Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science
Volume 11, Supplement 1, 2013 © Mary Ann Liebert, Inc.
DOI: 10.1089/bsp.2013.0039

Actionable Knowledge and Strategic Decision Making for Bio- and Agroterrorism Threats: Building a Collaborative Early Warning Culture

Per-Åke Mårtensson, Lars Hedström, Bengt Sundelius, Jeffrey E. Skiby, Armin Elbers, and Rickard Knutsson

Current trends in biosecurity and cybersecurity include (1) the wide availability of technology and specialized knowledge that previously were available only to governments; (2) the global economic recession, which may increase the spread of radical non-state actors; and (3) recent US and EU commission reports that reflect concerns about non-state actors in asymmetric threats. The intersectoral and international nature of bioterrorism and agroterrorism threats requires collaboration across several sectors including intelligence, police, forensics, customs, and other law enforcement organizations who must work together with public and animal health organizations as well as environmental and social science organizations. This requires coordinated decision making among these organizations, based on actionable knowledge and information sharing. The risk of not sharing information among organizations compared to the benefit of sharing information can be considered in an "information sharing risk-benefit analysis" to prevent a terrorism incident from occurring and to build a rapid response capability. In the EU project AniBioThreat, early warning is the main topic in work package 3 (WP 3). A strategy has been generated based on an iterative approach to bring law enforcement agencies and human and animal health institutes together. Workshops and exercises have taken place during the first half of the project, and spin-off activities include new preparedness plans for institutes and the formation of a legal adviser network for decision making. In addition, a seminar on actionable knowledge was held in Stockholm, Sweden, in 2012, which identified the need to bring various agency cultures together to work on developing a resilient capability to identify early signs of bio- and agroterrorism threats. The seminar concluded that there are a number of challenges in building a collaborative culture, including developing an education program that supports collaboration and shared situational awareness.

Per-Åke (Aake) Mårtensson is Senior Adviser at the Executive Office, Coordinations and Operations Department, at MSB Swedish Civil Contingencies Agency, and Senior Adviser seconded to the Swedish National Defence College, Stockholm. Rickard Knutsson, PhD, is Director of the Security Department, National Veterinary Institute (SVA), Uppsala, Sweden. Lars Hedström is Director General, Institute for Defence and Strategic Policy Studies, Swedish National Defence College, Stockholm. Professor Bengt Sundelius is Strategic Adviser, Executive Office, MSB Swedish Civil Contingencies Agency, Stockholm. Jeffrey E. Skiby is Senior Communications Officer, Division of Food Microbiology, National Food Institute, Søborg, Denmark. Armin Elbers, PhD, MSc Ag, MSc PopMed, is a senior scientist and epidemiologist in the Department of Epidemiology, Crisis Organisation and Diagnostics, Central Veterinary Institute (CVI) of Wageningen University, The Netherlands.

Various biological agents such as bacteria, parasites, toxins, and viruses may be deliberately spread through feed, food, water, or air with the intent to cause harm and panic.[1] Therefore, it is important for emergency organizations to understand the threats and consequent risks, and risk intelligence experts have to make agencies in charge aware of these threats and risks. The understanding among organizations is crucial, and actionable knowledge is a concept that is relevant to the everyday world of practice.[2,3] Furthermore, agencies have to have response plans in place and keep their capabilities updated. An awareness procedure for accurate risk and threat assessment, assessment of vulnerabilities, and modeling of bio- and agroterrorism scenarios enables improvements in cooperation among intelligence, law enforcement, public health, and animal health communities: the "one health" concept. Thus, a successful strategy to counter bio- and agroterrorism requires cooperation among agencies that traditionally may have been reluctant to share information.[4] The EU CBRN Action Plan is an example of an effort to improve cooperation among agencies; it includes a generic approach that is appropriate for chemical, biological, radiological, and nuclear incidents (ie, horizontal actions).[5] There is also a need for specific action under each category (eg, specific biological incident actions). In addition to the EU CBRN Action Plan, the EU has a counter terrorism strategy.[6] In Europe, these strategic documents form the basis for early warning and decision making on bio- and agroterrorism threats (Figure 1).

As an example, bioterrorism in the food chain is complex.[7] For multidisciplinary threats such as bio- and agroterrorism, agencies and organizations that respond to these threats need to take a common approach so as to be able to communicate with, understand, and respond to each other. Therefore, preparedness organizations cannot hold on to relevant information, or knowledge and details of a situation. Instead, sharing relevant information among involved preparedness organizations will facilitate the response to these types of threats and risks.

