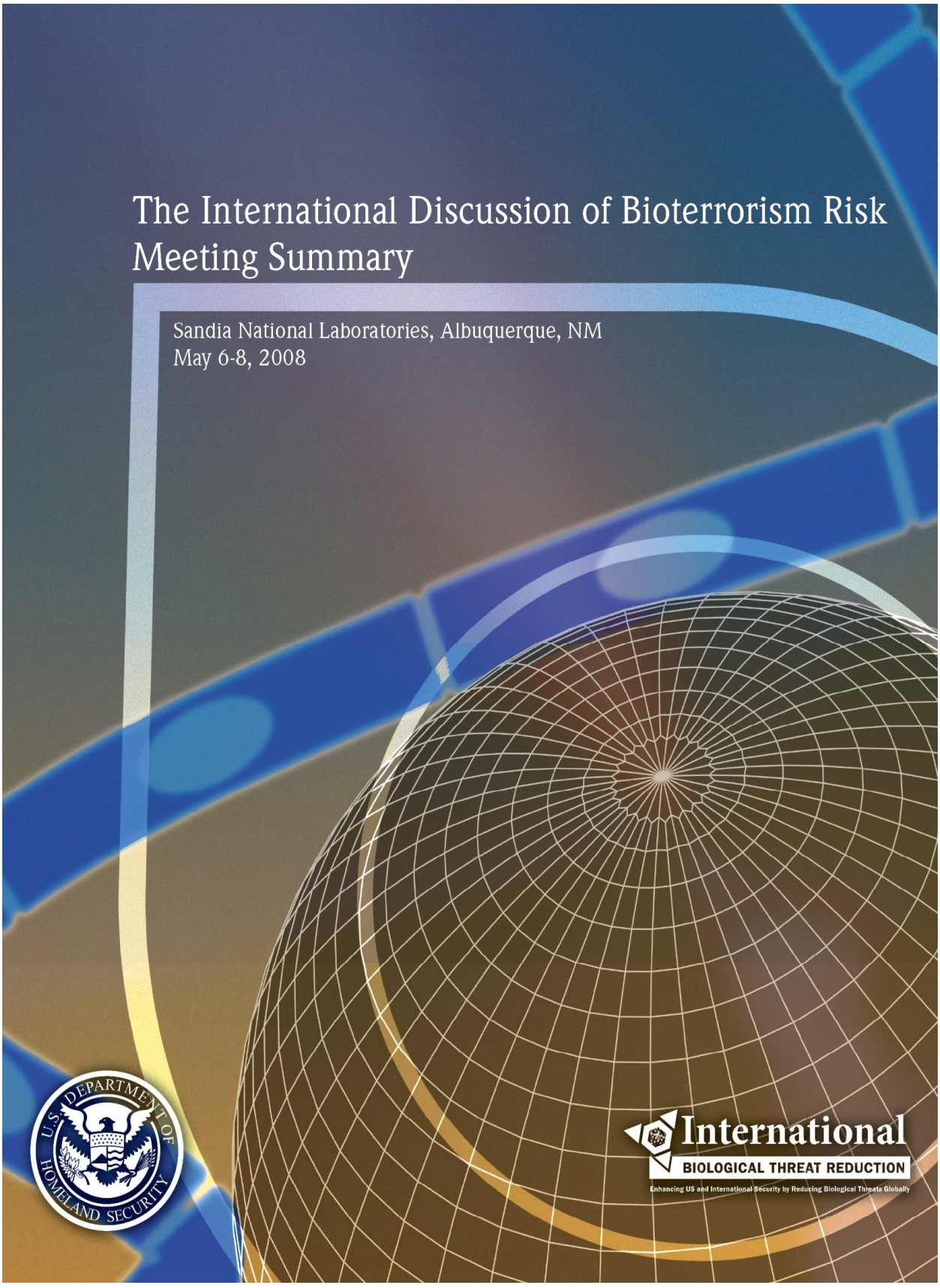
SAND2008-5858P

The International Discussion of Bioterrorism Risk Meeting Summary

Sandia National Laboratories, Albuquerque, NM
May 6-8, 2008



Prepared by International Biological Threat Reduction program of Sandia National Laboratories.

SAND No. 2008-XXXX
Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

TABLE OF CONTENTS

Executive Summary

DHS International Discussion of Bioterrorism Risk symposium

On behalf of the United States Department of Homeland Security (DHS), the International Biological Threat Reduction (IBTR) team at Sandia National Laboratories (SNL) hosted the **International Discussion of Bioterrorism Risk** symposium in Albuquerque, New Mexico on May 6-8, 2008. The primary purpose of the symposium was to share national risk assessments and exchange ideas and information regarding threats from biological agents and bioterrorism. This unclassified symposium gathered 29 subject matter experts with extensive experience in bioscience, biotechnology, public health, security, intelligence, and risk analysis. Representatives from eight countries were in attendance. Participant countries included Australia, Canada, Denmark, France, Japan, Sweden, the United Kingdom, and the United States.

International Observations and Key Issues

Representatives from each country provided an overview of national efforts in the areas of bioterrorism risk assessment methodologies and preparedness. Participant presentations revealed different perceptions of terrorist threat within the countries. Bioterrorism risk, as well as other types of terrorist threats, has varying levels of importance relative to other national priorities. Commonly cited reasons include variable perceptions of national terrorist threat by different nations. Other countries struggle to balance terrorist concerns with more immediate public concerns, such as catastrophic natural disasters and other non-intentional risks. Others have diverse perspectives regarding the ease or appropriateness of combining the threats into all-hazard approaches. Lastly, funding mechanisms are also often unreliable and erratic, directly affecting national capacities to approach and respond to these threats.

There were many commonalities in the risk assessment methodologies, yet there were also many differences. All of the participant countries initiated execution of their assessments by constructing and discussing a variety of scenarios; however, there were many differences in how the scenarios were enumerated. Some used only a "worst case" scenario; others used "worst case" with some level of plausibility required. Others used a full range of possible scenarios.

Generally, participants presented a consistent definition of risk. Some definitions used Likelihood x Consequences; other definitions used Threat x Vulnerability x Consequences. Most risk assessment methodologies used a multi-criteria decision analysis (MCDA) approach. The Likelihood/Consequence Scoring systems ranged from "1 to 5", "Negligible to Extreme", or "-3 to +3". Criteria weights generally were not discussed much, but many approaches included weighted criteria. In general, the Probabilistic Risk Assessment (PRA) approach was not frequently used and discussed by only a few participating nations.

Most participants felt more comfortable addressing the "consequence" side of the risk equation rather than the "likelihood" side. Many approaches modeled 'quantitative' consequences, such as number of fatalities, illnesses, and economic impacts. Participants had divergent opinions and approaches on how to model the 'qualitative' consequences including social disruption, outrage, or anxiety. Participants were also uncomfortable quantifying likelihood or probability. Many identified this area as the hardest part of the risk assessment process; Subject Matter Experts in the intelligence communities were often solicited for help in this area.

Lastly, participants reported many similarities and differences in decision-making environments with respect to how risk assessments are received, interpreted, and used. Government support for risk assessment efforts is often inconsistent; consequently, there are varying levels of willingness by decision makers to use the assessment results. In addition, nearly all participants report challenges in defining, capturing, representing, and communicating uncertainty in the risk assessment process. This limitation has also had a significant impact on decision makers and policy.

Conclusions

The **DHS International Discussion of Bioterrorism Risk** symposium presented a unique opportunity to learn about risk assessment methodologies and bioterrorism concerns around the world. Results of this symposium revealed a range of similarities and differences in methodologies, national strategies, funding, opinions, and ideas. More importantly, this symposium also revealed a strong and unified commitment within the international community to mitigate the threat of terrorism. The symposium concluded with a unanimous desire to meet again and collaboratively work together to assist in effective future counterterrorism policy.

Document Overview

This report provides an overview of the presentations, discussions, and opinions shared at the **DHS International Discussion of Bioterrorism Risk** symposium held in Albuquerque, New Mexico on 6-8 May 2008. A list of the 29 participants is presented in Appendix A. The primary objective of the meeting was to share national bioterrorism risk assessment methodologies and identify current international challenges. Information was shared using presentations and guided roundtable discussions. The report is organized into two major topic areas. These sections do not necessarily reflect the order of discussion during the symposium; a copy of the three day symposium agenda is presented in Appendix B. Furthermore, the information presented in this document is not verbatim, but rather a highlight of significant themes and topics addressed during the symposium's presentations and guided discussions.

Section I presents a broad summary of each presentation. The eight international presentations on risk assessment methodologies are listed first and are arranged alphabetically. The last three presentations include overviews of the US Department of Homeland Security Chemical and Biological Division, the Office of Health Affairs countermeasure strategies, and an overview of security risk assessment methodologies. Section II summarizes the symposium roundtable discussions. All roundtable discussions were non-attribution to promote an open exchange of information and ideas; therefore, identifying individual comments were not captured in this summary. The final roundtable addressed future directions, next steps, and proposals for similar international meetings.

