DIMACS Technical Report 2002-39
May 17, 2002

Report on DIMACS Working Group Meeting: Mathematical Sciences Methods for the Study of Deliberate Releases of Biological Agents and their Consequences

by

Carlos Castillo-Chavez
Cornell University

Fred S. Roberts
DIMACS, Rutgers University

DIMACS is a partnership of Rutgers University, Princeton University, AT&T Labs - Research, Bell Labs, the NEC Research Institute and Telcordia Technologies. Affiliate members include: Avaya Labs, IBM Watson Research Center and Microsoft Research

Presented under the auspices of the Special Focus on Computational and Mathematical Epidemiology.

DIMACS would like to thank the National Science Foundation for the support of this Working Group program.

Table of Contents

Preface 3

Biosurveillance 11

Evolution 16

Modeling Bioterror Response Logistics 20

Design of Disease Control Strategies via Mathematical Modeling 25

Challenges for Computer Science 30

Agriculture and the Food Supply 35

Agent-based and Differential Equation Models for Transition Dynamics 44

Appendix I: Program 47

Appendix II: Participant List 52

Report on DIMACS Working Group Meeting:
Mathematical Sciences Methods for the Study of Deliberate Releases of Biological Agents and their Consequences

Preface

Authors:

Carlos Castillo-Chavez, Cornell University
Fred S. Roberts, DIMACS, Rutgers University

Introduction

On March 22-23 at Rutgers University in Piscataway, NJ, a selected group of computer scientists, mathematicians, statisticians, biologists, epidemiologists, NSF and NIH program directors, government health officials and scientific leaders involved in homeland security met at DIMACS.[1] The meeting, which was supported by the National Science Foundation, had as one of its main objectives to explore the potential use of mathematical sciences methods and approaches to the study of the deliberate release of biological agents and their consequences. An additional goal was to catalyze the establishment of working groups with the expertise to investigate the potential uses methods of the mathematical sciences (mathematics, computer science, statistics and operations research) to defend against bioterrorism. This meeting also provided a forum for the identification of additional issues associated with homeland security in which mathematics could play a useful role.

The meeting focused on the identification of the challenges posed by bioterrorism and the potential uses of mathematical methods and approaches to meet them. Twenty short talks laid out some of these challenges.[2] Participants split up into self-selected discussion groups. The results of these discussions were documented through white papers co-authored by the group participants. [3] The potential uses of these documents are multiple: they may lead to follow-on efforts in particular areas identified during this meeting as well as to the identification of areas where expertise is lacking. Furthermore, it is the hope of participants and organizers that the series of white papers included in this document will also help members of the scientific enterprise, funding agencies, health officials as well as those in charge of homeland security establish productive partnerships in the fight against bioterrorism.

Background

CDC[4] in the early 1950's established and developed intelligence epidemiological services. This decision, driven in part by national concerns about the potential use of biological agents as a

[1] DIMACS, the Center for Discrete Mathematics and Theoretical Computer Science, is a consortium of Rutgers and Princeton Universities, AT&T Labs, Bell Labs, NEC Research Institute, and Telcordia Technologies, and is headquartered at Rutgers.
[2] A program is included in an appendix.
[3] The list of all participants is provided in an appendix.
[4] Centers for Disease Control

source of terror, was one of the first systematic responses to bioterrorism. The horror of September 11 and the events that followed have shown that the delivery of biological agents can be carried out by the systematic use of humans or by nontraditional means (mail).

Recent acts of bioterrorism using anthrax have highlighted the use of biological agents as weapons of mass destruction as well as psychological agents of terror. Speculative discussions on the possible impact of the deliberate release of viruses such as smallpox into unsuspecting human populations have taken place from time to time over the years. The possible genetic manipulation of highly variable viruses such as influenza, for which there is not an effective vaccine in storage, and their deliberate release are a source of great concern.

The current national emergency has forced us to consider alternative preventative national and global measures such as vaccination, vaccine dilution, and antibiotic and vaccine stockpiling. Responsive strategies such as the systematic isolation (quarantine) of individuals, buildings, populations and regions, the rapid control of mass transportation systems and the systematic surveillance of food and water supply remain present issues for which mathematical modeling is extremely relevant. Integrated bioterrorist management techniques must be tested and developed with the aid of the most recent computational and statistical methods and tools.

Surveillance approaches have typically been based on the assumption that the problem begins with a single outbreak, a single source, a concentrated focus or a well identified region of infection. There were further advances, for example, when Rvachev and collaborators in the 70's and 80's looked at the role of transportation systems on the geographic spread of the flu and pondered the potential use of transportation systems as a mechanism for the deliberate release of biological agents. Today, the likelihood of multiple and simultaneous releases poses a challenge not only to those in charge of the surveillance and control of unexpected outbreaks but to our national security.

The impact of deliberate releases of biological agents (Foot and Mouth, Mediterranean Fruit Flies, Citrus rust, etc.) on agricultural systems and/or our food supply needs to be addressed and evaluated. For example, Foot and Mouth disease was most likely accidentally introduced in Britain nearly simultaneously at multiple sites via the cattle food supply and agricultural personnel movement. Hence, it was difficult to contain this outbreak despite Britain's effective post-detection response (stamping-out). The costs associated with its containment have been estimated to be over $15 billion.

The use of agents like anthrax highlights the need to look at existing models for the dispersion of pathogens in buildings (models of air-flow in buildings) and in water systems (e.g. dispersion while flowing through pipes). However, new paradigms are needed for the study of releases of these agents in rather unconventional ways. The potential use of communication systems (e.g., mail) for the deliberate spread of lethal pathogens poses formidable practical and theoretical challenges. Hence, the need to model detectors and to develop innovative methods of detection is important. The possible deliberate contamination of water systems raises disturbing scenarios and, consequently, formidable challenges since detection, evaluation and response must be effective and immediate.

Current advances in genomics provide useful tools that could be used to defend against and prevent bioterrorism. DNA sequencing is now routinely used to characterize pathogens' strain phylogenies, a critical step in the identification of potential sources of supply of an agent and, consequently, in the possible identification of networks of terror. In fact, the use of genomics research may allow us to fingerprint and hence document the work carried out at national laboratories and other facilities where scientists work with potentially dangerous biological agents. This sort of research will be of great help not only in forensics, after an attack is over or well underway, but may allow for the development of increased national and international security measures for the handling of biological agents.

Preventing terrorist attacks depends heavily on understanding the subtle and highly unstable social processes that provoke terrorism. Much research is needed in this area. The deliberate release of biological agents is likely to be carried out by sophisticated and highly indoctrinated groups of individuals. The dynamics of these groups (how they are formed and maintained) as well as those associated with the spread of fanatic ideologies (which can be modeled as a serious disease) need to be understood. The survival and reproduction of bioterrorist cells depends on the mechanisms behind these dynamics (for example, the impact of their activities in the local or regional modification of cultural norms). A serious effort to understand and model the dynamics of these groups, their impact on cultural norms and the identification of pressure points is therefore critically important.

Role of the Mathematical Sciences

The mutually beneficial relationship between mathematics and biology has a long tradition. Its impact in the fields of ecology, physiology, epidemiology, immunology, genetics, resource management, the health sciences, to name some key areas, has been well documented[5]. Further development of these methods is stymied by associated difficult computational and theoretical challenges. Progress will require the involvement of computer and computational scientists who have not previously worked in this field. Support and encouragement of computer, and computational scientists and mathematicians who are willing to work in close collaboration with teams of interdisciplinary scientists to address these challenges is of utmost national importance. The current explosions in computer technology and computational methods have resulted in the availability of new methods of potential importance for bioterrorism defense, for instance through an accelerated growth in the field known as computational biology. New types of mathematical methods, for instance those at the intersection of discrete mathematics and theoretical computer science, also hold promise.

An exciting and critical current scientific frontier lies in biology. The events of September 11 have shown that this new frontier must also include sociological and economical concerns in a rather fundamental way. Mathematical methods are the most effective way that we have to make precise some of the efforts being carried out at the intersection of the natural and social sciences that are critical to our national security. This use of mathematical methods should be a natural and fundamental component of the policy decision making process.

[5] *Mathematics and Biology, The Interface, Challenges and Opportunities*, Simon Levin, ed., NSF PUB-701

The marriage between mathematics and some sub-areas of the social sciences is not as well established as that between mathematics and biology. Further interactions between sociologists and economists and mathematical and computer scientists need to be fostered if we are to increase our understanding of the structure and dynamics of social networks/social contacts**,** a critical piece of any bioterrorism attack response plans. Understanding and modeling the spread of and support for opinions or ideologies that underlie terrorism is a vital job that falls at this interface as well.