The Stimson Center report *New Information and Intelligence Needs in the 21st Century Threat Environment* says that globalization requires that warning be a part of various analytical processes,[8] 3 of which are explained: (1) warning as a byproduct of daily expert activity, (2) persistent surveillance for a specific outcome with routine reporting, and (3) strategic reconnaissance by looking for early signs of threat and opportunities.[8] In addition to establishing an effective biological warning system, there needs to be an understanding of the existence of a dynamic baseline—that is, what is the normal level of incidence, morbidity, and mortality for a specific disease in a specific area? Too often, baseline data are incomplete because they are collected sporadically, not shared properly, complex, and involve a disease that is understudied or caused by a novel pathogen.

Early warning decision making is complicated. To achieve a coordinated decision-making process, shared situational awareness and availability of coordinated external information must be based on information sharing and

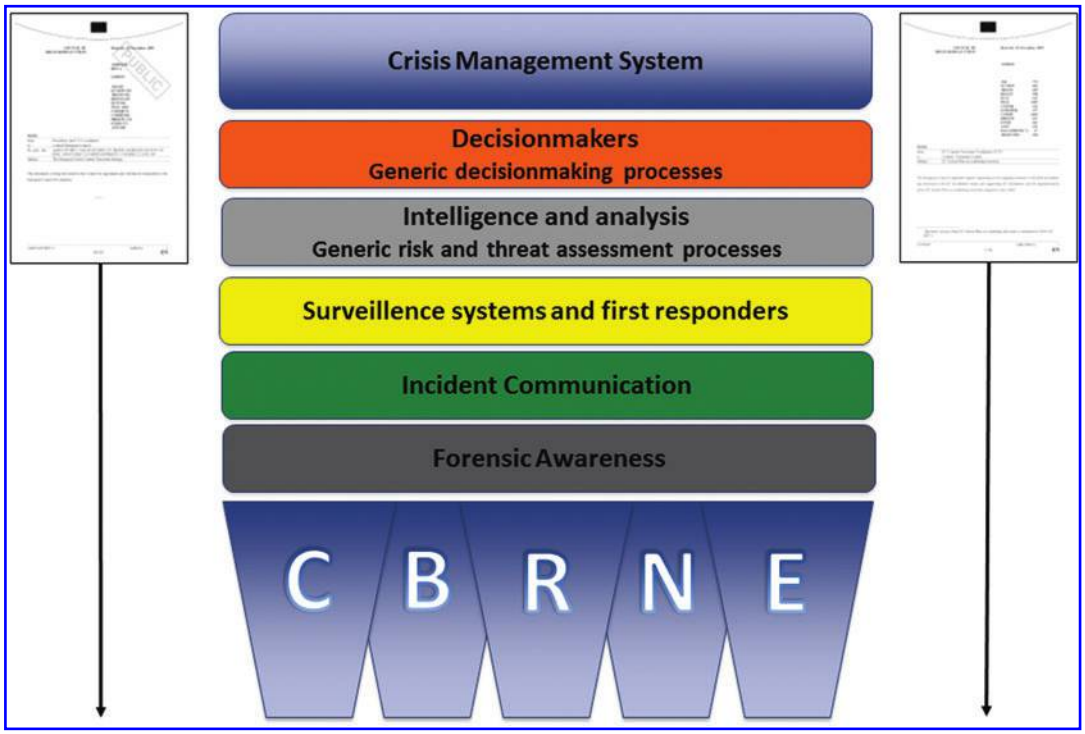

Figure 1. Example of a model illustrating generic measures from the EU CBRN Action Plan. Color images available online at www.liebertpub.com/bsp

actionable knowledge. Efficient "sense making" is important before decision making, followed by "meaning making."[9] Early warning decision making based on signs of early threats requires a strategic planning process and structured analytical techniques.

Strategy Needed

To get to a common approach, a program is needed that includes many levels of education, shared experience, and different tools. In the AniBioThreat project, several of these elements have been developed. One of the 6 work packages (WPs) focuses on early warning (WP3), and a strategy has been generated. The strategy is based on the following 6 strategic challenges:

1. *Cooperation*—Cooperation is needed to improve national and international collaboration. Covert and overt incidents will lead to various early warning and response activities. In a covert incident, which is characterized by an unannounced release, the early detection and consequent warning and response will be driven by public and animal health organizations. But an overt incident is characterized by the fact that the perpetrator claims responsibility, so the response will primarily be law enforcement–driven. Forensic capabilities must be in place in both types of attacks. Cooperation between the relevant agencies is a key requirement for bioterrorism countermeasures and preparedness.[4,10,11]

2. *Surveillance awareness*—Few surveillance systems have been specifically designed for collecting and analyzing data for the early detection of bioterrorism events.[12] Law enforcement organizations need to be aware of passive and active animal disease surveillance, as well as other types of surveillance, such as pandemic surveillance, biosurveillance, and medical intelligence. The public and animal health organizations also need to have a general overview of how the intelligence agencies work. There is a need for at least a minimum level of education and training in surveillance techniques. Collective intelligence and crowd sourcing, such as social media, are also examples of crucial indicators to consider.