Section I: Presentations

Participant Presentations

AUSTRALIA

Title: Australia's national approach to assessing and managing CBRN security risk
Presenter: Andrew Matz

Since 9/11, Australia decided to take a national approach to security. This interest was also due to a series of terrorist events that occurred within its own region, including the Bali attacks in 2002 and 2005 and the Jakarta attacks in 2003 and 2004. A number of national efforts were taken to build counter-terrorism policy such as the establishment of the Council of Australian Governments (COAG), and the National Counter-Terrorism Committee (NCTC), including the NCTC CBRN Security Sub-Committee (SSC).

Mr. Matz first presented the results of the COAG "Review of Hazardous Materials – Chemicals Report", published in December 2002. Its purpose was to review the regulation, reporting, and security around the storage, sale and handling of hazardous materials. The review process included the following steps 1) Identification of potential chemicals of concern 2) Examination of current control arrangements for chemicals in Australia 3) Review of international efforts 4) Development of a discussion paper 5) Design a chemical security framework 6) Draft a report and consultation and 7) COAG consideration. Australia used a technical working group to identify 2000 chemical agents of concern. Later, it was reduced to 95 chemicals they believed were the most dangerous. Ammonium nitrate the first chemical reviewed and it has been strictly regulated; is now banned as a fertilizer in Australia. The group also spent an extensive amount of time determining which regulations would have a security impact as well. Australian policymakers looked overseas to see what others were doing in these areas. In 2005, a Discussion paper was published and in January 2008, a Draft report was published.

Australia's Chemical Security Management Framework assesses the risks associated with chemicals. This group works with states and territories to implement controls to mitigate these risks. The Commonwealth Government, in collaboration with State and Territory Governments and industry, conduct the risk assessments. Australia looks to the AS/NZS 4360:2004 Risk Management Standard which defines risk as a product of Likelihood (or threat) and Consequences.

Matz commented that threat is a black box for Australians. They do not capture uncertainty as do the American methodologies. Threat assessments are usually undertaken by their national security intelligence. Threat is considered a product of intent and capability. Australia measures threat on a wide scale ranging from "extreme", "high", "medium", "low", "very low" to "negligible". In addition, Australia has identified nine broad scenarios they think are realistic in terms of how chemicals could be used by terrorists in Australia. In addition, Australia considers several factors which may

contribute to the degree of consequences suffered. These factors can be used to determine a qualitative consequence rating. Examples of consequences types considered include injury or loss of life, infrastructure damage, evacuations/displaced people, contamination, and economic impact. Consequence also considers duration, or how long it takes to get back to normal. Using threat and consequence, risk is calculated and plotted. Depending on the level of risk, varying levels of actions would be required. There are three risk level descriptors: Very Low, Moderate, and Extreme.

The National CBRN Security Subcommittee (SSC) has several primary functions: 1) consider implications for CBRN security policy and capabilities, 2) provide national policy coordination, 3) advise the NCTC, 4) oversee the implementation of the National CBRN Security Strategy, and 5) oversee the implementation of COAG Review of Hazardous Chemicals. Membership of this group consists of the Department of the Prime Minister and Cabinet, State and Territory Representatives, and various agencies within the Australian Government.

In November 2007, the CBRN SSC agreed to prepare a Risk Environment Statement. Its purpose was to make judgments about the relative risk of attack involving specific CBRN materials and to assist the NCTC to prioritize its resources accordingly. This was a significant step, marking the first time a risk-based approach had been taken to national security policy. This Risk Environment Statement was based on a national risk standard, the AS/NZ4360:2004 and the supplementary security risk standard. Items considered included threat inputs on CBRN issues, potential consequences of CBRN incidents, and potential vulnerabilities in the supply chain of CBRN materials.

This statement estimated and ranked CBRN outcomes and trends in 2004, 2007, and 2010. For 2010, the relative risks in descending order were: HME precursors, toxic industrial chemicals, incendiaries, biological and radiological materials, and lastly, nuclear materials. Generally, Australia views the risk associated with the terrorist use of nuclear material as very low; but HME precursors have a high and continual threat. The working group believes it is important to consider all CBRN materials but realize that all cannot be considered equally. Matz concluded that the working group had a good in-depth discussion on consequences but found it difficult to discuss threat.

The NCTC considered the Risk Environment Paper at its meeting March 25, 2008. They agreed to the judgments in the paper and plan to distribute the paper to the CBRN SSC and other sub-committees. Mr. Matz concluded that NCTC hopes to perform similar Risk Environment Statements annually.

CANADA

Title: Canada – National Presentation
Presenters: Team Canada represented by Alain Goudreau, Shane Roberts, Maureen Ellis, Harry Gardiner, Stephen Norman, and Joan Armour

Team Canada began the presentation with an overall review of Defence R&D Canada's (DRDC) Center for Security Science (CSS). Since 2001, there have been significant national investments to provide science and technology services to address national public safety and security. The CSS, a joint endeavor between DRDC and Public Safety Canada, was created to strengthen Canada's preparedness for, prevention of, and response to potential threats. Some of the current priorities of the CSS include the Consolidated Risk Assessment (CRA) and capability-planning processes. Specifically CSS is interested in promoting a better understanding of risk, learning risk methodologies, simplifying risk's approach, and disseminating the information.

There are four major programs within the CSS:
1) Chemical, Biological, Radiological-Nuclear, and Explosives (CBRNE) Research and Technology Initiative (CRTI)
2) DRDC Counter-Terrorism Technology Center (CTTC)
3) Public Security Technical Program Secretariat (PSTP)
4) Canadian Police Research Center (CPRC).

The CRTI is the most heavily funded of all the programs. The 2001 the budget was $175 million which was renewed again in 2006. In addition to these areas, the CSS also supports forensics, risk perception, and risk awareness.

The CRTI and the PSTP support a framework for the management of Canada's public security and S&T activities which focus on four mission areas: 1) Defeat the CBRNE Threat by developing capabilities to prevent, prepare and respond; 2) Critical Infrastructure Protection (CIP) which assesses and reduces critical vulnerabilities' 3) Surveillance, Intelligence, and Interdiction (SI2) to identify and stop terrorists or criminals; and 4) Emergency Management Systems Integration (EMSI).

The CSS Risk Portfolio has eight major priority demands. Some of these demands include risk assessment production; promotion of risk and capability-based planning; intelligence analysis and support; provision of support tools; and providing advice on risk, threat, vulnerability, and international initiatives. CSS has looked into fuzzy logic to perform its risk assessment. They also looked at Proteus for security issues. One of the biggest limitations CSS faces is the lack of support and funding. This department has much work to do nationally and it is severely understaffed.

Team Canada next described three major CSS initiatives sponsored by the CSS Risk Portfolio. The first initiative described was the Public Security Capability-Based Investment Model. Its objective is to implement a capability based investment model and associated tools to better inform public security science and technology and other capability related investments. The second CSS Initiative described is the CBRNE

Consolidated Risk Assessment (CRA). The objective of this initiative is to improve the CRA process and implement a similar process in other public security domains. This initiative has three fundamental pieces. The first is Threat Scenario Identification. The second is Vulnerability Determination and the last is Intelligence Judgment which together produces an overall Risk Prioritization rating. To do the CRA, CSS brings together approximately 70 experts and scientists into a room. Their methodology is not based on a ranking system; rather the scenarios are rated. However, after hearing Dr. Bennett's presentation, they are also interested in exploring applications of PRA.

The last CSS initiative is the All-Hazards Risk Assessment (AHRA) Study. Its objective is to demonstrate a harmonized framework for AHRA across the malicious and non-malicious domains. This initiative tried to map all-hazards risk events. They looked at AHRA from many different angles, and tried to be consistent in its approach. The risks were all described differently; however in the end they believe it is simply all the same. They also tried to define threats, vulnerability and consequences in a Risk Taxonomy. Finally, the AHRA published a lexicon.

Team Canada next presented Public Safety Canada: Risk Assessment as a Tool in Emergency Preparedness. This department is concerned with large scale national security and emergency management. For biological threats, this department works with federal and provincial departments and the private sector. In the event of a crisis, the individual provinces, which have a significant amount of power, first notify the local first responders. Then it goes up the chain. One of the most significant problems they face is the resistance of some locals to turn the problem over to the federal government.

Public Safety Canada is very interested in exploring and assessing risks and threats over a long period of time. They are interested in considering concepts of "risk" across several disciplines. They are also working with Agriculture Canada and the Canadian Food Inspection Agency on assessing the risk in the food and agriculture sector. This department feels that this area is often neglected, but there is much evidence to suggest that there are plans to target these areas due to its economic impact.