The policy and economic issues associated with globalization have increased the impact that local and global perturbations may have on otherwise stable communities. Furthermore, the time scales at which their effect operates have dramatically accelerated. Influenza epidemics travel around the world at an increasing pace. The economic impact of the national economies of countries like Argentina, Brazil, Canada or Mexico may impact our own economy "instantly." Globalization and the possibility of isolated or systematic bioterrorist acts have increased the demand for the development of theoretical and practical frameworks that anticipate, prevent and respond to acts of destabilization. Theoretical frameworks and the development of models that respond to specific focused questions are essential. These models will be useful in the identification of key pressure points in the system, to test for robust system features, and to look at the importance of system modularity and redundancy in addressing threats to various system components. The use of models is not limited to the biological sciences but in fact their use must be deeply connected to the social, behavioral and economical sciences. For example, the impact of bioterrorist acts on national and cultural behavioral norms has to be of great concern to those in charge of our national and homeland security. The destabilization of national cultural norms could make unacceptable population and behavioral risks not only acceptable but also pervasive. The consequences of such instabilities are obvious from the wave of suicide/homicide bombers in the Middle East.

Mathematical models have been widely used by government and industry; for the development of economic policy, transportation planning, logistics, scheduling, resource allocation, financial**,** health and military planning and forecasting. Mathematical models are at the heart of many of the decisions made in these and related areas by such federal agencies as Transportation, Commerce, Defense, Energy, Centers for Disease Control, to name a few, and in the private sector in industries such as airlines, oils, biotechnology, financial, etc.

The efforts to guide the fight against bioterrorism that are based on the intuition of experts, while invaluable, may indeed be insufficient. The levels of complexity associated with the multiple facets involved in the fight and planning against bioterrorist threats are paralleled in current biological research. For example, components of host-pathogen systems are sufficiently numerous and their interactions sufficiently complex that intuition alone is insufficient to fully understand the dynamics of such interactions. Experimentation or field trials are often prohibitively expensive, unethical or impossible. Furthermore, there are no real data to validate most hypotheses of interest. Thus, mathematical modeling has become an important experimental and analytical tool of the policy maker. Models, just as they have done in the biological and environmental sciences, will help our efforts to fight bioterrorism. They will sharpen our understanding of fundamental processes; allow us to compare alternative policies and interventions; help make decisions; provide a guide for training exercises and scenario

development; guide risk assessment; aid forensic analysis; and help predict or forecast future trends. .. The use of mathematical models to help in the fight against bioterrorism is not only natural but so critically important that several groups have already began to apply them in urgent policy decisions (e.g., in the recent smallpox vaccine discussions).

The use of mathematical models and methods to fight bioterrorism does not have to be developed from scratch. A wide variety of tools are available in the mathematical sciences as well as a wealth of modeling approaches that have been developed in the natural and social sciences. These methods and approaches provide a natural starting point for the use of quantitative methods for homeland security and defense.[6] The key is to make policy makers aware of the wide variety of mathematical sciences tools that are already available. Approaches that include mathematical components will be extremely useful as long as there is a national effort that promotes, supports and fosters partnerships between modelers and policy makers and between mathematical scientists and epidemiologists and public health professionals. This meeting was designed to play the role of catalyst in this direction. An important message coming out of our meeting is that the appropriate modification of existing methods as well as the blending of new approaches with old ones will go a long way in preparing for the fight against bioterrorism and its consequences. The researchers involved in this project endorse the view that it is essential to create and support the required mechanism that will make effective use of the talents of the mathematical sciences community in this critical area of homeland defense.

White Papers

In all, seven discussion groups met and prepared white papers[7], emphasizing challenges for the mathematical sciences in bioterrorism defense.

The *Biosurveillance*[8] Group focused on sources of data, data mining, and on the development of technology and methods that would facilitate the quick identification of threats or attacks. The group emphasized the importance of three steps: data collection, analysis, and reporting. The group emphasized the fundamental challenge of dealing with the twin goals of rapid detection and preservation of privacy.

The *Evolution* Discussion Group[9] stressed the fact that models of evolution can advance the analysis and understanding of transmission systems in several ways. In the context of bioterrorist threats, they can help identify the source of agents in bioterrorist events. The fitting of transmission models of common infectious agents was identified as an important step in the estimation of parameters.

---

[6] SIAM's 50th anniversary meeting will feature three special sessions organized by Castillo-Chavez, on the use of models in homeland defense. The DIMACS "Special Focus" on Computational and Mathematical Epidemiology will feature numerous workshops and working group meetings at which mathematical scientists will team with biological scientists, epidemiologists, and public health professionals in the use of quantitative methods in homeland security and defense. This workshop was the first event totally dedicated to homeland defense

[7] While minor editorial changes have been made or recommended, for the most part, we (CC and FR) left the content of these white papers to the entire discretion of the members of each group. When agreement was not total dissenting views were sometimes noted by the group itself in their white paper.

[8] Facilitator, Marcello Pagano, Harvard University

[9] Facilitator, James Koopman, University of Michigan

Knowledge of the ranges of such parameters may help differentiate natural versus man-driven events.

The discussion group on *Modeling Bioterror Response Logistics*[10] focused on responses to a major bioterrorist attack. This group stressed the importance of logistic modeling in planning of two types: structural level (pre-attack) and operational level (during or after an attack), and noted the importance of logistic models of distribution, inventory, scheduling and manpower.

The group discussing *The Design of Control Strategies*[11] focused on the use of models as tools for public policy decision making. The context for such models included: agent release, spread, detection, analysis (modeling), advice, and action. It was noted that models may help prepare for possible terrorist attacks, as well as to aid in responding optimally in real-time. This group identified the nature of the threat and response as well as human behavior as critical components in the design, evaluation and implementation of any policies.

The *Computer Science*[12] Discussion Group identified challenges for the computer sciences in six areas: simulation and virtual environments; database policies and information exchange; intelligence and detection; fault tolerance; consequence management; and computational molecular biology.

The *Agricultural Study Group,*[13] whose work was driven by concerns about agriterrorism, focused on forestry and aquaculture as well as on food and the food industry. Economic, health and safety, social and vulnerability issues were addressed in a broad context. Mathematical challenges identified included ways to model multiple attacks across large geographic regions; the application of methods of risk analysis to calculate the degree to which various sectors of the food industry are vulnerable to agriterrorist attack; and the development of mathematical models to determine the cost effectiveness of deterrence strategies that depart from current agricultural practice.

The *Agent-based and Differential Equation Models for Transition Dynamics*[14] Discussion Group identified key simulation scenarios for which agent-based and differential equation models can be combined to address critical strategic policy and planning issues. Associated with the threat of bioterrorism, this group focused on highlighting the importance of model robustness, complexity, sensitivity and modularity in model building.

Concluding Remarks

One of the highlights of the meeting was the remarkable interest in and willingness to communicate among the participants from many different disciplines. Participants in this meeting stressed the importance of absorbing the fact that we are facing a truly new paradigm.

[10] Facilitator, Ed Kaplan, Yale University
[11] Facilitators John Glasser (CDC) and Ellis McKenzie (NIH)
[12] Facilitator, Fred Roberts, Rutgers University
[13] Facilitator, Simon Levin, Princeton University
[14] Facilitator, Mac Hyman, Los Alamos National Laboratory

Effective approaches to dealing with the new reality will require truly interdisciplinary efforts and bold new initiatives.

The fact that perpetrators of bioterrorism on the one hand and politicians, scientists, health and government officials on the other have a different set of cultural norms was highlighted as a major barrier to our mode of thinking, operating and reacting. The ability to plan under shifting bioterrorist cultural norms was highlighted by all participants.

The theory developed by those working in mathematical epidemiology, while effective, has been carried out in a setting that does not allow for experimental verification and validation in typical scientific fashion. Furthermore, epidemics have been studied under the assumption that they are natural phenomena. The same ethical considerations that apply to epidemiological research also apply to research associated with bioterrorist threats. We are left with no recourse other than the use of mathematical models in strategic ways.

Furthermore, it was clear that current mathematical paradigms have to be modified to include the potential deliberate release of pathogens under conditions (critical pressure points) that are likely to cause the most damage and destruction to human populations. This is a different way of thinking and, consequently, it is not part of traditional mathematical epidemiology.