3. *Weak signals*—Both in intelligence and disease surveillance, identification of weak signals is crucial because these might be the first signs of a suspect situation (high sensitivity). But because of the generally low specificity of these signs, an agency can be overwhelmed by investigating false-positive signals to exclude the presence of an undesirable pathogen or disease. A framework for computer-supported outbreak detection is a basis for early detection of diseases.[13] Inference-based statistical approaches and Bayesian networks are useful in developing a clinical decision support system (CDSS) for early detection, and they can help to filter signs that need follow up.[14] It is important to have methods for processing large volumes of data, identifying weak signals, analyzing multiple indicators, and accounting for spatial structure.[15]

4. *Keeping abreast of advances and trends in the life sciences*—It is important to be aware of activities in the life sciences—for example, synthetic biology that enables proliferation of pathogenic DNA.[16] Research trends and developments in the life sciences need to be followed up. It is also important to be aware of volunteer communities such as DIYBio (a do-it-yourself community), which operates in more than 30 countries and shares virtual laboratories.[17,18]

5. *Information sharing and communication plans*—From earlier bioterrorism exercises and workshops in AniBioThreat, it has become apparent that a key obstacle is the lack of a formalized cooperation and coordination structure for sharing critical information across disciplines.[4,19] Media management and crisis communication are key aspects, which require communication plans and integrated understanding of new means and forms of information dissemination. The legal framework for sharing information and documents is also a challenge for agencies.

6. *Joint situational awareness and coordinated decision making*—There is a need for a decision-making framework for bioterrorism incidents. Two key phases in such a framework are preevent planning, and incident characterization and initial response.[20] The work is related to Action B.14 in the EU CBRN Action Plan, in which it is recommended that a bio-specific checklist of requirements for consequence management be developed. Therefore, various common operating picture platforms for coordinated decision making are needed (Figure 2).

The WP in AniBioThreat that focuses on early warning is run by partners from 2 EU member states, the Netherlands and Sweden. The national emergency organizations from these countries have identified a need to work closely together throughout the project. This collaboration includes planning how a response to a bio- or agroterrorism attack should be organized. The results of the work will be helpful when judging the current animal disease surveillance system with respect to the detection of an animal bioterrorism attack. In addition, strategies are needed to facilitate the national activities for a future crisis management doctrine or framework based on CBRNE generic measures for coordinated decision making and crisis communication. The work will be integrated and coordinated with the national CBRNE activities, including use of correct terms and improving forensic awareness, training, and exercises. Based on the strategy, 2 questions have been identified:

1. How can links be established among different sectors, such as intelligence, law enforcement, public health, and animal health organizations?
2. How can AniBioThreat reach out to member states to support the national preparedness efforts?

AniBioThreat has an iterative approach to improve awareness among individuals and organizations through the

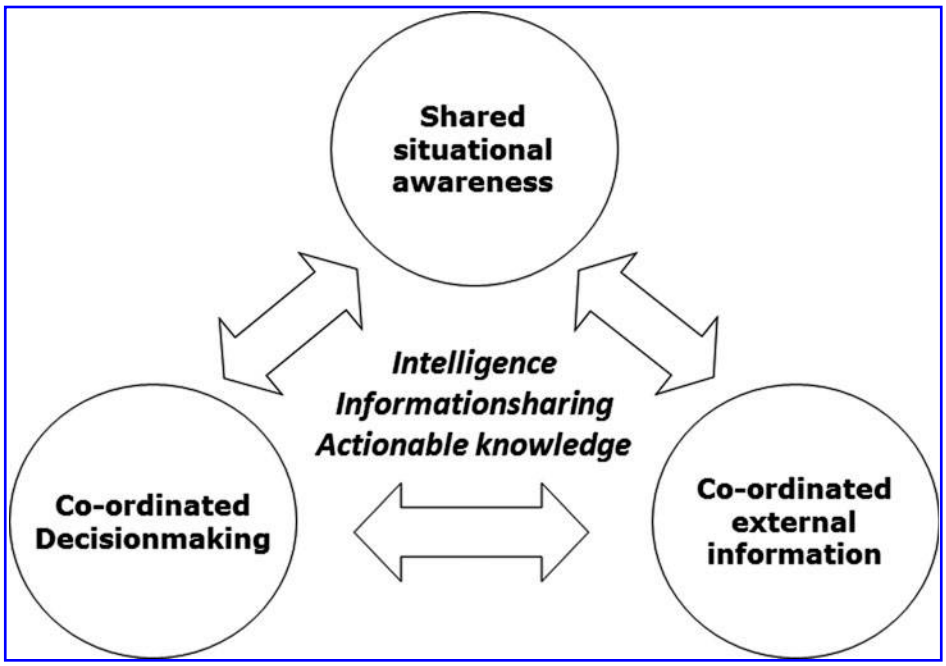

Figure 2. Model illustrating early warnings system and signs of early threats

use of R&D activities, study visits, mobility programs, workshops, training events, and exercises.