Team Canada next provided the background of Canada's Foreign Affairs and International Trade Global Partnership Program. This program is working on a variety of projects including redirection of former Soviet scientists. Team Canada provided a historical background of the Soviet Union's large offensive biological weapons program. At one time, this program involved 40 institutes in Russia and the former Soviet Union (FSU), employing more than 30,000 scientists and technicians, and weaponized more than 50 biological agents. Following the collapse of the Soviet Union, the scientific facilities became dilapidated and the scientists were underpaid or out of work. These events are a severe biological threat.

Team Canada provided a summary of the work done by the Global Partnership Program in this region. Canada has committed over US$1 billion to this cause: US$100 million was contributed specifically for biological non-proliferation. Canada has developed a comprehensive strategy to work together with Russia and FSU countries to enhance

biosafety, biosecurity, and biocontainment. These efforts include establishing several biosafety and biosecurity guidelines and standards, including several from the World Health Organization, offering numerous workshops, training tools, CDs, and regional training centers, establishing many biosafety associations, and upgrading various facilities. Lastly, Team Canada mentioned publication of the CEN CWA 15793 document, which is a laboratory Biorisk Management Standard.

Next, Team Canada discussed the control of pathogens within its country. In 1994, Canada enacted the *Human Pathogens Importation Regulations* (SOR/94-558). This law required anyone importing human pathogens in Risk Groups 2-4 to obtain a permit to import and to comply with the Laboratory Biosafety Guidelines. A permit was granted only when a facility demonstrated compliance with a Containment Level 2-4 laboratory. This law had several shortcomings including the lack of regulations on exports, the lack of control on domestically acquired pathogens, the lack of requirements for personnel security screening, and it was based on civil law. To address these shortcomings, the *Human Pathogens and Toxin Act* was tabled on April 29, 2008. Unlike the US select agent system, this act incorporates agents based on risk group definitions rather than just those deemed usable for bioterrorism. The Act also prohibits the possession, use, transfer, storage and destruction of human pathogens and toxins without a license, requires personnel security screening and laboratory compliance with technical standards, and requires the designation of a biosafety officer. Furthermore, all laboratory-acquired infections must be reported. In contrast to the earlier law, this Act is based on criminal law with considerable penalties.

Team Canada next presented ongoing work in the Canadian Food Inspection Agency (CFIA). CFIA's counter-terrorism role is to safeguard the national food supply, provide consumer protection, respond to food safety emergencies and outbreaks, and provide stringent border controls, surveillance, and laboratory capacity. CFIA runs assessments for food, animals, plants, (including novel plants and animals) and contributes to the annual consolidated risk assessment for CBRNE threats coordinated by the CSS. Canada is currently working on a funded program entitled "Vulnerability Assessment of Canada's Food Supply" due March 2011. Its primary objective is to enhance its capacity to conduct vulnerability assessment of the food supply against intentional acts, including terrorism.

CFIA describes risk analysis in three parts: risk assessment, risk management, and risk communication. They believe each has its own methodologies. To assess food risks, they incorporate information from disease intelligence and surveillance. The models they use can be tailored to specific scenarios. For example, a specific assessment of importing Chinese apples might generate a risk of introducing the Chinese apple moth into the country. All of CFIA's assessments consider likelihood and impact, and their results are communicated to decision-makers. CFIA also mentioned that their current likelihoods reflect just accidental risk; they are re-tooling this methodology to consider the likelihood of intentional risk. CFIA has asked the intelligence community for additional insight into their risk assessments, but found that these agencies do not have the necessary scientists or scientific capability that the CFIA has. Consequently, a cooperative relationship has

resulted between the CFIA and the intelligence community. Lastly, Team Canada presented several other currently funded projects including the Operational Urban Modeling System for CBRN. A major deliverable of this project will be publication of a report in 2011. This report will be distributed internationally.

DENMARK

Title: Center for Biologisk Beredskab/Center for Biological Defence
Presenter: John-Erik Stig Hansen

Dr. Hansen began with a review of Denmark's National Center for Biological Defence (CBB). This facility was established in 2001 by the Ministry of Health and is recognized as Denmark's national authority on biosecurity. Its annual budget is €3 million and it currently employs 28 full-time and 20 part-time military and civilian personnel. The Center is actively engaged in intelligence, counter-proliferation, counter-terrorism, surveillance, investigation, isolation, quarantine, treatment, triage, as well as decontamination activities.

Denmark has a unique methodology to assess threat. It is defined as: **Threat = Intention * Risk.** Intention and Risk can be further broken down into the following equations:

Intention = (Objective*Effectiveness) - (Cost+Unacceptability)
Risk = (Availability + Previous Use) * (Damage – Countermeasures)

CBB threat assessments consider a variety of factors such as if other places are under attack, if anyone has been exposed, if the aggressor or agent is known, and/or if the method of dispersal is known. CBB's operational response will depend upon the answers to these questions. CBB cooperates with many international organizations for assistance including the Health Security Committee, Australia Group, BTWC expert group as well as several European organizations.

Dr. Hansen provided a risk assessment example using a model that prioritizes biological agents. Mathematically, it is expressed as: **Risk = Likelihood * Consequence^2**
This model can be plotted on a two-dimensional graph. The Y-axis represents the likelihood an agent can be obtained and misused in Denmark. Its value is determined by the average of the values for Availability, Technique, and Historic Use. In contrast, the X-axis represents the maximum consequence if a given agent was used as a biological weapon in Denmark. This value is the average of Morbidity/Mortality, Treatment, Transmission, and Non-health Aspects such as psychological impact. Finally, this value is squared. The final calculation of the maximum risk score is the multiplication of both values.

Dr. Hansen next provided a table of risk scores. Biological agents with a low score (between 2 to 4) included *Balantidium coli*, *Burkholderia pseudomallei*, and non-pathogenic *E. coli*. Agents with the highest score included *Yersinia pestis*, *Bacillus anthracis*, and Botulium toxin. Next, Dr. Hansen presented a plot of several biological

agents using this model. Those agents that were considered the highest risk, based on their likelihood and consequence values, were subject to the most stringent control regulations in Denmark. Those with a lower calculated risk therefore, were subject to lesser regulations. Interestingly, CBB risk assessments also consider recent developments in genetic engineering. If an organism is naturally very rare but could be recreated using publicly available information and technology, it can be factored into the likelihood calculation. Dr. Hansen acknowledged that CBB defines risk much differently than other countries, especially the United States. Their assessments are indeed more generalized, but the Denmark military and other funding groups prefer this approach as it can be tailored on a case-by-case basis to account for intent and accidental risk.

Dr. Hansen concluded with a summary of some enabling dual-use biotechnological tools currently on the market. He suggests that with this new potential and its increasing accessibility, biological weapons of the future could be completely different than our knowledge of historical biological weapons. For this reason, it is important to be vigilant in our efforts to continually define and assess threats. Dr. Hansen ended with results of a Denmark survey conducted on two civilian groups and one military group. The survey asked what weapons were permissible in national defense if an enemy was attacking. Results showed that the use of assassination, napalm, chemical and nuclear weapons were acceptable at least 50% of the time in one or more groups whereas the use of biological weapons had one of the lowest acceptability ratings, especially within the military group.

FRANCE

Title: Some aspects of Bioterrorism Risk Assessment in France
Presenter: Herve Raoul

Dr. Raoul began by explaining biological risk assessments in France are approached in four ways: classifying pathogens of concern, having a national plan, laboratory networking, and using research programs. He stated that one of the most difficult challenges in France is determining what a risk and a threat are.

The risk assessments used to group pathogens of concern in France were determined by a methodology similar to those previously presented, and therefore was not discussed in his presentation. For each pathogen, a score is generated using a series of criteria. This score places each pathogen into one of two broad categories. Some of the criteria include epidemiological factors, infectious dose, morbidity and mortality rates, availability of prophylactic treatment, viability, and transmission rate. Examples of pathogens that present the highest risk to public health (scoring ≥35) include *Yersinia pestis* and viruses such as Lassa, Junin, SARS, Ebola, Marburg, Nipah, and Hendra. Pathogens that present a high risk to public health (scoring <35) include *Bacillus anthracis*, *Burkholderia mallei*, *Burkholderia pseudomallei*, *Coxiella burnetti*, *Francisella tularensis*, hantavirus, Rift Valley Fever virus, Kyasanur Forest hill virus, poliovirus, and avian influenza H7 and H5. Examples of toxins include ricin, botulium toxin, and saxitoxin.

There are three major CBRN antiterrorism contingency plans within the French Government. These are the Piratome governmental plan for nuclear and radiological

terrorism, the Piratox governmental plan for chemical terrorism, and the Biotox governmental plan for biological terrorism. Under the Biotox plan, the country is divided into seven defense zones. There are response capabilities in each of the zones, including a regional reference hospital with diagnostic capabilities. The Biotox plan also has an emergency stockpile resource that consists of antibiotic treatment for one million people, 2100 respirators, and 95 million doses of smallpox vaccine. Dr. Herve added the smallpox vaccine is old and it is likely not all of it would be authorized for use. Also, immuno-suppressed people and pregnant women would not likely be eligible.