In general models should be initially used to identify worst case scenarios, to identify critical pressure points in systems and to provide scenarios that are likely to increase our understanding of the possibilities and dangers. Mathematical models or approaches must nevertheless be evaluated by a community of experts and by the wealth of methods that have been available in fields like epidemiology, ecology, transportation science, and military logistics. Sensitivity analysis to model assumptions and model robustness should be applied whenever feasible and a variety of group efforts and alternative approaches should be encouraged. Models should be used as an aid in the development of policies, approaches and defense systems that help anticipate terrorist attacks. Therefore, the issues associated with modeland system redundancy and the importance of system modularity need to be systematically addressed.

There was considerable discussion of the game-theoretic aspects and deterrence effects of revealing response strategies in bioterrorist defense. It was in this context that the need for new mathematics, new computational approaches, new models, and new paradigms was discussed.

It was clear to participants that current models and efforts did not systematically consider the impact of deliberate biological releases by humans who have access to some of the same information that we have. Moreover, making information available to potential adversaries was a source of concern to the participants in the meeting.

Issues of homeland security and defense have brought into sharp focus the importance of interdisciplinary research and the critical responsibility that we have to foster joint research efforts in fields that have previously communicated in a peripheral manner. Mathematical sciences provide the language needed to open, enhance and support the channels of communication required for this effort.

[15] Institute for Mathematics and its Applications, University of Minnesota

The working group coorganizers were delighted with the response of the participants and appreciated the hard work of all involved. We hope that the white papers included in this report will help stimulate further discussion, expansion and clarification of the issues raised by a distinguished group of members of the scientific community. We also hope that the content and questions raised by these white papers will lead to expanding partnerships among the participants and their colleagues both through continued activities of this working group and in the broader community.

Finally, it must be noted that by its own nature, this effort was the result of the participation of a selected group of distinguished scientists. Many who were invited could not join us. Furthermore, our own limited knowledge of the issues associated with bioterrorism limited our choice of invitees. We apologize for the obvious and not so obvious omissions.

[16] Mathematical Sciences Research Institute, UC Berkeley

Report of the DIMACS Discussion Group on Biosurveillance

Group Members

Marcello Pagano, Harvard University (facilitator)
Sankar Basu, IBM
Marco Bonetti, Harvard University
Drew Harris, University of Medicine and Dentistry of New Jersey
Richard Heffernan, NYC Department of Health
David Madigan, Rutgers University
David Ozonoff, Boston University (writer)
Henry Rolka, CDC
David Rosenbluth, Telcordia Technologies
Daniel Wartenberg, University of Medicine and Dentistry of New Jersey

Introduction

Surveillance is a core function of the public health infrastructure, used for policy, planning, evaluation and timely response to evolving health problems in the community. Surveillance is an ongoing activity that relies upon indirect and coarse-grained data, less for specific research purposes, than for the direction of administrative objectives. Surveillance data plays an important role both in the guidance of public health policies, planning, and evaluation, and in the detection and recognition of important public health events and trends. The value of monitoring the health of the populace and of establishing norms arises from the use of these activities in detecting and recognizing deviations from these norms. Moreover, once an epidemic has been recognized, data gathered from a surveillance system enables the characterization of the epidemic and the formulation of a response. The value of surveillance systems is highlighted by examining the consequences of lack of monitoring in those places around the world where surveillance is poor. Despite their basic importance to public health, surveillance activities and research are chronically underfunded and consequently attract little academic interest.

Concern about naturally emerging or criminally instigated infectious disease outbreaks have renewed interest in surveillance as one of the first lines of defense in protecting the community. Both in the efficacy of treatment and, more importantly, in preventing spread of an infectious disease or further exposure to a chemical agent, “time” is the enemy. Days or hours are the time scale that matters here, not weeks, months or years, the scale of usual surveillance activities.

Given the limitations of current surveillance systems and the need for response on such a short time scale, two important questions were asked with respect to applications of mathematics to surveillance: Could new mathematical techniques be used to enhance the utility of existing systems? and Could new mathematical techniques be used to design or devise new surveillance systems useful for detecting emerging infections or bioterrorist events?

The group considered the low signal-to-noise problem in the detection of a disease outbreak (for example in the case of anthrax or smallpox) and the role of the astute clinician in the conventional medical care system in detecting such weak signals. Detection of rare events by a

clinician requires that diagnostic evidence raise the probability of the existence of the rarity above threshold in the mind of the clinician. Several factors work against this probability being raised above threshold. Many diseases have non-specific symptoms or share symptoms with common illnesses (for example anthrax shares many symptoms with the flu). Another factor is the rarity of bio-terrorist events. Any surveillance system with any appreciable transaction cost connected solely with such occurrences would soon wither from lack of financial support and fading interest from those who collect the data.

The fact that the only two documented bioterrorist events in this country prior to the recent anthrax attacks both involved more common infectious agents, *Salmonella* and *Shigella* (each important in their own right as food- and water-borne pathogens of public health importance), coupled with the non-specific symptomology of many of the rarer bio-terrorist threats, implies that routine surveillance systems may need to raise initial alarms to ambiguous signals (such as an increase in "flu-like" symptoms) that would then require further investigation. It thus seemed to the group that the most reasonable application for mathematical applications would focus on timely and more accurate detection of common infectious, acute and chronic outcomes already the focus of existing or envisioned surveillance systems rather than new systems specifically designed to handle rare bio-warfare agents like anthrax, Q fever or tularemia[17]. This conclusion is based both on the likelihood of being able to design a feasible routine system that provides the kind of needed response and the principle that a dual use system—one that is useful in normal times as well as times of crisis—is the most practical strategy.

The group abstracted the activities of a surveillance system into three components: collection, analysis, reporting.

Data Collection and Reporting

In a true surveillance system (as opposed to a special purpose or research data collection system) data collection is continuous, routine and stretches into the indefinite future. The occurrences that are registered and transmitted to the system happen in time and space so the different patterns and scales of those events and their transmission to and through the system might be amenable to analysis using a variety of mathematical techniques already available in other fields. For example, keeping track of sales and inventories is a common problem that has been handled with techniques from operations research and computer science, as is the problem of fault detection in computer networks and fraud detection in the use of credit cards. Having a "real time" picture of the state of the system would be an important objective for many uses of a surveillance system and increase its utility across the board. This could also encourage an existing goal of many public health systems today, the use of real time reporting for things like emergency department volume, HMO visits or fulfillment of certain kinds of indicator prescriptions or sales of over-the-counter drugs.

The group spent considerable time brainstorming various usual and unusual sources of data that might be employed in a surveillance system, including data designed originally for billing purposes, pharmacy data, 911 rolls, emergency departments, grocery, quantity of calls to MD

[17] Of course, surveillance at military installations or during military campaigns will not fit this general scheme. Biosurveillance in the military is critical and its planning requires reliable intelligence reports.

offices, cancelled dentist appointments, nurses hotlines, poison control centers, school absences and similar sources. More unconventional sources might be records of hits to certain web sites relevant to the symptoms of interest. More important than the specific sources, however, was the possibility that certain kinds of mathematical techniques might suggest new kinds of data that could be exploited for surveillance purposes, for example, by showing how many different kinds of data could be combined in real time to yield information not obtainable by any one separately. This might be done by conventional multivariate methods of statistics or through pattern recognition algorithms generated in computer science and discrete mathematics. Use of cluster analysis or mathematical taxonomy techniques might allow definition and detection of syndromes that would signal an emerging epidemic or unusual cluster associated with a biowarfare agent. Moreover, combining outcome data with networks of environmental monitors or sensors might be a particularly useful way of early warning that could rescue some warfare agent specificity with the requirement for routine and dual use of the outcome data. Thus in a Bayesian system routine and noisy outcomes in the context of environmental data might allow a much earlier warning than outcome data alone by changing the prior probability of an event. It is not always clear, however, that adding additional data is a benefit if the extra data does not carry pertinent information. In that case it only adds to the noise, not the signal. Selecting useful ancillary data to combine with health outcome data will require close collaboration among biostatisticians, mathematicians and experts in biology, environmental science and epidemiology. Each data source captures specific populations or at least has its biases. New research is needed to eliminate such biases.

Discussing wearable devices to track health status of a selection of sentinel individuals, or sensors (e.g. microphones) or biosensors in public spaces to detect unusual coughing or sneezing, for example, inevitably brings up issues of informed consent. Indeed, data which might be extremely useful for surveillance purposes is often not available because of privacy concerns. The group felt that it was worth exploring the extent to which mathematical approaches might be used to mask identities and thus possibly make more data sets available. Economic incentives might also be explored to encourage the flow of information. Overall strategic issues need to be studied, perhaps using game theory.