Seminar, Workshops, and Table-top Exercise

On November 20, 2012, a seminar on actionable knowledge was organized at the Swedish National Defense College (FHS). Participants from intelligence, law enforcement, and animal health organizations were present, and Ken Knight, Analytical Director at CENTRA Technology, Inc., gave a keynote lecture about actionable knowledge. The purpose of the seminar was to apply the concept of actionable knowledge to strengthen the capability of decision makers and communicators to prevent, prepare for, respond to, and follow up a crisis. The seminar included a small bio- and agroterrorism exercise that used a quad-chart analysis focused on expert identification of the factors most likely to affect the future of bio- and agroterrorism and an analytic process to prompt thinking about the potential consequences of alternative futures. The seminar identified several needs for the future, especially education needs. In addition, the seminar identified awareness and generic core values and principles for individuals and organizations to facilitate a culture that will build collaborative bridges between various sectors and agencies (Table 1).

Table 1. Attitudes Toward Willingness to Work Across Sectors

Core Values	*Core Principles*	*AniBioThreat Core Values*	*AniBioThreat Activities*
Integrity	Objective	**C**ollaborative	Research & development
Competence	Economy of resources	**L**earning	PhD students
Courage	Unity of command	**E**fficient	Study visits
Teamwork	Security	**A**lert	Mobility program
Delegation	Simplicity	**R**obust	Workshop
			Training
		CLEAR	Exercise

The table presents a summary of values and principles presented at the seminar in combination with values and activities performed in AniBioThreat. The 2 left-hand columns depict generic values; the 2 right-hand columns depict core collaborative values and activities that are critical to the AniBioThreat project.

Concerning early warning and decision making, several workshops and smaller tabletop exercises have taken place. Two workshops in decision making concerning bioterrorism prevention and response have been held in AniBioThreat. On March 15, 2012, the first workshop took place in Stockholm. The aim was to gather decision makers from intelligence, law enforcement, and public and animal health organizations to create trust and credibility for future joint interagency activities concerning bioterrorism preparedness. It was a 1-day workshop with 30 participants in which each sector and organization gave oral presentations concerning how to work on information and decision making. Working with a multiagency approach requires bridging mechanisms. The workshop resulted in improved awareness about information cultures in intelligence, police, and animal and public health sectors that will help decision makers to understand the complexity of coordinated decision making before and during a bioterrorism event. Furthermore, the workshop provided insight into the challenges for sharing information, and it was decided to have a follow-up workshop with more hands-on scenarios.

The second AniBioThreat decision-making workshop took place on September 12, 2012, in Stockholm, Sweden, with the same organizations invited as in the first workshop. After an introduction with a follow up from the first workshop, the participants were split into 2 working groups with approximately 15 people in each group. Each group was given a scenario. Group 1 was given an overt bioterrorism scenario in which the perpetrator claims responsibility for releasing a disease-causing agent. The second group was given a covert bioterrorism scenario, characterized by an unannounced release. A deliberate release of a disease-causing agent may not be evident until unexpected illness among animals and humans is recognized. From this workshop it was concluded that decision makers must be trained for both overt and covert incidents.

A table-top exercise was held on November 28, 2012, with decision makers from the 2 previous workshops. The aim of the 1-day table-top exercise was to create a common understanding of how the emergency preparedness system should interact for effective cross-sector collaboration to prevent and respond to a bioterrorism incident. The exercise also aimed to identify, interpret, and apply common generic processes and methods for operational decision making and communication. There are many juridical challenges to handling a bioterrorism incident, and the exercise clearly demonstrated the need for a legal advisory network linked to the decision-making process. The exercise also identified the need for interoperable communication across sectors.

On June 27, 2012, a meeting was arranged in the Hague between AniBioThreat and the National Coordinator for Security and Counterterrorism (NCTV) and the National Crisis Centre (NCC) of the Netherlands. The experiences gained from these activities will be used to develop a bio-specific checklist for consequence management and decision making.