France has complete plans to respond to specific scenarios considered to be the highest risk or highest consequence. Dr. Herve further added they perform annual exercises and drills to prepare for real incidents. Biotox has considered contamination of water, food, and drug supplies, dispersion of biological agents in the atmosphere or public buildings, biological homicides, and attacks against a laboratory. They have even considered a possible attack at the Inserm Jean Merieux BLS4 laboratory. Due to lax security, they hired a private company in 2004 to do an assessment at the BSL4 lab. Since this assessment, the government has mandated increased security and the laboratory now has upgraded access control points, guards, systems, personnel checks, and visitor authorizations. Biotox also has several specialized response plans including a Smallpox Plan, a Plague-Anthrax-Tularemia Plan, and a Toxins plan.

Biotox has also organized a national laboratory network. This network is composed of three laboratory levels. The first level consists of first responder labs spread over all seven zones. These labs are responsible for sampling, packaging, transfer, and in some cases diagnostics. Level two are reference laboratories. Level three are national reference centers, including the Inserm BSL4 laboratory. This lab was given the role of being the highest national laboratory and is the only facility allowed to confirm diagnosis of the highest class of pathogens.

In addition to the Biotox research program, France also supports the NRBC Research Program. This program is actively working on many new technologies to reduce biological threat. In the area of immuno-chromatography, they have developed detection tickets for seven toxins including ricin and botulinum toxins, and have developed fluorescent labeling that is 10 times more sensitive than current technologies. They have also developed an extensive RNA expression pattern system and a SMART DROP multiplex PCR laboratory on a chip which can detect 15 various pathogens simultaneously. This technology can be used in the field and then analyzed for diagnostic purposes.

JAPAN

Title: Aum Shinrikyo's Biological Weapons Programs and Japan's Response
Presenter: Katsuhisa Furukawa

Dr. Furukawa explained that Japan brings a unique perspective to the discussion of terrorism because they have actual events to reference and have learned many lessons. In

addition, they have experienced a variety of natural disasters, such as tsunamis and earthquakes. In some ways, Japan's preoccupation with disaster preparedness has become more important to policy makers and has overshadowed the country's preparedness for terrorism. In addition, Japan's governmental ministries responsible for terrorism oversight lack national coordination.

There is not a formal risk assessment methodology currently in place for Japan. National threat reduction activities are based on lessons learned from the previous events. To prepare for future attacks or natural disasters, Japan organizes integrative exercises; more than 20 exercises took place last year. This approach is preferred because it is multi-purpose.

Dr. Furukawa presented an in-depth description of Aum Shinrikyo and its BW program. Aum Shinrikyo was a multinational religious cult that began in 1984. Under its leader, Shoko Asahara, this group had an active biological and chemical weapons program. The cult's membership included thousands of people across all generations, institutions, and countries. Cult members were believed to be controlled by sophisticated mind techniques and were indoctrinated with illegal drugs. They received thousands of dollars, equipment, and weapons in state-sponsorship from Russia. They were also believed to be involved with other organized crime networks. Their purpose was to establish the cult as a widespread state in order to save the souls of human beings. They also firmly believed in a conspiracy theory of the United States and US embassies and military bases were the sites of frequent attacks. Dr. Furukawa added that in many ways, this group resembles al Qaeda.

Aum Shinrikyo's biological weapon program lasted less than five years. It began in 1990, with cultivation of botulinum bacteria and toxin although there is no indication to suggest either were produced successfully. Aum planned to disseminate the bacteria by balloon, which was not carried out due to technical delay in the bacterial cultivation. Aum dispersed what they believed to be botulinum bacteria both by car and in a water reservoir. In 1992, Aum Shinrikyo began their anthrax program under the direction of Seiichi Endo, a cult member who had a Master's degree in genetic engineering. During the summer of 1993, Aum dispersed anthrax vaccine from the top of its Tokyo headquarters. There were also reports that Aum Shinrikyo attempted to acquire *Coxiella burnetii* and Ebola virus, although this was never proved. Aum Shinrikyo's BW program and its attacks ultimately failed. Many believe its failure was the result of Seiichi Endo's inability. Aum Shinrikyo is best known for its successful sarin gas attacks in Matsumoto city and the Tokyo subway line in 1994 and 1995, respectively. Results of these attacks killed 19 total people.

One of the Japanese government's major responses to prevent bioterrorism includes revising and enforcing the "Law Concerning the Prevention of Infections and Medical Care for Patients of Infections". The last revision of this law went effect June 1, 2007. Under this law, a legally-binding standard of laboratory facilities is established with legally-binding standards of possession, storage, use, and transportation of specific

pathogens. Seventy-two pathogens and two toxins are categorized into four regulatory groups. Japan also has several infectious surveillance systems in place.

SWEDEN

Title: Swedish Perspectives on Bioterrorism
Presenters: Magnus Normark and Ake Forsberg

Dr. Normark reported that the current national threat level in Sweden is generally considered to be low. Yet recent events have increased the risk of terrorism in Sweden. This risk is due to several factors including the influx of refugees from conflict-laden areas into the country, Sweden's increased engagement in international operations, and the increasing threat level in neighboring countries. The recent and controversial cartoon illustration of Mohammed by a Swedish artist has also brought Sweden into the terrorism spotlight; this event was the first time Sweden was directly mentioned in al Qaeda rhetoric. In February 2008, Sweden finally announced a National Strategy on Terrorism; however the national resources dedicated to CBRN are limited. Most resources are focused on accidents and natural outbreaks. Current efforts involve developing a framework for risk analysis and management.

The Swedish Defence Research Agency (FOI) is an independent agency under the Swedish Ministry of Defense. It currently employs approximately 1,000 employees and 800 researchers. There has been a major re-organization of FOI in 2007 and it is still evolving. Funding has changed, so the focus of FOI has changed as a result. Their limited counter-terrorism resources are funded mainly by the Swedish Armed Forces, the Defence Material Administration, Ministry of Foreign Affairs, and other Swedish authorities. Dr. Forsberg stated national perspectives need to be broadened. Risk assessments have been conducted primarily without intelligence community input. However, within the next year they hope to have a more developed architecture for risk assessments.

The FOI has been primarily involved in threat assessment, and not as much in risk assessment. Dr. Forsberg said their model is simple due to lack of funding and FOI does not have a clearly defined role. In their model, various actor characteristics are considered; other criteria considered are access, effect, production (culturing), stability, infectious dose (toxicity), and safety for the actor. All criteria are scored (using a 1-3 scale), totaled, weighted, and ranked for each agent. Their weighting method was decided on by a panel of Swedish scientists.

Dr. Forsberg stated they would like to have more input on actors. They also plan to assess the effect of specific release incidents on food and validate their model for other types of attacks and releases. Dr. Forberg ended by saying they plan to return to Sweden with many ideas about the different methodologies and criteria they have learned from this symposium.

UNITED KINGDOM

Title: Resilience Capability Framework
Presenters: Bevan Brownhill

Dr. Brownhill began with an overview of the UK's Resilience Planning Cycle. This cycle considers four primary questions in the following order: 1) What risks do we face? 2) What planning assumptions should we make? 3) What are our resilience requirements and 4) What is the current level of capability/gaps? From here, a readiness assessment is determined which may be modified and/or cycled though the process again.

The risk assessment process is comprehensive and covers all types of risks supporting the full range of planning at all levels. The assessment has a consistent application of the approach to all risks. Lastly, it has an agreed basis for planning to all those who plan. Likelihood and impact are considered equally and together they determine risk. This process assumes a reasonable worst-case scenario. Worst-case scenarios are agreed upon by subject matter experts. This process is not perfect; however, they have been working on it annually for more than four years. Each year they challenge a different aspect of the process from the methodology to the plausible risk, etc and it improves continually. The UK risk assessment process is sensitive and is its methodology is not published.

Impact assessments evaluate the overall impact of six categories: Economic (such as GDP), Fatalities, Casualties, Social Disruption, Outrage, and Anxiety. The first four are easily quantitative; the last two they often conduct workshops to survey the public to help quantify the impact.

The UK evaluates likelihood based on natural hazard risks and malicious threats. Information concerning likelihood is primarily gathered from specialized agencies within the intelligence community. Hazards are evaluated using historical evidence, predictable events (such as weather), and expert advice. Threats are regarded more as plausibilities and require intelligence about capability, intent, and vulnerability. Threats and hazards are both measured in logarithmic scale. The risk matrix is a graphical plot of both impact and likelihood. The plot illustrates a gradation of risk. The upper right hand corner presents the highest risk; the lower left hand corner presents a low risk. They often communicate risk to decision-makers by writing preparedness statements using hypothetical scenarios that fall into the high likelihood and high impact areas.