The question of what kinds of information, its cost and its uncertainty or accuracy, are matters that are amenable to modeling. In some cases information models are available that would enable estimating the value of earlier detection, as in the recent case of post-exposure prophylaxis for anthrax exposure. In other cases, models might show what kinds of information yet need to be developed to allow such determinations and thus enable better decisions for future surveillance systems. Modeling could also be of value for designing a fault tolerant system that provides needed information for command and control (for example, who is affected, who are their contacts, what is the likely pattern of spread, where are they located, when were they affected, etc.).

The group noted the value of multi-purpose systems. (For example, surveillance of asthma, injury, violence, etc. have a synergetic relationship, thus adding value.) Multiple data sources are also useful, but they may complicate the system to such an extent that they depreciate its value. A two-stage approach could be useful: If a signal is picked up in an unlinked dataset, then one could go to other datasets or activate a full-scale, multiple source surveillance system.

Analysis of Collected Data

The group suggests that a "data warehouse" that provides a single portal for a variety of relevant information for surveillance and interpretation of surveillance data would be useful. This would be a dataset of datasets that could combine real time environmental data, surveillance data of various kinds, administrative data (such as census information and health service resources) and other datasets of interest to those who must interpret and act upon surveillance data. Use of relational database technology or distributed database techniques could be helpful. The group believes any such Information System should adhere to an Open Source philosophy so workers could understand and improve the kinds of information provided.

Use of multivariate and pattern recognition techniques noted in the section on what data to collect are clearly relevant for analysis and the remarks in that section are pertinent here as well. The simultaneous analysis of multiple data sources is a multivariate stochastic model problem about which there is relevant biostatistics research. Questions of how to combine information from many sources might also be looked at from the computer science perspective where the same problem is faced in many different disciplines.

Finally, the group believes that providing typical and publicly available "real" dataset or datasets to the research community would be an important step in allowing researchers to develop and test new methods of analysis and interpretation[18]. The use of current data, such as the NYC ED data, and historical data are worth considering in this regard.

Reporting and Using the Surveillance Results

A surveillance system is embedded in a larger command and control system. No surveillance system is useful if the results aren't or can't be used. Mathematics can have a role in considering various architectures for command and control, explicitly considering the surveillance system as a component part. The vulnerabilities of the system and the role surveillance plays in those vulnerabilities is an important question. It could be helpful in deciding what kinds of information get reported and to whom.

The problem of false positives and false negatives and their costs is also important and will depend on how the information is used and where it fits into the sequence of actions. High false alarm rates are not only costly but can easily lead to the abandonment of the system or disregard of accurate information. Use of ROC curves might be helpful in analyzing this problem and for the question of where to set thresholds for optimal effect.

Modes of presentation of the data for line personnel, policy makers and support staff is also a problem which needs attention. Among the ways the group discussed were maps, color-coded alerts, and other visualization tools, some fairly sophisticated, from the theoretical computer science literature. Reducing complex quantitative information to easily assimilable form is an urgent task. Such techniques must reveal pertinent information while not misleading. Research

[18] Giving access to data to researchers has proved useful in genomics research.

needs to be performed to make this transmission of information as powerful, understandable and accurateg as possible.

Summary

The group considers that even in a cursory consideration of the surveillance problem there are many places where mathematical techniques, both conventional and those under development in other areas, might be helpful. In particular, it suggests that it might be useful to survey applications of discrete mathematics, computer science and operations research as they are now researched and used in other areas such as inventory control, bad credit or fraud detection or weather forecasting, to find new techniques for use in surveillance.

Report of DIMACS Evolution Discussion Group

Group Members:

James Koopman, University of Michigan (Facilitator)
Donald Burke, The Johns Hopkins University
Peter Merkle, Defense Threat Reduction Agency
Mel Janowitz., Rutgers University
Irene Eckstrand, NIGMS – NIH (Rapporteur)

Evolution is an aspect of infection transmission systems. Agents and hosts evolve as a result of their interactions in the system. An important view of such evolution, however, is a view of the evolution of the transmission system and not just the agent or the host. Many models of transmission systems achieve their objectives while ignoring such evolution. But models that look at evolutionary process at the level of the system can advance the analysis of transmission systems in several ways. Relevant to bioterrorist threats, they can

1. Help identify the source of agents in bioterrorist events.
2. Help fit transmission models of common infectious agents so as to
    a. Better differentiate a bioterrorist dissemination of agents from a natural dissemination of agents
    b. Better prepare public health services to diminish circulation of either naturally disseminated or bioterrorist disseminated infectious agents
3. Help predict the evolution of bioterrorist infectious agents with regard to transmissibility, pathogenicity, immunogenicity, and antimicrobial sensitivity.

Source Identification

With regard to the first area of identifying the source of agents in bioterrorist events, phylogenetic models play a key role by indicating past history of the infectious agent spread through bioterrorism in relation to its evolution from known strains. The determination of the source of the anthrax in the recent bioterrorism incident is a case in point. Phylogenetic models first help to identify the subtype of the organism and thus narrow the search. Since the organism encountered has been cultured between the times it was passed from lab to lab, phylogenetic analysis also has the potential to indicate which lab the organism is coming from. Admittedly that requires extensive sequencing to find SNPs occurring at the rate of 10^{-8} per replication. But in this case, that is very much worth the effort.

Particular needs in improving phylogenetic analysis models include models capable of including more causal model structure while examining high numbers of specimens. Also needed are better models of crossover and models that can be used for crossover detection. Also, models that can better estimate phylogenetic distances in the presence of crossover are needed. Once secondary transmission from multiple foci of a bioterrorist spread agent has occurred, good phylogenetic models should help to better pin down the times and numbers of cases directly caused by bioterrorist dissemination rather than by secondary transmission.

Transmission Model Fitting

With regard to the second area of fitting transmission system models to data, the role of phylogenetic models can help specify transmission dynamic history because the fixation of evolved population variation results from the bottleneck events of transmission. Within any host, infectious agent evolution leads to variation around consensus nucleotide patterns related to the agent that started the infection. Transmitted agents come from a part of that variation that most usually establishes a new but related consensus pattern in the new host. The pattern of consensus sequences or the distribution of sequences in different hosts allow for inferences with regard to transmission distance between agents isolated from different hosts.

Thus phylogenetic (or in this case of within species analysis more appropriately "genealogic") distance to the most recent common ancestor parallels transmission distance to the most recent common ancestor. Each infection transmission system model implies different patterns of transmission distances between the infectious agents isolated from infected individuals at different times. Thus competing models of a transmission system can be compared to actual data on genealogic distances to see which better fits observations. Also, when one model form is selected, the pattern of observed genealogic distances can be compared to the pattern of model predicted transmission distances for the purpose of estimating model parameters.

A particular area of mathematical investigation needed here is the elaboration of how virus dynamics within the host and the number of agents involved in transmission events affect the relationship between genealogic distance and transmission distance to the most recent common ancestor. The classic model of Rogers and Harpending is a bare beginning for what needs to be done.

Patterns of transmission distances will be particularly valuable in distinguishing models of bioterrorist dissemination from models of natural dissemination. This distinction should be an immediate task when a new infectious agent emerges and one cannot be sure if the enhanced virulence of that agent arose naturally or artificially.

The use of genealogic distances to model the logistics of response to a bioterrorist event depends absolutely on studies of natural transmission. After a bioterrorist event has occurred, it is too late to undertake such studies. It is before the bioterrorist event that such studies need to be employed on natural transmission events. Genealogic distances should be used to fit transmission system models for airborne and enteric infections at local, regional, and national levels. Particularly useful agents to study in this regard are influenza and caliciviruses. RSV and rotavirus studies may also be very valuable. The local, regional and national models of these agents should be adapted to natural history of infection and immunity parameters of the involved bioterrorist agent and to initial immunity and bioterrorist source conditions.

Predicting Evolution of Bioterrorist Agents

The pattern or "network" of contacts that can transmit infection are a key determinant of infectious agent evolution. Socio-economic change, population growth and population mobility

(travel) are changing contact patterns in ways that affect the evolution and the evolvability of infectious agents. For some kinds of contact, such as airborne transmission, contact patterns are becoming denser and more capable of sustaining altered infectious agents until they can adapt enough to better sustain their circulation with more usual levels of contact. In these cases there can be a "compression of genome space" in the sense that increased opportunities for genetic exchange accelerate the exploration of genome space. For some kinds of contact, such as fecal oral, hygienic improvements are diminishing the network connections that sustain transmission and permit evolutionary adaptation. Obviously, characterization of the social landscapes and social landscape dynamics and their role in disease evolution are central.