Discussion

Disease outbreaks have a severe impact on public health and the global socioeconomy.[21] Global surveillance and early warning are crucial in preventing spread of disease. "Sense making" applies to all types of crisis management.[9] This was discussed at the 2 decision-making workshops, the seminar, and the table-top exercise in AniBioThreat; all these activities identified a need to improve common awareness about existing surveillance and early warning systems in the various domains. In law enforcement, Interpol has since the beginning of the 20th century reported biological incidents in a "biocrime database."[22] In recent years, Interpol has also produced a report (*BioT Quarterly Report*) covering bio-crimes (intentional) and bio-risks (unintentional).[23] The United Nations Office for Disarmament Affairs has initiated work on developing a biological incident database.[24] In addition to global efforts, there are national efforts for gathering information about bio-incidents in combination with other CBRN incidents—for example, the Australian CBRN database from the Australian Federal Police (AFP).[25]

The AniBioThreat project focuses on bridging security, safety, and research. To enhance global response, we must build bridges between disease surveillance networks and international organizations.[26] There are many animal and public health early warning and surveillance systems in place monitored by organizations such as the World Health Organization (WHO),[27] the Food and Agricultural Organization of United Nations (FAO),[28] and the Office International des Epizootes (OIE).[29]

The complex nature of bio- and agroterrorism threats requires multisectoral intelligence that can be seen as the aggregated competence of a broad range of expertise to make use of a broad spectrum of technologies. Education is needed to circumvent "mental gaps" in awareness about various agency cultures. Training and education on early warning and decision making must be provided at all levels. A special focus should be on how to use available data and how to collectively respond to it. The training and education need to include the following points:

- Warning is meaningless unless it leads to improved decision making, response options, and resilience;
- Warning is a specialized discipline with specialized tools and techniques;
- Warning expertise is required; having only technical or subject matter expertise is not enough;
- To continue with the early warning work in AniBioThreat, there is a need to operate in 3 dimensions: (1) early detection for rapid response, (2) persistent monitoring of known threat scenarios, and (3) horizon scanning for future and emerging threats.

A Word on Warning Expertise

Warning is about generating actionable foresight, in order to improve system-wide decision making, develop better contingency and response options, and increase overall resilience. It involves alerting recipients to potential challenges (and opportunities) with sufficient insight and in sufficient time for them to shape events, prepare more fully for future contingencies, develop and implement mitigation options, and respond to, exploit, and/or more quickly recover from disruption. Warning depends, as much as anything, on an analytic mindset that assumes the next major discontinuity is already taking shape and on analytic processes designed to resolve that hypothesis.

Building effective warning systems is difficult. The nature of surprise—by definition, a deviation from the most likely or expected event—presents an incredible analytic challenge. Experts can spend their entire careers without ever experiencing a major one. Often, the earliest signs of change are weak, fragmentary, ambiguous, and/or contrary to existing assumptions and judgments, making it hard to determine whether the next moment is going to be significantly different from the last. Experts have developed sophisticated analytic frameworks that allow them to process large amounts of information, distinguish the important from the interesting or unimportant, and put major developments into context. They are right more often than not, but when the underlying fundamentals that shape a given subject shift, or new patterns emerge, expert mindsets—culturally encoded by background, education, and experience—can find it extremely difficult to recognize, challenge, and overcome the new situation. This is especially true during crisis situations, when time and other pressures make it problematic to step back and reexamine basic assumptions and analytic perspectives. Perception biases, mirror imaging, molding data to fit what we expect to see, and drawing inappropriate or obsolete analogies are the foundations of surprise.

Effective warning requires analytic systems to identify the processes and patterns that define "normal"; establish information sources, criteria, and metrics to detect (as early as possible) that the situation is moving away from "normal"; and develop and employ sophisticated threshold criteria to determine how far from "normal" things must be before a warning is issued. That means developing an integrated analytic capacity to rapidly synthesize multiple complex factors, proactively engage and apply knowledge from diverse expert sources, and readily employ tools and techniques designed to deal with huge amounts of data, challenge base assumptions, spot emergent patterns and behaviors, handle multiple potential outcomes, and address significant complexity, ambiguity, and uncertainty. Warning professionals can have various backgrounds such as epidemiologists, statisticians, or communicators, but they can also be data analysts capable of working on technical programs on surveillance for bioterrorism[15] and global health surveillance.[30,31]

Building an effective biological event warning system will require the merging of 3 fields of expertise: animal-biological, intelligence and security, and warning. The EU project AniBioThreat currently involves the first 2. It is imperative that warning experts be brought on board to provide the training and knowledge necessary to augment, focus, and synthesize all 3 areas of expertise to build a warning system that can operate across the full spectrum of biological event challenges.

Three-Dimensional Warning Capacity

Deliberate and naturally occurring biological threats pose at least 3 distinct warning challenges, and an effective bio warning system should have 3 elements: (1) early detection for rapid response, (2) persistent monitoring of known threat scenarios, and (3) horizon scanning for future and emerging threats and opportunities. A future goal is a 1-week facilitated training exercise (and 1 or more follow-up events) that will bring together warning, animal disease, and security experts to begin the process of creating a 3-dimensional warning (3DW) system based on the EU project AniBioThreat. Training, facilitation, and 3DW system development will be built around the ideas, concepts, and outcomes outlined below.

