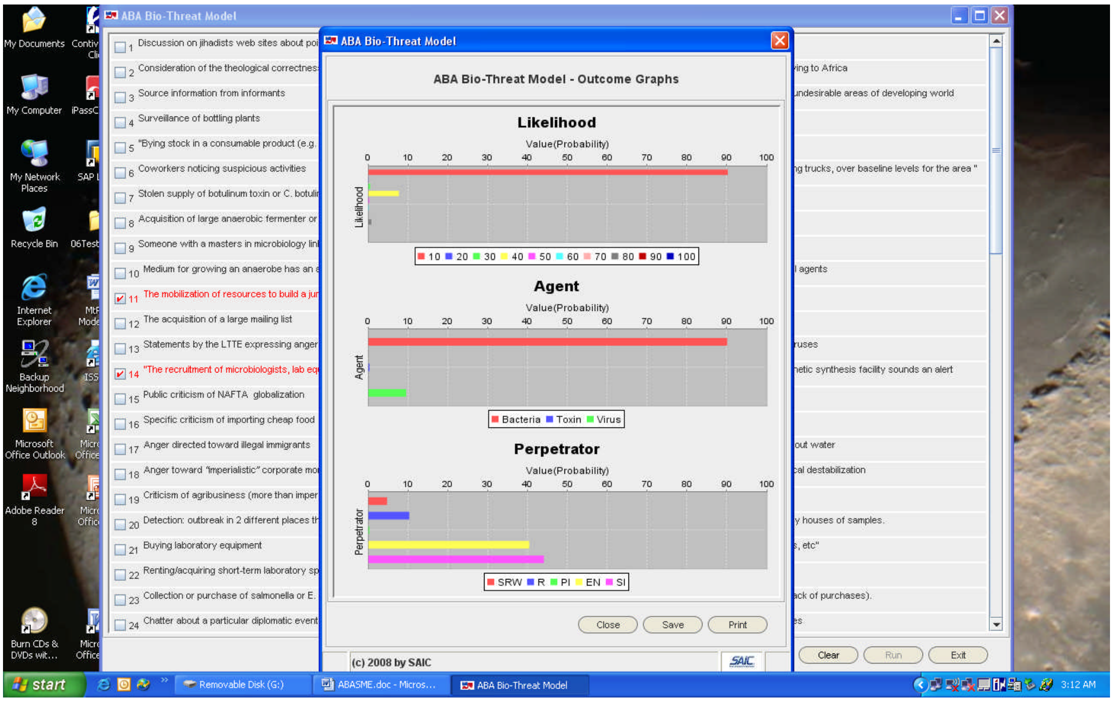
Figure F-2 shows a screen shot of the input screen and Figure F-3 show a screen shot of the results.


ABA Bio-Threat Model

☐ 1 Discussion on jihadists web sites about poisoning
☐ 2 Consideration of the theological correctness of poisoning
☐ 3 Source information from informants
☐ 4 Surveillance of bottling plants
☐ 5 "Bying stock in a consumable product (e.g. Pepsi, Coca Cola, etc)"
☐ 6 Coworkers noticing suspicious activities
☐ 7 Stolen supply of botulinum toxin or C. botulinum
☐ 8 Acquisition of large anaerobic fermenter or other distinctive aspects of anaerobic fermentation
☐ 9 Someone with a masters in microbiology linked to al Qa`ida travels to Pakistan
☐ 10 Medium for growing an anaerobe has an awful taste
☑ 11 The mobilization of resources to build a jungle lab
☐ 12 The acquisition of a large mailing list
☐ 13 Statements by the LTTE expressing anger at the US.
☑ 14 "The recruitment of microbiologists, lab equipment, etc. "
☐ 15 Public criticism of NAFTA globalization
☐ 16 Specific criticism of importing cheap food
☐ 17 Anger directed toward illegal immigrants
☐ 18 Anger toward "imperialistic" corporate monopolies
☐ 19 Criticism of agribusiness (more than imperialist monopoly)
☐ 20 Detection: outbreak in 2 different places that can't really naturally be coming from same place
☐ 21 Buying laboratory equipment
☐ 22 Renting/acquiring short-term laboratory space
☐ 23 Collection or purchase of salmonella or E. coli
☐ 24 Chatter about a particular diplomatic event or chatter about a high profile person's schedule.