The impact of contact dynamic networks on disease evolution is quite relevant. The issue of the evolution of virulence in the case of enhanced bioterrorist organisms is critical. In most cases, virulence enhancement will decrease transmission fitness. Thus the chances of the virulence-enhanced agent becoming endemically established may be diminished. But high transmission environments will increase the opportunity for the bioterrorist organism to adapt and thus increase its transmission fitness. Priority should be given to bioterrorist agent control in these settings. A clear analysis of what these settings are should be pursued with studies on the detailed transmission dynamics of naturally circulating agents. It will be too late once a bioterrorist event has occurred to identify these settings.

For this purpose, models of virulence and its effects on transmissibility are particularly important. Such models must link infection dynamics within the host to infection dynamics at the population or **community** level (higher level of organization may be required in a globally connected society). Such linkage can be sought using brute computational force or by identifying simple algorithms or mathematical principles that facilitate this linkage**.** The integration of game theory or other decision approaches and models into transmission system models and policy seems like a promising direction.

Relevant to this area in general are the models being developed to assess the evolution of antimicrobial resistance. They are relevant not only to the issue of adaptation of virulence enhanced organisms but also to combating bioterrorist agents that have been engineered to be resistant to antimicrobials.

A key area for all infectious agent evolution models is how to include a wide variety of cross-reacting strains of infectious agents in a model. Evolution almost always takes place in such a context and to assess evolution, evolved strains must be modeled separately from source strains. In most transmission system models, the number of strains increases model complexity in a highly exponential fashion. Some efforts that involved the development of models that incorporate crossimmunity (influenza) or increase susceptibility have been carried out but additional theoretical and mathematical work is needed.

Specific Mathematical and Computer Science Challenges

The previous discussion has identified the following needs:

1. Better within host infection models that can provide a base for understanding any new agents that might appear as well as helping to better model infection transmission systems
2. Models relating within host infectious agent dynamics to transmissibility
3. Models relating transmission events to genealogic distances
4. Better models for calculating genealogic distances, especially given crossover
5. Transmission system models with multiple cross-reacting strains
6. Game theory based evolutionary models that can be integrated into infection transmission system models

Other mathematical issues affecting evolution to be addressed include

7. How network models relate to compartmental models
8. How scalability issues of network structure affect transmission dynamics
9. Optimization models for epidemiological study designs

Concluding Comments

Evolutionary models on networks can be very complex but can be computationally more efficient than complex compartmental models that assume mixing in broad contexts, especially when multiple strains are involved. It seems that finding ways to integrate network and compartmental modeling approaches will help all areas of infection transmission system modeling, including models of evolution.

Recently there has been interest in human contact patterns that may be non-scalable and therefore have quite different properties than those predicted from compartmental or lattice type models. Internet connection models have especially kindled this interest. While we felt that on some dimension all infection transmission contact networks had to be scalable because they all have strong geographic and social space determinants, the issue of risks of very large epidemics should be addressed in terms of network scale.

The final issue relates to the fact that ongoing surveillance systems that elucidate transmission dynamics are essential to bioterrorist control in general and to the risks of evolution in general. Surveillance systems should be established on the basis of continuous quality improvement from analysis of data using a transmission system model as the base. For this to be the case, models that can define the optimal sets of data to be collected either on a routine basis in the system or in special studies that will help solidify the surveillance system are needed.

In conclusion, efforts to integrate research in immunology (within host infection models), recent advances in genomics and molecular biology in the context of social networks interactions, and the impact of social landscape structure (at various scales) and their dynamics are critical to disease evolution. The challenge, common to many mathematical efforts, lies not only in this direct question but also in the associated inverse problem, namely, how can we use system transmission information to characterize pathogens' evolution in natural as well as in human-induced (bioterrorism) epidemics.

Report of the DIMACS Discussion Group on Modeling Bioterror Response Logistics

Group Members:

Edward Kaplan, Yale University (Facilitator)
Douglas Arnold, Institute for Mathematics and its Applications, University of Minnesota (Rapporteur)
David Banks, FDA
Joseph DiPisa, Rutgers University
Richard Ebright, Rutgers University
Teresa Hamby, NJ Department of Health and Human Services
Jon Kettenring, Telcordia Technologies
Moshe Kress, Ctr. for Military Analyses (CEMA), Israel (writer)
Lone Simonsen, NIAID – NIH

Motivating Philosophy

The group felt that the following points were essential to remember:

- Logistics planning and operations will be a major factor in the outcome of a terrorist attack.
- Proper logistics modeling can have a major impact on logistics planning and operation, and thus on the outcome of an event.
- Logistics is just as important as epidemiology ("what we do to smallpox versus what smallpox does to us").
- Logistics/operations modeling has been employed and deployed successfully in disaster planning, military, manufacturing/supply chains, many industries, urban services, etc.
- Logistics modeling is intended to support decision making at two levels:
  (a). Structural (or policy) level decisions made in advance.
  (b). Operational (or real-time) decisions taken during an event.

Modeling is a crucial component of logistics planning and operations. Models are mathematical/computer constructs to represent realistic scenarios. Such models guide thinking and provide insight; predict consequences of different decisions in different scenarios; identify key operational variables, system bottlenecks (e.g., maximum vaccination rate, quarantine capacity), critical paths, and so forth.

Models help frame decisions. They can be used to determine a set of policy options. Models can be used to estimate the consequences of these options (e.g., in terms of cases of disease, deaths, economic loss, damage to infrastructure, etc.).

The ultimate consumers of models are decision makers. Models must be "good enough" to distinguish between policy options or construct good alternatives. Descriptive/prescriptive accuracy *per se* is not the primary objective. Many other factors beyond the results of the models go into the decision making. Models don't make decisions, people do. But modeling can be valuable for training and educating decision makers in advance of attacks.

There are mathematical modeling methods that have been developed and applied successfully in many related areas. These could be, but largely are not, being applied in the planning for bioterrorist threats. Certainly there are ways in which the application of planning for and dealing with bioterrorist threats will bring in aspects which may not have received much attention in other applications. But identifying and focusing on these at this point may not be the most important thing to do.

Modeling the Bioterrorism Situation

A malevolent agent (the "Attacker") engages a population (the "Defender") with acts of terror by releasing contagious biological agents. The Attacker may be an individual, an organization or a state. The Defender is typically a state. The Defender's objectives are:

- To minimize the number of casualties;
- To minimize economic cost of the attack;
- To capture the Attacker and eliminate his threat.

The Defender attempts to respond to the attack by:

- Taking preventive measures such as modularity[19] oriented vaccination;
- Detecting the attack and identifying the biological agent;
- Providing medical help to infected;
- Tracing contacts and vaccinating susceptibles;
- Isolating and quarantining infected and suspected carriers of the virus;
- Identifying the Attacker (individual, organization or state) and neutralizing him.

The Attacker may try to disrupt the response attempts of the Defender.

The Types of Problems

There are two types of problems that the Defender has to deal with:

- Structural (strategic) level decisions that need to be made in advance;
- Operational (real-time) decisions that are taken during the attack.

Structural Level Decisions

Structural level decisions concern strategic issues that relate to the readiness of the Defender to counter bioterror attacks. These issues are:

- Size and mix[20] of inventories (e.g., vaccine and other perishable items) at the national level;
- Policies for managing and controlling the inventories (e.g., concentrate the supplies or distribute);
- Deployment of the counter-bioterror infrastructure (e.g., detection systems, inoculation facilities);

[19] See Simon Levin's talk at the working group meeting.

[20] There may be a need to produce and store different types of vaccines according to demographic classifications such as age, weight and health condition.

- Manpower requirements and personnel pre-assignments;
- Intelligence capabilities for detecting, identifying and eliminating the threat.

It should be pointed out again that *structural* level decisions are made *before* any occurrence of a bioterror event.

Operational Level Decisions

Operational level decisions apply to situations where a bioterror event has occurred (i.e. there is operational or clinical evidence) or is suspected to be in progress. The single most important input for the operational-level decision making process is the time-dependent spatial probability distribution of susceptibles, asymptomatic contacts, etc. This probability distribution, which affects many of the operational-level decisions, may take a special (multimodal) shape if multiple outbreaks occur. There are situations where some policies are dominant over others for any distribution of susceptibles, and so this distribution may not be so important all the time.

The decisions that are made at this level concern:
- Identifying the type of the bioterror event.
- Contact-tracing process. This process is important for obtaining better estimates for the aforementioned spatial probability distribution. (This may or may not make sense depending upon circumstances and should be considered a proposed option to be evaluated.)
- Prioritization with respect to monitoring, isolating, quarantining and vaccinating – based on the spatial probability distribution.
- Coordinating the supply chain of vaccines and other supplies (allocation of supplies, transportation schedules, etc.).
- Operations management of service (i.e., vaccination, quarantine) centers. In particular identifying bottlenecks and potential congestions, determining capacities and setting service rates.
- Identifying the threat (the Attacker) and trying to eliminate it or at least to reduce its effectiveness.