The Risk Assessment process is shared with a number of external players at the national, regional, local, and business level. In addition, this process drives future planning assumptions and local risk assessment guidance to the capability response teams and decision-makers. The planning assumptions attempt to identify risks (such as what risks should drive planning? What is the worst case scenario?) and consequences (such as what are the general consequence? Is there regional variation or military involvement?). These results are not published.

The Capabilities Program is the UK governmental framework to build a robust infrastructure of response. Its purpose is to respond rapidly and effectively for the

consequences of civil devastation and widespread disaster. There are 11 functional areas that deal with the assessments of risks and consequences. These include such areas as animal and plant diseases, CBRN, evacuation, flooding, infectious diseases, and humanitarian assistance.

The UK assesses risks associated with biological agents. The UK's "Anti-Terrorism Crime and Security Act (ATCSA)" is one large piece of national legislation that has been revised to accommodate a growing number of biological pathogens and toxins which could potentially present a risk to the country. It was mentioned that although the process is not formal, the UK government has the right to ask about pathogen research, and to prohibit certain people from working on pathogens. The current list includes approximately 120 human and animal pathogens. This legislation also includes genetically engineered pathogens. Interestingly, there are no plant or fish pathogens on this list; national subject matter experts are not worried about these pathogens as the UK has not been self-sufficient in crop production for over 100 years. Biological risk is based on historical threats, including state and non-state, current intelligence, and what is feasible within the country. The list is divided into a primary list of agents presenting the most risk, and a lesser secondary list. These agents are used in various scenarios and the All Hazard Risk Assessment. Finally, recently the UK government mandated a hazardous substance review list.

UNITED STATES

Title: An End-to-End Quantitative Approach for Estimating Bioterrorism Risk
Presenter: Steve Bennett

Dr. Steve Bennett presented the DHS Bioterrorism Risk Assessment (BTRA). These assessments are a formal process intended to help prioritize and guide investments in biodefense-related research, development, planning, and preparedness. These assessments are continually updated to address the changing nature of the bioterrorist threat and the changing availability and capability in science and technology. Consequently, the US prepares the BTRAs biannually. DHS believes that the quality of their risk assessments will be improved through information sharing in venues such as this meeting.

DHS uses the standard definition of risk, where **Risk = Probability x Consequences.** Risks are calculated for specific scenarios; these scenarios consist of specific notional adversaries using specific biological agents in certain categories of release events. In contrast to risk assessments for common events, risk assessments for rare or data-poor events are very difficult. Previous US work on risk assessments of low frequency and high consequence used a Probabilistic Risk Assessment (PRA) approach. DHS has continued with the PRA methodology for the BTRA. In general, the PRA divides the spectrum of possible events into a discrete set of scenarios. For each scenario, consequence and probability are estimated. Probability estimates are calculated on an event tree corresponding to specific scenarios. An event tree is a visual tool that is used to represent multiple outcomes for consecutive events. Each path through the tree is a

unique scenario. One of the DHS goals is to modify established PRA techniques for terrorism risk assessments.

The general scope of the DHS BTRA includes: 1) analysis of potential bioterrorism agents (38 human and five livestock pathogens were analyzed in the 2008 BTRA); 2) millions of enumerated scenarios grouped into aerosol (indoor and outdoor), food and water contamination, human vector, and transportation categories; 3) probabilities elicited from the intelligence community; and 4) physically-based consequence modeling using fatalities, illnesses, and direct and indirect economic impacts. Specifically, it is composed of an event tree with 16 different events. Events in the tree are grouped into five phases including 1) Initiation and Agent/Target Selection 2) Acquisition 3) Production and Dissemination 4) Transport and Storage, and 5) Response. The event tree probabilities come from structured elicitations of quantitative probabilities primarily from the intelligence community. This judgment can be refined as experiences are gained. Dr. Bennett mentioned one of the most difficult parts of the BTRA is communicating and translating the data to the decision-makers in a way that conveys the uncertainty, and provides broad spectrum needs to mitigate risk groups.

Dr. Bennett emphasized that risk is uncertain. Characterization of this uncertainty is one of the most difficult parts of the BTRA. Dr. Bennett summarized the advances with the 2008 DHS risk assessment. In contrast to the 2006 report, the 2008 assessment will be an integrated CBRN risk assessment (iCBRNra). This will include two key deliverables: 1) a iCBRNra report and 2) a WMD risk analysis toolset for evaluating risk reduction potential of future Medical Countermeasures. The 2008 assessment will be delivered to multiple customers. It offers many significant expansions and improvements in modeling and information gathering since the 2006 assessment.

Additional Presentations

An Overview of the DHS Chemical and Biological Division
Presenter: Elizabeth George

Dr. George presented a descriptive overview of the US Department of Homeland Security (DHS), its Science and Technology Division, and more specifically, its Chemical and Biological Division. The mission of the Chemical and Biological Division is to increase the Nation's preparedness against these types of threats through improved threat awareness, advanced surveillance and detection, and protective countermeasures. Within the four pillars of US national biodefense, DHS is specifically responsible for threat assessments, critical infrastructure protection, attack warnings, attribution, response planning, and risk communication.

Dr. George stressed the importance of risk assessments in guiding US national biodefense investments. Three major goals of risk assessments are to inform national priorities, prioritize risks for various sorting parameters, and identify key vulnerabilities and knowledge gaps. The US has produced two national bioterrorism threat risk assessments (BTRA) to date, in 2006 and more recently in 2008. The National Biodefense Analysis

and Countermeasures Center (NBACC), also collaborates on these assessments, providing scientific support for threat characterization. Their work helps eliminate the knowledge gaps identified by risk assessments.

The Biological Division of DHS is also actively working on detection capabilities to mitigate consequences. Dr. George presented a thorough explanation of the Aerosol Biothreat Agent Environmental Monitoring program, also called the BioWatch program. The detection and monitoring system, first implemented in 2003, was established in more than 30 cities. The third generation of this technology, planned for 2009-2012, is expected to cover a major portion of the US population. In addition, this technology is already being adapted for use at the borders and has been deployed at such high risk places as Plum Island. Dr. George concluded with a discussion of other DHS-sponsored technology and a brief overview of the Chemical programs.

Risk-Informed Biodefense Countermeasure Strategies and Policy-making
Presenter: Bob Hooks

The Office of Health Affairs (OHA) serves as DHS's principal agent for all medical and health matters. Its primary goals are to function as the principal medical authority for DHS, lead the Department's biodefense responsibilities, direct a coordinated national architecture for WMD planning and catastrophic incident management, and ensure DHS employees are supported by effective occupational health and safety programs. OHA has numerous external customers including the Department of Defense, Department of State, United States Department of Agriculture, state and local government, and private sector partners.

Mr. Hooks gave a brief introduction to the DHS integrated chemical, biological, radiological, and nuclear (CBRN) Risk Assessment and Risk Management approach. Theis integrated approach facilitates an effective countermeasure strategy across several weapons of mass destruction (WMD) threat areas. For example, this information directly impacts the efforts of both DHS and the US Health and Human Services to accelerate cutting-edge research and defense technology, and develop, purchase, stockpile, and deploy priority medical countermeasures to protect the US population from the effects of CBRN threat agents, as required under the Project Bioshield Act of 2004. In addition to the Bioterrorism Risk Assessment (BTRA), other assessments, such as the "Material (Population) Threat Assessments," impact the Department's efforts to implement the Bioshield Act. . These assessments are a set of plausible, high consequence scenarios used to estimate the potential number of exposed individuals, their exposure levels, contaminated areas, and other "collateral effects". Mr. Hook ended his presentation with a brief overview of the BioWatch National Network and DHS food and agricultural defense.

Overview of Risk Assessment Methodologies for Security Applications
Presenter: Susan Caskey

Susan Caskey provided a general overview of risk assessment methodologies. This talk was designed to provide a common framework and language for discussion of risk assessment methodologies.

A hazard is defined as the way in which an object or situation may cause harm. Risk is the chance that harm will actually occur. Risk is a function of likelihood and consequences.

Traditional security assessments characterize the assets and the threat. Using a vulnerability assessment the likelihood is calculated. The consequences are also calculated. These data points provide the risk assessment results. For traditional hazard assessments, the hazards are identified and the consequences are calculated. Typically both indirect and direct consequences are determines. The likelihood is assumed for a hazard assessments therefore not directly part of the overall risk calculations.