☐ 66 establishment of covert laboratory
☐ 67 Former Biological Weapon scientists / experts moving to Africa
☐ 68 Group of Biological scientists moving en masse to undesirable areas of developing world
☐ 69 Strange odors near laboratory facilities
☑ 70 Illness from around suspected laboratory facilities
☐ 71 "Sudden increase in construction activities, including trucks, over baseline levels for the area "
☐ 72 Acquisition of barrels / trucks with water tanks
☐ 73 Observation of dumping into water sources.
☑ 74 Anyone researching HIV aerosolization
☐ 75 Ethno-nationalist groups interested in any biological agents
☐ 76 Counterfeit drug activities or production activities
☐ 77 Surveillance of transportation hubs detected
☐ 78 Resynthesis of any H5N1 or any other influenza viruses
☐ 79 Screening software of production equipment in genetic synthesis facility sounds an alert
☑ 80 Diversion of genetically-engineered strain
☐ 81 Contained testing in laboratory setting
☐ 82 Solving the problem of requiring life to survive without water
☐ 83 Intelligence that group is seeking widespread political destabilization
☑ 84 Research on inhibiting human immune response
☐ 85 Formal or informal reports of diversions from supply houses of samples.
☐ 86 "Sick people walking through airports, train stations, etc"
☐ 87 Acceptance of the use of mass murder as a tactic
☐ 88 Purchase of agricultural sprayers (need to keep track of purchases).
☐ 89 Known extremists embarking on bioscience degrees

Figure F-2. A portion of the scrollable indicator input screen when the ABA/SME application is called on a laptop.


ABA Bio-Threat Model

ABA Bio-Threat Model - Outcome Graphs

Figure F-3. The outcome screen generated by the pattern classifier assessment engine. Indicators presented result in projections of event likelihood, perpetrator type and biological agent type.

F.2. Next Steps

The ABA/SME application is complete as a functional design for academic SME input. The next steps will include expansion using classified scenarios and indicators and extensions in outcome generation.

Gary M. Jackson, PhD (Chief Scientist/Engineering Manager)
Sara Olsen, MA (Intelligence Analyst)
Reconnaissance and Surveillance Operation, SAIC

G. Using Bayesian Networks for Evaluating Relative Risk of Biological Terrorist Attacks

This document provides a high-level summary of how relative risk analyses are performed in support of ranking biological threat scenarios. Pacific Northwest National Laboratory's (PNNL) contributions are focused on prioritizing bioterrorism threats to the United States (U.S.) or U.S. Forces through 2015 using Bayesian networks (Bayes Net). Bayes Nets are directed acyclic graphs that represent the probabilistic relationships between nodes in a graph. The New Horizon's team identified indicators of early threatening behavior (precursors). The Bayes Net integrates the indicators into an analysis framework, to enable moving bioterrorism threat detection far left of boom. In support of these goals, PNNL modified a general threat Bayes Net for data integration to allow for estimation of relative risk of bioterrorism scenarios, as developed and provided by the New Horizon team, under JIPOE auspices. The intended outcome of the PNNL efforts is to identify and demonstrate the process, methods, and potential information sources necessary to provide relative risk estimates for bioterrorism events.

Approach:

For this work, PNNL is estimating risk, a function of likelihood and consequence. Scenario likelihood and the scenario consequences are multiplied to calculate risk. Scenario consequence has three components: 1) measure of human harm in terms of causalities or mortality, 2) the economic cost, and 3) the sociological / psychological consequences from implementation of the scenario.

Relative risk assessments include probability or likelihood estimates associated with each scenario, as well as estimation of the consequences from implementing a given scenario. Each scenario has elements of who, what, where, why, when, and how. When appropriate, scenario elements can be summarized into scenario classes, based on bioterrorism material type, target/target-type, and groups/group-type. In a Bayes Net, each node is a variable, and the linkages between nodes represent conditional relationships. Nodes are evaluated based on knowledge and evidence about the node, and the model's output provides information about the likelihood distribution.

G.1. Methodology and Implementation

PNNL first constructed a model that incorporated the following components and represents threats at a very high level: 1) intent and environmental, 2) capability, and 3) target. The model is broad scale and computes relative risk across scenarios based on currently available information. Technical aspects of the example model are represented in capability related notes and in the consequence components of the models. Social aspects are captured in the Motivation and Intent and Target Selection nodes.