Modeling Challenges

Models for bioterror emergency response logistics are not necessarily prescriptive. Their main purpose is to supply relevant input data and information to the decision making process and to provide insights about the situation to decision-makers. Consequently, descriptive or predictive accuracy *per se*, that is prevalent (and needed) in mathematical epidemiology models, is not a primary objective in this case. Modeling issues are:

- **Estimating the time-dependent spatial probability distribution of susceptibles.** As indicated above, this is an important process in managing a response to a bioterror event. The distribution is updated as more information (e.g. new infection cases, tracing results) is obtained. This dynamic updating process lends itself to ***information-theoretic*** models such as ***entropic algorithms.*** Also other statistical methods such as ***Bayesian prediction*** models and ***maximum likelihood*** models may be useful for obtaining the desired distribution.

- **Solving a two-stage problem**. Structural and operational decisions take place in highly uncertain environments and therefore can be naturally represented by ***stochastic programming*** models. Structural decisions must be taken in advance while (at least some of) operational decisions may be postponed until a bioterror event actually occurs (and its characteristics unfold). Hence, a ***two-stage model with recourse*** or some variant of a ***chance-constrained programming*** model may be an appropriate way to approach this complex problem. Dynamic programming is also natural in this area.
- **Modeling the conflict situation**. Notwithstanding questions regarding rationality (of the Attacker), ***game theory*** models may be incorporated to obtain efficient (*threat, response options*) matching**.** In particular, the question of whether or not publicly stating a response policy for a given threat has an impact on bioterrorist decision making can be analyzed.
- **Modeling the "combat" situation.** The objective of the Attacker is to cause attrition to the Defender. The Defender will try to repel this attack by taking defensive measures (vaccinating, isolating) but also aggressive measures against the Attacker. This situation of mutual attrition is a classical combat situation and as such may be modeled by ***stochastic combat models*** (e.g., ***Lanchester Stochastic Models***). The characteristics of the combat model depend on the type of the Attacker – individual, organization or state.
- **Logistics Management.** For the logistics problem, standard OR models such as: ***inventory models, location models, assignment models, queuing models*** and ***transportation models*** are needed to be applied. Applications of these models must reflect the central and most profound feature of this bioterror situation – the "race" between the two time scales: the epidemic time and the logistics time. Tradeoffs between regimes such as ample service vs. (different levels of controlled) congestion must be quantitatively evaluated.

Some more general and important comments should be added. Models need to be validated, but validation won't happen against real data very often (we hope!). Simulation or other more complex models can be used as **a** test bed to evaluate policies derived from simpler logistics models. We want to be able to revise/update our models, perhaps in real time, as data arrive (so self-evaluating systems, data assimilation are key aspects). Different models are appropriate for different threats. Some general models can be developed to apply to a variety of pathogens, but pathogen-specific models should incorporate specific threat/response pairings and relevant models of disease spread. Incorporating logistics into epidemic models changes standard results due to competitive time scales of epidemics and interventions. For example, epidemic outcomes differ greatly depending upon whether or not available response capabilities result in congestion.

Suggestions for Getting Started

To get started, we need to gain a feel for policy options and associated decisions, at both structural and operational levels, at different levels of jurisdiction (local, regional, state, federal). One approach is to treat existing plans for bioterror response as data, and review them with an eye towards creating an inventory of response logistics concerns. Since different threats require different responses, we could organize a binary matrix with threat possibilities along one dimension and response options along the other, to summarize threat/response matchings. It will help to consider existing bioterror response templates (structure of "incident command,"

detailing different agency responsibilities and chain of communication). It will also be useful to contrast civilian chains with military (the latter issue orders, operate privately; the former "muddle through" and act publicly). A different idea is to formulate an action/state matrix as suggested in *Science* (3/8/02, p. 1839). This would have states (high risk, low risk, safe) and actions (intensive intervention, monitoring/some restrictions, nothing), with payoffs (scaling from 0 (worst) to 1 (best) case). These approaches should help us to focus attention on key issues/decisions. The general principle is: "When uncertainty is extensive, what really matters are the consequences of different actions."

Challenges for the Mathematical Sciences

Several branches of mathematical sciences are relevant, including (but not limited to):

- Operations research (natural for logistics)
- Mathematical epidemiology (natural for disease)
- Probability and statistics (natural for uncertainties, parameter estimation)
- Computer science (natural for more advanced computation)
- Game theory (natural for modeling conflict)

The key mathematical sciences challenge is to adapt modeling methods used for logistics in other fields to applications in bioterrorism defense. As noted earlier, the problem may not be to develop new methods so much as it is to adapt existing methods to new applications. The section on modeling challenges has described very specific challenges, namely to develop:

- Information-theoretic models for estimating the time-dependent spatial probability distribution of susceptibles.
- Bayesian prediction models and maximum likelihood models for estimating the probability.
- Stochastic programming, chance-constrained programming, and dynamic programming methods for solving the two-stage problem of decision making required for bioterror attack defense.
- Game-theoretic models to understand the threat/response pairings in conflict situations.
- Stochastic combat models.
- Applications of standard OR models such as inventory models, location models, assignment models, queuing models, and transportation models, with an emphasis on the tradeoffs between "ample" service vs. "congestion."

Recommendations

- Mathematical modeling for bioterror logistics should be developed and encouraged.
- A cross-disciplinary approach is needed.
- Collaboration between relevant decision makers (public health officials, first responders, political leaders/staff), public health professionals, and modelers is essential.
- A federal agency should take the lead in advancing bioterror response logistics research, recognizing the multidisciplinary nature of the problems (Office of Homeland Security?).

Report of DIMACS Discussion Group on Design of Disease Control Strategies (e.g., isolation, quarantine, vaccination, …) via Mathematical Modeling

Group Members:

Jean Marie Arduino, Merck ResearchDavid Banks, FDA
John Bombardt, Institute for Defense Analyses
Carlos Castillo-Chavez, Cornell University
Richard Ebright, Rutgers University
John Glasser, CDC, Facilitator
Karl Hadeler, University of Tuebingen, Germany
Alun Lloyd, Institute for Advanced Study
Ellis McKenzie, NIH, Facilitator

Preliminaries

Our discussions focused on models as tools for public policy decision making, within the following context: agent release, spread, detection, analysis (modeling), advice, and action. Models could be used to prepare for possible terrorist attacks, as well as to aid in responding optimally in real-time.

We perceive this as an opportunity for direct service (i.e., to ensure optimal deployment of available resources in the event of attack) rather than the development of mathematical innovations only loosely inspired by policymaking need. Recognizing that simplicity always is a virtue, our sessions were dominated by discussions of possible means of identifying the simplest model that would address policy issues responsibly (other than anticipating questions and reducing realistic models via sensitivity analyses).

We assumed that releases would be deliberate, and undertaken by intelligent, knowledgeable people. With smallpox, for instance, variolation generally produces a mild disease that nonetheless is infectious, enabling those variolated to move about places where susceptible people congregate. Terrorists are willing to blow themselves up, so surely they would risk variolation, which is only occasionally fatal.

Nature of Threat

The nature of threats affects the strategies that must be evaluated. Deliberately introduced pathogens differ from natural ones in some respects, offering special modeling challenges. We focused on smallpox, whose potential as a terrorist weapon has been described (in, e.g., J.B. Tucker, *Scourge: the Once and Future Threat of Smallpox*, Atlantic Monthly Press, 2001), and recognize that our thoughts may apply less well to other pathogens.

Introduced pathogens may be unfamiliar, and may become known only via observation during the early epidemic phase. They may be diseases that occur elsewhere, for which we have little native immunity (e.g., many tropical diseases in the Northern Hemisphere); natural or induced mutations may enhance virulence. With advances in molecular engineering technologies, a truly

determined and skilled adversary could turn even commensal microbes into weapons (see, e.g., Tim Beardsley's piece in *Scientific American*, http://www.sciam.com/1999/0499issue/0499infocus.html).

In their delivery of familiar pathogens, terrorists are not limited to the means by which they are or were transmitted naturally: for instance, smallpox (historically person-to-person, but also via scabs or fomites), pneumonic plague (respiratory), anthrax (aerosolized), and bioengineered influenza (presumably respiratory). Pathogens might be disseminated at a single or multiple sites, or over wide areas. The utility of historical experience in this context remains unclear.

One response to these uncertainties might be to develop generic models with which to simulate the behavior of any agent or agent combination, given some idea of its properties. The most useful "model" for the kind of near-real time operational support needed would be essentially pathogen-independent. This appears tractable, given our collective experience modeling contagious diseases for which interventions exist, but see the "Possible Modeling Approaches" section below.