Early Detection, Rapid Reporting

Some potential threat issues—an infectious disease outbreak or a bioterrorism attack, for example—put a very high premium on warning system speed because warning-dependent response mechanisms must be quickly implemented if the situation is to be effectively neutralized or contained. An early detection, rapid reporting (EDRR) warning system must provide early detection, accurate event characterization, rapid warning report formulation, and fast, comprehensive dissemination in order to meet recipient response, containment, and recovery imperatives. That means creating a system capable of wide-area monitoring of diverse information sources, and rapid review, processing, and reporting of intelligence and information of all types concerning events of critical interest. EDRR system output would typically consist of descriptive snapshots or summaries that provide real-time or near-real-time alerting and situational awareness (who, what, when, where) and are disseminated to essential decision and response stakeholders with minimal delay. An EDRR warning system would depend on the following:

- Reliable access to all (or as much as possible) relevant information and reporting on developments throughout the area of interest (geographic and/or functional,) regardless of the source;

- Automatic (or near-automatic) data integration, sorting, processing, prioritization, and display;
- Full-spectrum analytic expertise (drawing on diverse expertise across administrative, geographic, and functional boundaries);
- Threshold criteria—either pre-identified or the result of analyst judgment—used to sort critically important from interesting and unimportant information and developments;
- Rapid report generation; and
- Direct communications access to decision and response staff.

Persistent Surveillance of Known Threats

Some biothreat-related warning events would be monitored using a persistent surveillance analytic approach. Planning and preparation for a bioterror attack, or systematic disregard of safety regulations at an animal slaughterhouse, for instance, can theoretically be identified and described ahead of time. Moreover, because these and similar scenarios would play out more slowly over time and involve potentially detectable and/or observable actions, they might be uncovered by an analytic framework focused on systematic change detection. Such a system would start with expert identification of critical parameters—for example, potential perpetrators, likely or historic methods of attack, critical targets, key elements and vulnerabilities in the animal bio infrastructure—and use these parameters to build an information collection and a persistent monitoring capability centered on specific indicators associated with event timelines, actors, behaviors, organizations, facilities, and the like. A generic model of a persistent surveillance of known threats (PSKT) warning system is shown in Table 2.

PSKT warning systems can detect early (albeit ambiguous) indications that the warning event may be unfolding, enable systematic tracking of the situation as it evolves, and generate tactical precision on the pace, scale, and timing of threat developments. Ideally, PSKT warning reports will provide enough information, with enough lead time, for recipients to take decisions and actions to deter, prepare for, and/or mitigate the worst consequences of the event. PSKT warning systems depend on:

- Prior identification of the "bad outcome" (knowing precisely what to warn about);
- Detailed knowledge of warning event dynamics (enough to build chronological timelines [scenarios] depicting how the situation would move from "normal" to "crisis");
- Analyst development of timeline-associated change detection indicators;
- Continual collection of information on critical indicator facilities, processes, entities, and events;
- Systematic monitoring by knowledgeable analytic staff; and
- Continuing interaction between warning analysts and decision makers.

Strategic Reconnaissance of the Emerging Environment

EDRR and PSKT warning systems are less useful for issues that cannot be fully framed or described ahead of time; present little historical context for building timelines, indicators, and normalcy patterns; and cannot be systematically monitored by traditional means—in short, issues that change dramatically or emerge unexpectedly from the complexity and dynamism of today's world. Biotechnology and the nature of terrorism are 2 issues whose dimensions, characteristics, and areas of intersection might evolve along multiple paths at different speeds over time.

Anticipating dynamic, emerging challenges requires analysts to continually scan and probe the environment for undetected or weak signs of change, risk, and opportunity—much like broad area surveillance radar—and be able to meaningfully assess, explore, categorize, and track those over time. This means building comprehensive and enduring analytic processes to systematically examine the forces and factors driving strategic change and identify, assess, and prioritize "over-the-horizon" challenges and opportunities. An effective strategic reconnaissance of the emerging environment (SREE) system should integrate horizon scanning, risk assessment, and other "best of class" futures-oriented analytic techniques to look beyond traditional sources of information and normal time scales, explore ideas at the margins of current thinking and planning,

Table 2. Overview of a Generic Persistent Surveillance of Known Threats (PSKT)