There are numerous published risk assessment schemes and each can provide a better assessment of risk depending on the type of risk being assessed. That is, the risk assessment problem should drive both the method and the schemes use. Risk assessments can utilize multiple schemes, but should be as simple as possible and be elaborated upon when needed. In a quantitative scheme, the risk assessor assigns numerical values to the likelihood and consequences of the adverse event. In a qualitative scheme, the risk assessor may rely on linguistic variables to estimate the likelihood and consequences of the adverse event. Probabilistic schemes are quantitative assessments of the likelihood. Probabilities are used to calculate the likelihood of an adverse event occurring. Relative schemes are typically qualitative assessments of the likelihood and consequences of an adverse event, the results provide the relative risk to other possible adverse events or to the status quo. Multi-criteria techniques break down both the likelihood and consequences in to sets of criteria and sub-criteria and score each criterion independently from the overall risk. These scores are then combined to determine the resulting risk. Criteria can be weighted to highlight the differing overall impact each criterion has on the resulting score.

It is critical that a common language be used to avoid miss understanding of the results and allow for repeatable assessments. Risk assessments can be combined or layered to address more complex questions. It is important that those conducting risk assessments should be explicit about uncertainties. The model is only as good as the data (Garbage in = Garbage out).

Participants commented that the definition of risk is a problem. It is inherently a fuzzy concept. There is a lot of writing on risk, but the definition is not consistent. Countries often struggle with what their definition of risk is.

The use of a 2-dimentional graph highlights the two different axes to avoid the numeric 'risk'. There is a multiplicative relationship and sometimes an additive relationship between criteria. For example, Denmark multiplies the consequence times two, which in their model defined consequence is twice as important as the likelihood.

It was mentioned that for assessing the risk of base cases, a risk assessor can use qualitative values in a quantitative scheme, by substituting a dummy value for unknowns. This is an acceptable model, but it is critical to clearly show all assumptions, or dummy values. Documentation of the assumptions within the model makes the model much more defensible. There is no right answer on how to model or how to define unknowns. Humans are unpredictable, bioagents are unpredictable, and therefore there will always be unknown factors in this type of risk assessment. Visualization of uncertainty and data sensitivity can help provide a better understanding of the model.

Section II: Roundtable Discussions

Incorporating Threat and Quantifying Likelihood

This roundtable aimed to explore mechanisms for incorporating threat into risk assessments and the related difficulties associated with quantifying likelihood.

Some participants commented that thresholds for relative comparison might be better than absolute likelihood. Additional comments addressed concerns of ranking risk. Ranking risk can be misleading; risk could be rated highly because of consequence and/or ease of acquisition. Therefore, it is important to rate, not rank. It is politically problematic to rank risks #1, #2, or #3 because often there is a tendency for decision-makers to put all the money to #1 while it is possible that a risk ranked #3 could hypothetically be an emerging threat that needs immediate attention or it could become a #1 ranked risk in the future. It is also important to make all results of a risk assessment reproducible and consistent. Taxonomies encourage consistency, consider specific criteria, and then are used to rate the risks.

In general, there is not enough intelligence to evaluate likelihood. A small scale attack would likely go unnoticed. Clever terrorists could go to a university, work with non-Select Agents, buy standard equipment, and initiate an attack without any warning and/or knowledge of the event. To mitigate this risk, policy makers should also consider what is readily available, determine the necessary control mechanisms, and worry less about the "high consequence" agents that come with a high rate of interdiction or failure.

Policy tends to be incident driven. Some countries use a "threat informed" concept.

One cannot be prepared for everything. The international community should develop a short list of easily acquired and deployable agents. It is unwise to focus only on "high consequence" pathogens, because many of the "realistic threats" could be easily missed. The growth of the biotechnology industry will make it even more challenging in the future—terrorists are getting smarter, and scientific literature is readily available. And terrorists have begun to think about WMD. One participant indicated the bioterrorist threat of biggest concern is an individual with a bachelor's degree who has access to PubMed. The future of terrorism is impacted by the facilitation of exchanges of ideas and doctrine that are widely available online.

It is technically easier to make a bio-weapon than to build a bomb. However, CBRN is an aspiration of many terrorist groups; bioterrorism is only one component. Therefore, it is important to have a more integrated approach to risk.

Sociology is an important factor to consider. A participant asked, "Where did the ideas for the anthrax letters, including the hoax letters, come from?" Media has helped to propagate the hoaxes. One participant wrote to the editors of the newspapers telling them

they are perpetuating the terror. Two months after the newspapers stopped reporting the hoaxes, the letters stopped.

Intention is also important; if there is intention, then it does not matter how easy it is to use the weapon. The weapon does not have to be effective to create terror. The use of smallpox is a different intent than the use of anthrax. There is no way to know if someone has the intention to kill thousands indiscriminately.

In the case of Aum Shinrikyo, Japan was able to see a dynamic interaction with capabilities and intent. Public reaction to an accident or malicious event cannot be quantified. The risk-based approach seems to only be concerned with capability and success, and does not account for public reaction. Cost is also an important consideration. What is the lowest cost agent that will give the desired consequence? There are several things that can impact the likelihood of an attack including political, social, and personal factors. In some instances, the intelligence of an adversary correlates with increased likelihood. An example of this is seen in the hacker mentality. A person might not be intending to do harm, but they are attracted to whether they can do it or not.

The work of the intelligence community in this area is also problematic because they have often been wrong on several important issues. Now, assessors are hesitant to say anything without overwhelming evidence. Without strong evidence, they will not make extrapolations or predictions. It might be helpful to have the intelligence community look more deeply at past incidents and current situations to provide foresight for likelihood.

What about the spread of effective techniques to other groups? Is anyone evaluating the time and evolution of the spread? For example, the occurrence of suicide bombs in shopping malls originated with one terrorist group but has spread within multiple countries. Also, in that "copy-cat vein" is 9/11 the new bar or standard for what other groups will aspire to copy? Or will they wish to "top" it? Is the objective body count or innovation? Some of the failed attempts could be an inspiration for future attempts, i.e. the failed '93 bombing of the WTC and Yusef's famous response that he might have failed, but the towers wouldn't stand for long. The motivation of a terrorist would affect the types of agents attractive to them. A religious terrorist group would have a different goal than a militaristic group. The objective could be body count for some, and incapacitation for another.

Why have we not seen more terrorist events if the likelihood is so high? One theory is that skill is often overestimated. There are intangible skills that one cannot quantify and this is taken for granted by many developed countries. Legitimate scientists in developing countries frequently have trouble with cross-contamination and laboratory practices issues. This could have a direct affect on the likelihood of a successful bioterrorist attack. Another theory believes that a terrorist group with a sufficient motive would go to great lengths to acquire the training/expertise necessary to develop a bioweapon. It is difficult to truly know the frequency of these events; actual interdiction

could be higher than we know because they are either unsuccessful events and/or they are not widely reported.

Consequence Analysis: Methods and Metrics

This roundtable discussed consequences in a risk assessment, including the various factors that make up consequence, human vs. animal impacts and variation of mitigation measures in factoring consequence.

Metrics are difficult, especially the operational and psychological impact metrics. It is difficult to determine whether they should sample to zero, or sample to "clean". In the case of one building contaminated with anthrax, the cost of cleaning was approximately US$35 million. Although no one died, it was necessary to sample and resample to reassure the employees the building was "clean". Billions of dollars were spent as a result of the 2001 anthrax attacks. Morbidity and mortality are important but it is also necessary to consider the time it takes to return to normal. This is also a huge cost. Media coverage often contributes unnecessarily to the economic impact of an event. What is the indirect consequence of the media coverage? There is some speculation that the media coverage following 9/11 influenced elections, led to the invasion of Afghanistan/Iraq etc. How far do you measure the indirect consequences?

It is important to determine what is more important to a terrorist – to kill or to sicken? For example, the 9/11 attacks caused more deaths than injuries; if it had been the reverse, what would have been the lifetime psychological and emotional effect of the injured victims? Another non-terrorist example is the comparison of Katrina and the Southeast Asia tsunami. In the case of the tsunami, the metric was number of people who died and their identification. For Katrina, the metric was the housing impact, the lost or the dispersed citizens. The metrics for similar events may be different depending on the location of the event.

Agricultural and human consequence metrics are very different, especially the variance of economic and long-term impacts from an attack. More importantly, their value is perceived differently by terrorists and the general public. If one maps the impact in a uniform way, it is possible to translate all the factors into economic values. However, one must then confront the problem of putting a dollar value on human life.

The US is extremely risk adverse. The government will set up billion dollar programs to mitigate the risk of another catastrophic terrorist event based on the 9/11 event that killed 3,000. However, there are 40,000 car deaths and 5,000 influenza deaths annually. Yet there are no cabinets or federal directives about driving and avoiding influenza. Intent becomes the key difference. One does not drive a car with the intent to kill people. Also, controllable risk is dealt differently than that which you cannot as well as the fear resulting from that. Additionally, some things are just more sensationalized; there are campaigns against cancer, but not heart disease, which kills more people. What is the acceptable risk? In the food industry, blowfish is an anomaly because people voluntarily

take that risk, but they won't buy Brazilian beef. Yet there is a much higher risk of dying from eating toxic blowfish, than getting encephalitis from Brazilian beef.