Nature of Response

Possible response strategies (more or less in order pre- and post-event), and other issues that should be considered include:

- When the vaccine stockpile suffices (as it may now for smallpox given the discovery of additional vaccine), permitting purchase under informed consent
- Vaccinating first responders and selected others pre-event (e.g., healthcare workers, bus drivers), becoming more inclusive as the risk increases
- Targeting super-spreaders (people who are very infectious, or who have many contacts, possibly because they are highly mobile)
- Isolating febrile or all contacts (including asymptomatic ones), quarantining households, schools, workplaces, neighborhoods, communities
- Vaccinating contacts, locales (e.g., households, …), everyone
- Initiating chemotherapy, if any exists and is available
- Composite strategies (e.g., the contribution of population immunity, attained via mass vaccination or disease, to the success of search and containment at eliminating smallpox in South Asia [where R_0 was high])
- Dealing with vaccine adverse events (via, e.g., vaccinia hyper-immune globulin, etc.)

We realize that another group focused on response logistics. Nonetheless, when introductions suffice to overwhelm the ability to search for cases and vaccinate/isolate to contain spread, the need to switch strategies and vaccinate locally or even indiscriminately may be obvious and/or irrelevant (because public reaction may force the issue). It is not clear what these thresholds are, however, and on what else they may depend (e.g., R_0, side effects of vaccination, speed of propagation, etc.).

Human Behavior

Our most daunting challenge may be accounting for the behavior of terrorists before and during attacks and the behavior of victims and the general public afterwards. We should involve social scientists to anticipate behavior and increase the probability of people responding as directed.

Appropriate modeling of index infections is extremely important, especially in bioterrorist scenarios (e.g., if they are terrorists). Attacks could involve anywhere from a few people up to many thousands, who might initially be localized (within a single city) or dispersed (throughout several). The non-uniform progression of index infections is another key influence on disease transmission and control strategies, particularly if unnaturally high doses affect progression.

How might people respond to an act of bioterrorism and to governmental disease control strategies? Because emergency declarations and federal responses affect state/local, community, and individual compliance, clear, panic-quelling, if not confidence-inspiring, instructions are interventions in themselves. How could such responses affect the implementation, and hence effectiveness, of control strategies? (The public's response to macroeconomic policies during deflationary or inflationary periods and the corresponding econometrics appears analogous.)

Mathematical Challenges

We make some comments about challenges facing us in the use of mathematical models.

Analytical Tools for Transient Behavior

Traditional mathematical approaches to the long-term behavior of epidemics and the persistence of endemic states (such as stability analysis near equilibria) will be of little value. Policymakers will need estimates of early transient behavior (number initially infected, cases per week, consequences of more or less efficient implementation of more or less timely vaccination and containment policies, probable outbreak durations, magnitudes, and costs under several scenarios). At present, few analytical tools are available for transients. Once developed, however, these would have other applications.

Possible Modeling Approaches

It is unlikely that any single model/approach could address all options or serve all purposes; furthermore, diversity enriches our appreciation of phenomena. The pros and cons of various mathematical models and methods should be considered, among which we discussed the following issues:

Simple versus realistic:

1. Simplicity facilitates communication, and parameters often can be estimated with precision, but the failure of realistic models (i.e., hypotheses about natural phenomena) can increase understanding;

2. The premise of applied population biology (i.e., epidemiology, demography) is that a relatively small number of characteristics (e.g., age) suffice to account for major patterns in disease. Models of populations composed of types (e.g., age groups, behavior classes, habitation densities) are relatively simple compared to ones composed of individuals;

3. Superficial versus true complexity (e.g., a system of many ODEs may be no more complex than a few integro-differential equations or PDEs).

Deterministic versus stochastic:

(NB: The issue is not if God plays dice, but if policymakers need realistic confidence intervals. They do if results encompass more than one option being contemplated, or force consideration of others. The "trick" is finding ways of considering variances, rather than one-point answers, when these matter within this broad decision-focused framework.)

1. Stochastic models are useful not only for confidence bounds, but information about the covariance of fluctuations enters into formulae for the mean (i.e., feedback into the calculation of mean values);

2. Complex probabilistic approximations may reside within deterministic ODE models, as in mean-field determinations;

3. Experience suggests that one can learn almost as much from proper sensitivity analysis of deterministic models (except close to bifurcations) as from stochastic ones;

4. Stochastic models may distinguish between minor and major outbreaks (and false alarms). Because decision makers are especially sensitive to the risk of catastrophic events, this may be of great help in the wider context.

Game-theoretic methods:

These have great potential in decision-making contexts, especially in adversarial situations where opponents value costs and benefits differently (or there are different or changing cultural norms). Statistical risk analysis offers tools that estimate the payoffs needed as inputs to either the extensive or normal, tree or matrix, forms of two-person non-zero-sum games. What other mathematical tools and techniques would be useful in representing post-attack behavior across the spectrum of epidemic models (deterministic, stochastic, spatial, ...)?

Data, Validation, and Sensitivity Analysis

What data would be useful in developing and refining these models? And how would we know if our results were qualitatively incorrect?

1. The NIAID has developed a Counter-Bioterrorism Research Agenda (http://www.niaid.nih.gov/dmid/pdf/biotresearchagenda.pdf) within which opportunities may exist for interaction/collaboration with scientists in other disciplines on studies to gather data useful for the development and evaluation of mathematical models.

2. Decision makers may be familiar with modeling when full-scale testing is infeasible (of, e.g., nuclear weapons); can we validate models experimentally (e.g., using role-playing exercises as experiments to validate computer simulations with independently-generated data and parameters) as well as against historical data (that may or may not be wholly relevant)?

3. It may also be possible to validate simpler models by comparing them to more complex ones. For instance, deterministic models, using average values can duplicate the results of more complex stochastic models.[21]

4. Sensitivity to assumptions (e.g., whether spatial heterogeneity matters), as well as to parameter values, must be checked, as must the influence of initial conditions.

Collegial Relations

We discussed the extent to which modelers should cooperate versus compete, and most agreed that cooperation on important common topics (e.g., biological details, public policies being contemplated) was best, but that groups modeling in different ways (e.g., as sketched above) would provide a sort of global sensitivity analysis in a situation with too much uncertainty to place proper confidence intervals on results of interest.

1. By having such working groups, DIMACS provides a forum for modelers to critique one another's work without needlessly confusing policy-makers. Having quasi-independent groups model foot-and-mouth in the UK was particularly instructive. But what would have happened had conclusions differed, particularly with respect to their implications for policy?

2. Could individual-level details in EpiSims (or superficially similar models, e.g., the one under development at Purdue) be mapped onto individual types (e.g., age groups) and the corresponding contact matrix be determined and provided to others for use in their simpler models? Similarly, could such information be obtained from proximity detectors, and similarly shared?

A minority view was that a competition of the sort exemplified by bi-annual computational modeling of protein three-dimensional structure (CASP, Community Wide Experiment on the Critical Assessment of Techniques for Protein Structure Prediction; http://predictioncenter.llnl.gov/casp4/doc/casp4-announce.html) would improve the quality of our work. Other examples are the computational modeling of intermolecular interactions (CATFEE, Critical Assessment of Techniques for Free Energy Evaluation; http://uqbar.ncifcrf.gov/~catfee/) and a recently announced blind test of protein docking algorithms (CAPRI, Critical Assessment of PRedicted Interactions; http://capri.ebi.ac.uk/).

One member of our group opined that CASP's impact on computational approaches for protein structure prediction had been immense, that CATFEE was expected to have a large impact too, and that an analogous competition could similarly affect development of epidemiological models. He imagined, for example, annual ranked competitions focused on prediction of each year's influenza and/or pneumonia outbreaks (predictions that would be assessed and ranked against subsequently available data) and annual un-ranked competitions focused on prediction of bioterror/biowarfare attacks (predictions that--one would hope--could not be similarly assessed and ranked).

[21] See, for example, Longini, et. al., *Math Biosci*., 38 (1978), 141-157.