The Figure 1 model constituents include:

- *Violent Scenario Likelihood*: This component represents the probability of a specific scenario, conditionally based on intent, the target accomplishing the intent goal, and the capability to accomplish the goal.
- *Motivation and Intent*: The degree to which an organization or individual is motivated to execute biological terrorism, including contextual as well as intrinsic information.
- *Target fits Group Goals*: This component considers, for example, whether the successful execution of a scenario against a specific target advances the group's agenda and is consistent with group ethics.
- *Target Select*: The perception of vulnerability associated with a potential target and whether it's a factor in the threat, as (presumably) an attack would be made only if success against the selected target was possible.
- *Perception of Vulnerability:* This component considers whether the group believes they can gain access to the target.
- *S&E Knowledge:* The group's access to the fundamental technical knowledge to execute a specific threat scenario. This could be decomposed into various compartments related to understanding, constructing, and delivering devices, sufficient to carry out the threat.
- *Capability for Scenario*: Whether the group has the capability to execute the threat, based on the contributions of contributing indicators.
- *Success of Scenario*: The likelihood of success, given threat and opportunity, and measures the extent to which the group objectives are achieved.
- *Target Opportunity:* This component examines the opportunity for the attack to take place against the target, dependent on target vulnerabilities and security posture.
- *Equipment:* The gear necessary to handle, process, and weaponize the material (for example, beakers, test tubes, personal protective equipment, etc.).
- *Operational*: Planners (thought / group leadership) and resources (people, money) required for executing an attack scenario.
- *Material*: The raw materials that contribute to the terrorist attack tool. For a bio-threat, this could be anthrax spores, or E. coli samples, or hoof and mouth slurry. For an IED, it would include the trigger and explosive. For a chemical threat, it could be the chemical, or a set of precursor chemicals

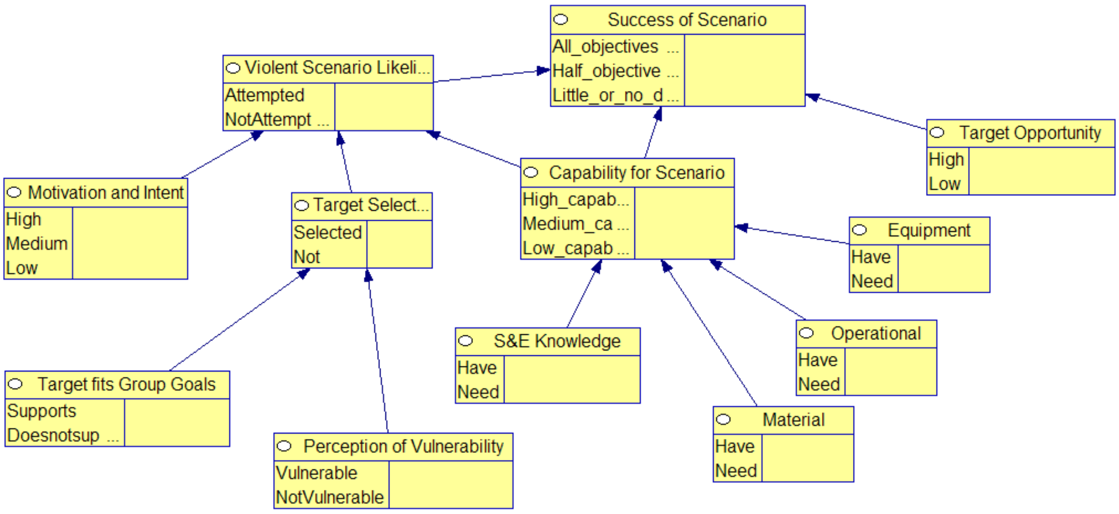


Figure 6: Threat Model Represented as a Bayes Network.

Model use is accomplished by inputting the probabilities for nodes that are ‘leaves’ of the network – a probabilistic calculation then propagates the values throughout the model’s network. Based on assessments, the motivation and intent for a group in a given scenario is placed into the Motivation and Intent node, the degree to which a Target fits Group Goals is placed into that node, and so on. These assignments result in likelihood and risk calculation.

G.2. Summary and Limitations

A methodology for relative risk assessment based on a high-level model was described and depicted. The generic model is consistent with anticipated behaviors and the open technical literature, and motivation and intent is a significant driver. However, this generic high level model is not calibrated against empirical observations – so, while useful for relative assessments, the probabilities should not be interpreted as forecast frequencies.

G.3. References

Paté-Cornell, M.E. and S.D. Guikema. “Probabilistic Modeling of Terrorist Threats: a Systems Analysis Approach to Setting Priorities Among Countermeasures,” Military Operations Research, Vol. 7, No 4, December 2002

Post, Jerrold, Keven Ruby, and Eric Shaw. The Radical Group in Context: 1. An Integrated Framework for the Analysis of Group Risk for Terrorism. Studies in Conflict & Terrorism. 2002; 25(2):73-100

Paul Whitney, Ph.D.
Sandy Thompson, Ph.D.
Pacific Northwest National Laboratory