The level of preparedness can also affect consequence – the time lapse from the initial attack to the return to normal. Timing and circumstance can affect consequence. Countermeasures are different if there is opportunity to prepare. For example, a nation can have more security and/or medical personnel onsite for the Superbowl or the Olympics, and therefore mitigate its risks and consequences; it is more difficult for something totally unexpected. The quantitative quality of consequence is much simpler an issue than likelihood.

Why hasn't an FMD attack happened? There is no risk to the people, it requires low technical capability, and would have a massive economic impact. One theory is that since it is only an economic impact and there is a low mortality and psychological impact it doesn't fit into the terrorist mission.

It is important to include some biological agents as controls in a risk assessment to validate the model. If a known low risk agent is scored highly, than it is evident there is a problem with the model.

Uncertainty and Risk Communication in Risk Assessment

In this roundtable, participants discussed uncertainty and the issues associated with communication of uncertainly to decision makers.

Depending on the data, uncertainty, or unknowable data, is resolvable. This may take intelligence, awareness, and research to expand knowledge in these areas but one can, at least, establish what unknown factors are in play. Uncertainty is a huge factor, especially data uncertainty and knowledge uncertainty. For example, in the case of ricin, the challenge is to factor in the uncertainty of whether the actor will choose ricin, if they will successfully acquire it, deploy it, how effective the deployment will be, and what the necessary dosage would be. Furthermore, it is extremely difficult to convey all of these uncertainties to the decision makers.

Uncertainty is inevitable and must be accepted. Biological weapons are very different than conventional weapons. No one can know all of the various ways a biological agent can be acquired and spread successfully. Unfortunately, one of the biggest challenges is that decision-makers do not want any uncertainty in their guidance.

Participants presented several ideas to solve the uncertainty problem including the use of 95% confidence ratings with significance levels of 5%. Additionally working very closely with subject matter experts and learning mechanisms to 'calibrate' the confidence of those experts can help provide better levels of confidence and uncertainty. Development of an "uncertainty taxonomy" would also be an interesting approach to address the various types of uncertainty. Then when results are communicated, one can highlight the cause of uncertainty whether because it is novel or there is a knowledge gap.

Relative probability takes some uncertainty into account, and by looking at reasonable worst case scenarios, it also takes into account uncertainty without quantifying.

When communicating a risk, one must communicate a recommendation and inherently assume those uncertainties. It is difficult to simplify the results. More and more, the decision-makers question the details of the influence on the recommendation. Some suggest having a bottom-up consensus that is agreed to. Therefore, when the planning assumptions are given, they accept it and do not question it because the methodology is already agreed upon. It is important when communicating your recommendation on risk, to also communicate an acceptable level of risk.

Some assessors separate risk management and risk assessment. The risk characterization is agreed upon by the risk manager and risk assessor. The risk manager then communicates the data to create buy-in with the stakeholders. A high level of uncertainty could also delay a decision. Possibly there is a link between criticality of the risk, and how to deal with that uncertainty.

Risk Communication and Supporting Decision Makers: Impacting Counterterrorism Policy with Risk Analysis

This roundtable provided discussion on communication with decision makers and the public and the potential risks inherent to communication and miscommunication.

Communication strengths and weaknesses depend on who is asked to perform the assessments, and how far up the decision maker chain it goes. Different risk assessment customers for the same assessment can be a problem. The circumstance of the assessment can also affect risk communication. If an assessment is produced in a time of public crisis, it may be classified which significantly can slow down the communication process to the public. Moreover, the media is historically poor with communicating scientific and technical information. It would be beneficial to develop relationships with media to help convey the message to those with poor understanding of science and technology issues. Caution should be taken with the media, though, as often, when you convey to the media not to panic, that is exactly what the public does. Finding trusted media representatives is key to effectively communicating your message.

If the experts do not deliver the information to the media, then the media will look for opinions elsewhere. This almost always causes panic and miscommunication. For example, during the FMD outbreak there was a lot of misinformation in the media that caused more panic than necessary. To best deal with the public is to have an actionable portion. Do not communicate a risk without means to mitigate the risk. Proactive information helps one react correctly to the questions. Miscommunication can easily proliferate and can be very difficult to undo the damage.

Information given by the government must, sometimes be communicated several times before the public responds. Even after many attempts, there are still some people who do

not listen. Furthermore, slower communication can lead to increased mistrust. Risk analyses must account for these types of issues, i.e. where those in charge may not follow regulations, or other factors may interfere with the mitigation of consequences. The policies need to be reflective and modeled to account for these things. There needs mechanisms to look at policy as another factor in the problem

A recently published academic paper that analyzes risk in several US cities relies on a flawed methodology and has inconsistencies in their data. It is of concern that the public might trust this report more than the reports produced by DHS or other Federal agencies with solid methodologies. In general, this can also be a problem with any private industry or academia publishing vulnerabilities to increase adversary awareness. Where is the balance for what the public needs to know to take action, and what should be classified to reduce the risk of adversary awareness? Risk communication with trade and industry is important, and conveying that sensitive information to those who do not have a clearance. The vulnerabilities need to be given to those who can solve them, but it is a problem packaging that information so it can be safely distributed. There are several factors to consider such as subject matter, classification, differing recommendations, etc. One must break down the message into talking points and translations for different audiences like the media and decision-makers, while keeping the message consistent. There is usually a different group for communication than for the analysis. It does not matter how well the analysis is done, if the communication is inaccurate; those communicating the risk could distort it from the analysis. There needs to be some integration of the knowledge management, communication and analysis groups.

Participants all believed that in the importance of international collaboration. This meeting was characterized as a right first step. If there is consensus internationally on what is dangerous, then we can all be safer from it. The countries represented at this symposium may already be safer, but what about non-represented developing counties and issues like SARS and avian influenza. In today's world, information is saturating the public. The constant communication of risk from SARS to avian flu to global warning, can ultimately desensitize the public. There needs to be a strategy to help communicate one's risk message above the roar of everyday doomsday scenarios.

Country Perspectives on Meeting Highlights, Future Opportunities, and Challenges

AUSTRALIA

It is reassuring to see risk assessment methodologies are so similar in the various countries. It is also encouraging to see that many countries are taking these threats so seriously. Future interests include learning more about how to use risk assessments to inform policy and decision making. This meeting was very informative; hopefully there will be future collaboration with fellow participants.

CANADA

Canada felt that there would be value in sharing their risk results to see how they compare with other countries' results. Canada is discussing using a common language and methods for risk assessments. There is not one model for everyone, but if it is possible to use different tools to approach the same results and identify where the commonality is, that would be beneficial.

Canada struggles with informing the scientific community where the priorities are, and at the same time getting that information to the decision makers. There is a common problem of balance of investment. Canada needs to instill consistency, reproducibility, and commonality. Once these are addressed, one can compare the results and mitigation practices. Education is another struggle; everyone talks about risk but they are not talking about the same thing. The language must be consistent so that there can be better inter-agency communication. Also, it is difficult to manage "reach-back", i.e., not just running an assessment and putting it on the shelf. In Canada, there are single focus points of contact, but no coordinated ongoing management. There are also time constraints on communication; they need to explore visualization to be more effective in the presentation of their results. It would be interesting to see an analysis of the investment at the different stages: preventative, management, and response.

One of the main struggles is application of the risk assessment. How can we prioritize our need for solutions? Is a better detector really the solution? After that, how do we get the consumer to embrace a new product to mitigate risk? There is also a need for advanced planning, to include communication, mitigation, policy, and stakeholders with different vested interests, etc.

It was very useful to see the larger perspective and how that can affects the program level.

DENMARK

It was interesting to see consensus within the countries - we are all either on the right track, or we are all wrong. The remaining challenges that need to be addressed include intent analysis; the threat assessments differ where our risk assessment is similar. It would also be valuable to see a methodology on how to do a threat assessment. Denmark is interested in finding a way to project threat indicators to help the intelligence community. This would be important for them because the intelligence community provides much of the data for their threat assessments.

JAPAN

The Japanese perspective is different because they have experience in each type of CBRN event. Japan runs scenarios and exercises and identifies the capability gaps, yet they never affect the decision makers. Japan struggles with effectively communicating the results to see appropriate policy change. It was encouraging to see other countries are

working actively in risk management. Hopefully, the information gathered from this symposium will persuade Japan to begin using risk assessments.

SWEDEN

There are many changes Sweden needs to make to establish a comprehensive approach to risk assessment. It was interesting to see that the capabilities seem to be benchmarked for many countries. It is also interesting to see where improvements are needed internationally. In Sweden, the lack of funding is a major limitation in creating a better methodology.

This symposium has been useful to see that these processes are not coordinated efforts in all countries; that there is not just one department responsible for assessment. It was also apparent that capabilities need to be influenced by risk assessments. It was valuable to learn risk assessments can be so useful to direct decisions.