Defining Normal	*Recognizing Important Deviations*	*Deciding When to Warn*
• Baseline threat assessment	• Applying specific criteria to readily distinguish signal from noise	• When new information and analysis changes the baseline assessment
• Identifying threat-related events, groups, individuals, goals, structures, methods of operation, attack means, general targets, etc.	• Keyed to sources, unusual activities or behaviors, consistent or repeated themes, key events, etc.	• When analysts are compelled to convey new judgments regarding likelihood, timing, target, method, scale, etc., of potential events

and examine novel and unexpected issues. Building that system would require at least the following basic steps:

- Identify the most important change agents with respect to political, economic, social, technological, military, environmental, and other sponsor-identified topics of interest;
- Identify the most important sources of information relative to each change agent topic;
- Regularly monitor critical information sources most likely to reflect the emerging stages of an issue's development;
- Apply advanced analytic tools (eg, web content extraction, event data and sentiment analyses, data integration and visualization, decision support, human terrain mapping, and others) and integrate them with more traditional expert-based analytic processes; and
- Have experts regularly review and analyze via clustering, ranking, and voting.

The future training and education needs for involved players in the EU project AniBioThreat will include a focus on (1) generic methodology; (2) creating a collaborative culture, based on a developed formalized strategic analytical working process; and (3) a commonly monitored early warning system based on shared criteria and pre-identified critical factors.

The contribution of a focused education and training activity will be a common collaboration process and working tool for early warning among the involved players. The rest of the AniBioThreat project period will be proposed to be an evaluation of the developed collaborative working process and the early warning system. The training and education program is planned to take place during the end of the project and will be planned within the AniBioThreat project together with American partners. The next step in AniBioThreat is to continue to perform joint education, joint training, and joint exercises. The outcome of the training and education will be presented in the implementation of the EU CBRN Action Plan and also for generic national crisis management systems and homeland security systems.

Conclusion

The actionable knowledge seminar concluded that there are a number of challenges that need to be overcome in order to build a collaborative culture among emergency organizations involved in early warning of bio- and agroterrorism. To support sustainable collaboration and shared situational awareness, specific education programs must be developed. Moreover, shared means for communicating information that may start informally but eventually result in standard operating procedures (SOPs) must be considered. Furthermore, exposure of communities involved in available techniques and tools that can be used for shared situational analysis and early warning is important. The established strategy in AniBioThreat and the early warning WP builds on the development of collaborative processes for what needs to be done. From these collaborative processes, concerning bio- and agroterrorism, it has been concluded that a joint early warning system should be developed that merges methodologies of law enforcement and public and animal health authorities. A common method of education must be set up to develop indicators that can form the basis for early warning. In conclusion, this study provides guidance to build a collaborative early warning culture in order to develop a future workforce that is responsive to unconventional threats.

Acknowledgments

This research was supported by the framework of the EU project AniBioThreat (Grant Agreement: Home/2009/ISEC/AG/191) with the financial support from the Prevention of and Fight against Crime Programme of the European Union, European Commission—Directorate General Home Affairs. This publication reflects views only of the authors, and the European Commission cannot be held responsible for any use that may be made of the information contained therein. We thank Ken Knight, CENTRA Technology, and Mark Polyak, Courage Services, USA, for significant help in preparing this paper and for valuable discussions.

References

1. Wilson TM, Logan-Henfrey L, Weller R, Kellman B. Agroterrorism, biological crimes, and biological warfare targeting animal agriculture. In: Brown C, Bolin C, eds. *Emerging Diseases of Animals.* Washington, DC: American Society for Microbiology Press; 2000:23-58.
2. Argyris C. Actionable knowledge: design causality in the service of consequential theory. *J Appl Behav Sci* 1996;32(4):390-406.
3. Yang K. Further understanding accountability in public organizations: actionable knowledge and the structure-agency duality. *Administration & Society* 2012;44(3):255-284.
4. Trufanov A, Rossodivita A, Guidotti M, eds. *Pandemics and Bioterrorism: Transdisciplinary Information Sharing for Decision-Making Against Biological Threats*. Amsterdam: IOS PRESS; 2010.
5. European Commission. Communication from the commission to the European parliament and the council on strengthening chemical, biological, radiological and nuclear security in the European Unioin - an EU CBRN Action Plan. Council of the European Union; 2009.
6. European Commission. The European Union Counter-Terrorism Strategy. Brussels, Belgium: Council of the European Union; 2005.
7. Knutsson R, van Rotterdam B, Fach P, et al. Accidental and deliberate microbiological contamination in the feed and