UNITED KINGDOM

It is useful to look at the crossover benefits of commonality and differences that each country faces. Next steps should address some of the common issues we all face in risk communication and social impacts in consequences.

It is reassuring to see many of the participant countries are doing many things similarly. The objectives for each country might be different, but the results are not that different. It is also encouraging to see consensus on the same issues and agents. For next steps, it would be valuable to know which agents participant countries are most concerned about, and how that threat is managed. Everyone should be cautious about interpreting risk assessments results because it can be dangerous to use the output of the data for other uses. It is also extremely important to clearly communicate the output and its purpose to the decision makers.

UNITED STATES

The US models have matured in the last several years. Major problems that continue to challenge the process include populating the model with sufficient data and managing uncertainties. There is also an issue with measuring many of the qualitative issues with consequence, especially how to measure social consequences. Other challenges include risk communication, data interpretation and visualization, and the use of risk assessments after they are completed.

The model has a “chicken and the egg problem” with identification of the data gaps and the data gaps dilute the model. They have tried to prioritize the data gaps in some way. It is likely there is too much detail, but it will be easier to prune later once it is determined if certain data criteria drive the assessment. Another challenge is knowing the right questions to ask.

When the assessments are completed, it is very difficult to answer the variety of questions posed by the results. Risk management issues are also very challenging. The US assessments drive how we handle and manage agents of concern in our country; it is very interesting to see how other countries prioritize their agents and their perspectives on risk assessment methodologies.

The perspectives on threat and intent have been useful. EPA is usually involved in clean-up and response. They are consequence management, and they are recently looking at threat and intention. The definition of risk at this meeting has helped her perspective. It is also valuable to see how other countries weight criteria.

It has been useful to see the need for international collaboration. Understanding how other countries are ranking threats will help everyone - there is not just one solution. The next steps should be to progress toward more collaboration.

The value of risk assessments is evident from this meeting for funding, for capabilities planning, etc. Future discussion should focus more on determining.

Next Steps and Future Directions for the Group

The final roundtable discussion stimulated thoughts and ideas for the group's next steps. Participants found the symposium to be very informative and reiterated their commitment to continued work in these areas. A variety of recommendations were generated during the discussions. Participants were eager to pursue these goals collaboratively.

- **Tools and Resources:** Participants identified the need for a variety of tools and resources to facilitate terrorism-based risk assessments. These tools and resources should be developed and distributed to the international community. Examples of necessary tools include a terminology lexicon, a metrics or rating table, and a message map that could be used for such topics as risk communication. It is believed these resources would be invaluable to create a common international language and understanding of basic bioterrorism risk assessment concepts.

- **Shared results:** Participants were eager to learn more about risk assessment methodologies and results in each other's countries. Many participants proposed collaborating and sharing results to strengthen their own national capability. The types of information requested most often included scenarios types and results, gaps and uncertainty results, risk communication, and risk management practices.

- **Focused discussions:** Participants acknowledged the lack of national commitment in all areas of CBRN terrorism preparedness. All agreed that the types of discussions promoted at the **DHS International Discussion of Bioterrorism Risk** symposium were invaluable and in the future, a similar forum which addreses specific risk issues would be welcomed. Participants recommended future discussions to specifically include risk communication and

consequence management issues, methods to quantify psychological and social impacts, in-depth reviews of historical bioterrorism events, the similarities and differences of biological and chemical terrorism, current dual-use biotechnology and proliferation issues, and reviews of policies that drive risk assessments as well as reviews of risk assessments that drive policy.

- **Future Meetings:** Participants agreed that similar **DHS International Discussion of Bioterrorism Risk** symposiums were crucial to sustain international efforts to mitigate the risk of bioterrorism. It was recommended future symposiums invite more countries from other areas of the world to engage diverse international perspectives in bioterrorism risk assessment methodologies. Participants also proposed that future symposiums be held approximately bi-annually.

Appendix A: Participant List
DHS International Discussion of Bioterrorism Risk

Kevin Anderson
United States
US Department of Homeland Security/NBACC

Sara Joan Armour
Canada
Defense Research and Development Canada

Steve Bennett
United States
US Department of Homeland Security

Bevan Brownhill
United Kingdom
UK Cabinet Office

Susan Caskey
United States
Sandia National Laboratories

Bradley Dickerson
United States
US Department of Homeland Security

Maureen Ellis
Canada
Foreign Affairs and International Trade Canada

Ake Forsberg
Sweden
Swedish Defense Research Agency

Katsuhisa Furukawa
Japan
RISTEX

Harry Gardiner
Canada
Canadian Food Inspection Agency

Jesper Nielsen
Denmark
Statens Serum Institut

Jennifer Gaudioso
United States
Sandia National Laboratories

Elizabeth George
United States
US Department of Homeland Security

Lisa Astuto Gribble
United States
Sandia National Laboratories

Alain Goudreau
Canada
Defense Research and Development Canada

John-Erik Stig Hansen
Denmark
Statens Serum Institut

Natasha Hawkins
United States
US Department of Homeland Security

Bob Hooks
United States
US Department of Homeland Security

Michael Kuhlman
United States
NBACC

Andrew Matz
Australia
Office of National Security

Tonya Nichols
United States
Environmental Protection Agency

Stephen Norman
Canada
Canadian Food Inspection Agency

Magnus Normark
Sweden
Swedish Defense Research Agency

Hervé Raoul
France
Inserm

Shravanthi Reddy
United States
US Department of Homeland Security

Shane Roberts
Canada
Public Safety Canada

Penny Satches-Brohs
United States
US Department of Homeland Security

Allison Saunders
United States
Department of State

Appendix B: Agenda
International Discussion of Bioterrorism Risk

Tuesday May 6, 2008

8:00 am	**Continental Breakfast/ SNL Badging**	
8:30 am	**Welcoming Remarks**	**Henry Abeyta** Sandia National Laboratories, Global Securities Program, Deputy Director
8:40 am	**Welcoming Remarks**	**Sandia National Laboratories, International Biological Threat Reduction Department**
8:45 am	**Introductions**	
9:30 am	**Overview of DHS S&T Chem/Bio Division**	**Elizabeth George, Ph.D.** US Department of Homeland Security, Chem/Bio Division, Science & Technology Directorate, Director
10:00 am	**Group Photo/Break**	
10:30 am	**Risk-Informed Biodefense Countermeasure Strategies and Policy-Making**	**Bob Hooks** US Department of Homeland Security, US Deputy Assistant Secretary for WMD and Biodefense
11:00 am	**DHS Bioterrorism Risk Assessment**	**Steve Bennett, Ph.D.** US Department of Homeland Security, Chem/Bio Division, Science & Technology Directorate, WMD Risk Assessment Program Manager
12:30 pm	**Lunch**	
1:30 pm	**Roundtable Discussion Topic I: Incorporating Threat and Quantifying Likelihood**	
2:45 pm	**Break**	
3:15 pm	**Roundtable Discussion Topic II: Consequence Analysis: Methods and Metrics**	
4:30 pm	**Adjourn**	
6:00 pm	**Bus departs Hyatt Place Hotel for Symposium Dinner at La Placitas Restaurant in Albuquerque Old Town**	

Wednesday May 7, 2008

7:30 am	**Continental Breakfast**	
8:00 am	**Session II – Participant Presentations (30 minute presentations and 15 minutes for Q&A per country)**	Australia
8:45 am		Canada
9:30 am		Denmark
10:15 am	**Break**	
10:45 am		France
11:30 am		Japan
12:15 pm	**Lunch**	
1:15 pm		Sweden
2:00 pm		UK
2:45 pm	**Presentation Discussions**	
3:15 pm	**Break**	
3:45 pm	**Roundtable Discussion Topic III: Uncertainty and Risk Communication in Risk Assessment**	
5:00 pm	**Adjourn**	
	Dinner on your own	

Thursday May 8, 2008

7:30 am	**Continental Breakfast**	
8:00 am	**Roundtable Discussion Topic IV: Supporting Decision Makers: Impacting Counterterrorism Policy with Risk Analysis**	
9:15 am	**Overview of Risk Assessment Methodologies for Security Applications**	**Sue Caskey** Sandia National Laboratories, International Biological Threat Reduction Department, Senior Member of the Technical Staff
10:00 am	**Break**	
10:30 am	**Country Perspectives on Meeting Highlights, Future Opportunities, and Challenges (5 minutes each)**	Representatives from each country
12:00 pm	**Lunch**	
1:00 pm	**Meeting Summary**	**Steve Bennett, Ph.D.** US Department of Homeland Security, Chem/Bio Division, Science & Technology Directorate, WMD Risk Assessment Program Manager
1:30 pm	**Roundtable Discussion Topic V: Next Steps and Future Directions for the Group**	
2:30 pm	**Adjourn**	