food chains—how biotraceability may improve the response to bioterrorism. *Int J Food Microbiol* 2011 Mar 1;145(Suppl 1):S123-S128.
8. *New Information and Intelligence Needs in the 21st Century Threat Environment.* Washington, DC: Henry L. Stimson Center; 2008. http://www.stimson.org/images/uploads/research-pdfs/SEMA-DHS_FINAL.pdf. Accessed July 1, 2013.
9. Boin A, Hart P, Stern E, Sundelius B. *The Politics of Crisis Management: Public Leadership Under Pressure.* New York: Cambridge University Press; 2006.
10. Parnell GS. Appendix D: bioterrorism risk analysis with decision trees. In: *Department of Homeland Security Bioterrorism Risk Assessment: A Call for Change.* Washington, DC: National Academies Press; 2008. http://www.nap.edu/openbook.php?record_id=12206&page=85. Accessed July 1, 2013.
11. Elbakidze L. An economic exploration of prevention versus response in animal related bioterrorism decision making. Doctoral dissertation, Texas A&M University; 2004. http://agecon2.tamu.edu/people/faculty/mccarl-bruce/papers/dissertation3.pdf. Accessed July 1, 2013.
12. Bravata DM, McDonald KM, Smith WM, et al. Systematic review: surveillance systems for early detection of bioterrorism-related diseases. *Ann Intern Med* 2004 Jun 1;140(11):910-922.
13. Cakici B, Hebing K, Grunewald M, Saretok P, Hulth A. CASE: a framework for computer supported outbreak detection. *BMC Med Inform Decis Mak* 2010;10:14.
14. Van der Gaag LC, Bolt J, Loeffen WL, Elbers A. Modelling patterns of evidence in Bayesian networks: a case-study in classical swine fever. In: Hüllermeier E, Kruse R, Hoffmann F, eds. *Computational Intelligence for Knowledge-based Systems Design.* New York: Springer-Verlag; 2010: 675-684.
15. Crubezy M, O'Connor M, Buckeridge DL, Pincus Z, Musen MA. Ontology-centered syndromic surveillance for bioterrorism. *IEEE Intell Syst* 2005;20(5):26-35.
16. Tucker J, Zilinskas R. The promise and perils of synthetic biology. *New Atlantis* 2006;12:25-45.
17. Bennett G, Gilman N, Stavrianakis A, Rabinow P. From synthetic biology to biohacking: are we prepared? *Nat Biotechnol* 2009;27(12):1109-1111.
18. Tucker J. Could terrorists exploit synthetic biology? *New Atlantis* 2011;31:69-81.
19. Danzig RJ. *A Policymaker's Guide to Bioterrorism and What to Do About It.* Washington, DC: Center for Technology and National Security Policy, National Defence University; 2009. https://gfbr.virtualbiosecuritycenter.org/resource_docs/Danzig+-+2010+-+A+Policymaker's+Guide+to+Bioterrorism.pdf. Accessed July 1, 2013.
20. Manley DK, Bravata DM. A decision framework for coordinating bioterrorism planning: lessons from the BioNet program. *Am J Disaster Med* 2009 Jan-Feb;4(1):49-57.
21. Jones KE, Patel NG, Levy MA, et al. Global trends in emerging infectious diseases. *Nature* 2008 Feb 21;451(7181):990-993.
22. INTERPOL. *Bioterrorism Incident Pre-Planning & Response Guide.* 2d ed. Lyon, France: INTERPOL; 2010.
23. INTERPOL. Bioterrorism. Lyon, France: INTERPOL; 2013.
24. *Developing a Biological Database.* New York: United Nations Publication; 2009.
25. Australian Chemical, Biological, Radiological and Nuclear Data Centre. Australian Federal Police website. 2012. http://www.afp.gov.au/what-we-do/operational-support/australian-chemical-biological-radiological-and-nuclear-data-centre.aspx. Accessed July 1, 2013.
26. Linking global disease surveillance networks. Rockefeller Foundation website. 2013. http://www.rockefellerfoundation.org/our-work/current-work/health-systems/linking-global-disease-surveillance. Accessed July 1, 2013.
27. Global Alert and Response (GAR). WHO website. 2013. http://www.who.int/csr/en/. Accessed July 1, 2013.
28. *Manual on Livestock Disease Surveillance and Information Systems.* Rome: Food and Agriculture Organization of the United Nations; 1999.
29. OIE. Animal health surveillance. In: *Terrestrial Animal Health Code.* Paris: OIE, World Organisation for Animal Health; 2010:Chap 1.4.
30. Calain P. Exploring the international arena of global public health surveillance. *Health Policy Plan* 2007 Jan;22(1):2-12.
31. Heymann DL, Rodier GR. Global surveillance of communicable diseases. *Emerg Infect Dis* 1998 Jul-Sep;4(3):362-365.

Manuscript received January 28, 2013;
accepted for publication April 24, 2013.

Address correspondence to:
Per-Åke Mårtensson
Senior Advisor
Swedish Civil Contingencies Agency
Fleminggaten 14, Stockholm
Sweden

E-mail: per-ake.martensson@msb.se