DIMACS Discussion Group on Challenges for Computer Science

Group Members

Adam Buchsbaum -- AT&T Labs
Alok Chaturvedi -- Purdue University (Rapporteur)
Sorin Istrail – Celera Genomics
William Mills –Federal Government
Rafail Ostrovsky – Telecordia Technologies
David Pennock – NEC Research Institute
Fred Roberts – DIMACS/Rutgers University (Facilitator)
Gary Strong – (NSF Observer)
Michael Trahan – Sandia Labs

Introduction

In dealing with potential bioterrorist attacks, one can divide approaches into two categories: prevention and response. Approaches to prevention build heavily on surveillance, which in turn involves the handling and sharing of massive amounts of data, with concomitant threats to privacy.[22] Approaches to response also include surveillance or detection (determining if a bioterrorist event is taking place is itself non-trivial). Response approaches typically include both advanced planning and crisis planning, and each heavily involves the use of mathematical models as tools to aid policy makers. Problems of surveillance, detection, massive data sets and data sharing, and computational support for mathematical models and decision makers all depend in important ways on methods of modern computer science. The development of improved methods of bioterrorism response and prevention presents new and important challenges to computer science research, which were the subject of this group's deliberations.

The group discussed a wide variety of challenges for computer science and divided them into six categories, which will be described in this report.

The six categories are:

1. Simulation and Virtual Environments
2. Data Base Policies and Information Exchange
3. Intelligence and Detection
4. Fault Tolerance
5. Consequence Management
6. Computational Molecular Biology

[22] Another major component of prevention involves understanding subtle and highly unstable social processes that provoke terrorism. This is a very important area for research that should involve computer scientists in partnership with social scientists.

Simulation and Virtual Environments

It is infeasible to run real-world bioterrorism experiments to test the effectiveness of our surveillance systems or our response plans[23], or to validate our models of disease spread, social movement, or terrorist recruitment. It is therefore essential that we develop virtual environments for experimentation and analysis.

Simulation is essential for understanding the implications of large ***transmission models*** and studying ***social interactions and social networks***. Better and more efficient simulation methods are needed for the large agent-based and continuum models being developed to model disease transmission.

Developing effective response strategies to a bioterrorist attack involves serious ***scenario planning***. Such scenario planning is one of a variety ***of analytic decision theory aids*** heavily based in methods of simulation. Along with each scenario, the response model must be subject to ***verification, validation, and accreditation***. These are all topics of modern computer science research, but new methods for them in virtual environments are called for. Simulation models are also helpful in forensics and in validating our theories about the cause of an event, akin to ***National Transportation Safety Board modeling experiments***.

Methods for deterring bioterrorist attacks depend upon models of competition between attacker and defender. These ***adversary models*** should be ***behavior-based*** and involve modern ***game-theoretic aspects***, often involving the kind of dynamic game situations of increasing interest in computer science research related to auctions and other e-commerce applications.

Many methods of the mathematical sciences have been used in epidemic modeling and in response planning in military and domestic industrial contexts. These models include well-known methods of ***operations research*** applied to inventory, distribution, task assignment, scheduling, etc. However, because of the large number of variables involved in realistic models of bioterrorism attack and response, the associated algorithms don't always scale, and so challenges for modern computer science research involve issues of ***architecture and scalability***.

Data Base Policies and Information Exchange

An important challenge to maintaining homeland security in general and to defending against bioterrorism in particular is to ***share information across multiple databases***, either within or between organizations. The technical problems are exacerbated by the need to maintain ***privacy and security***. The opposing goals of protection of sensitive information and the need for information exchanges among agencies or between databases lie at the intersection of some of the most challenging areas of research in modern computer science.

Data sharing is complicated by such factors as differences in representation of information among the various databases and the low and error-prone quality of stored information caused by manual entry, lack of uniform standards for content and formats, data duplication, and

[23] Or to evaluate the depth of our understanding of the causes of terrorism.

measurement errors. This calls for new methods of ***data cleaning***. The development of ***efficient coordination engines*** is also required.

Databases may not be integrated wholesale but only mined for individual records or pieces of information, which calls for sophisticated methods to protect the confidentiality, integrity, and availability of information. A major challenge to modern computer science is ***information exchange without revealing private data***: to provide techniques for efficiently, accurately, and securely sharing information among multiple databases.

Intelligence and Detection

It is crucial to develop surveillance systems that will detect impending bioterrorist attacks in time for us to take preventive measures. Should such surveillance systems fail to predict an attack, they are still critical in helping us identify that an attack has taken place, since early detection is crucial in minimizing damage. Moreover, once evidence of a biological attack is observed, for example increased illness and death in an area, the actual nature of the attack might still remain elusive. Methods for detecting and identifying biological attacks are thus critical. Intelligence and detection thus provides means to discover and report abnormal or undesirable events, such as biological attacks: before an attack occurs (detecting preparations for an attack); during or immediately thereafter (identifying that an attack has occurred and the nature of the attack); and during the response period (assessing the effectiveness of the response and facilitating heightened surveillance for subsequent attacks).

Important challenges for computer science lie in all aspects of the intelligence and detection problem. ***Data mining*** is a central tool of detection. Challenges in data mining include the development of new methods of ***data cleaning, dimension reduction, visualization of data***, and the development of ***spatial temporal models***. Methods of ***streaming data analysis***, widely under development for dealing with computer network intrusion, credit card fraud, and financial decision making, are needed for surveillance systems that are to respond quickly to abnormalities. Since many reports to surveillance systems involve natural language, new challenges to ***natural language processing*** also arise. Related problems of detection will also require new methods for ***classification/clustering in high dimension spaces***, new tools for ***pattern discovery***, and new algorithms for ***signal detection*** in the presence of noise. In turn, these methods already do and in the future will increasingly make use of ***learning theory*** to classify new data and signal the arrival of a "new event." Challenges in learning theory include development of new ***machine learning*** protocols and of ***hidden Markov models***.

As we develop surveillance systems, we will want to use computer models to help locate ***distributed sensors*** and interpret data from them. We might also wish to use the ***Internet as a sensor/communication device*** in our efforts to develop methods of ***global change detection***. Methods of ***biometrics*** provide another potentially useful detection tool.

Fault Tolerance

In defense against bioterrorist attacks, functionalities that can operate under malicious, coordinated attack and nevertheless remain robust and secure are essential. We must build our

bioterrorism defense systems, such as surveillance systems, vaccine or prophylaxis distribution systems, emergency communications systems, etc., to be reliable even if they consist of unreliable components.

Redundancy has traditionally been the fundamental mechanism for ensuring reliability. Increasingly, traditional approaches to using redundancy are not applicable to modern networked environments. Today's computer and communications networks rely more and more on loosely coupled, off-the-shelf hardware and software systems, which exhibit extremely complex fault behaviors that must be masked via ***large-scale redundancy***. The mathematical formalisms, tools, and methodologies for dealing with this situation need to be developed.

Fault tolerance cannot be an afterthought. Rather, it must be an essential ingredient of ***system design*** from the beginning. This is also true of ***security***, which is crucial to our surveillance systems and the development of our response plans. Security is just one aspect of the need to defend against an unknown or only partially known adversary. Game-theoretic models can help us identify promising policies; methods developing concepts and implementations of ***game-theoretic fault-tolerance*** will be very helpful.

Our complex, interconnected agricultural systems and our modern, high-speed, inter-city transportation system leave us vulnerable to biological attacks. Ever more powerful methods for ***assessment of vulnerability*** are needed.

Our response mechanisms will increasingly build on sophisticated computer models. To use them, we will need to maintain ***computation under continuous attack***.

Consequence Management

Another group has dealt with the various aspects of plans for responding to a bioterrorist attack. We need tools for such "consequence management," both to help us develop advance plans and test them, and to help us modify these plans in a crisis situation. In short, we need ***tools to assist crisis managers deal with any eventuality***.

Information is a key to modern "warfare." ***Information dissemination*** will be a key to consequence management, and a major challenge to computer science will be to develop ways to disseminate information in a distributed environment, with potentially unreliable systems, and with speed, efficiency, and security. Communication among the many individuals and agencies involved in a response to a bioterrorist attack is essential, and we shall have to develop ever better ***robust ad hoc communication networks***.

The plans we develop for a response will be intricate and involve ***strategies and models for mobilization, stockpiling, isolation, vaccination, quarantine***, etc. These strategies and models will have to be developed for testing in a virtual environment, and the users of the models will have to be supplied with highly efficient computational tools for modifying their models on the basis of developing situations.

Computational Molecular Biology

Computational molecular biology provides computational tools for molecular data analysis, design of predictive models, and bio agent identification.

Phylogenetic methods – developing the "***tree of life***" – are a central tool in modern computational biology. These methods are important in ***strain detection***, an important task in identifying the source of agents used in bioterrorist attacks. Phylogenetic methods help to identify the subtype of the organism and then can potentially indicate from which lab it is coming. This requires computationally intense analyses that would benefit from the development of new methods and algorithms.

Methods of computational biology, using ***finger printing*** and ***computational genetics***, also hold promise in distinguishing bioterrorist dissemination from natural dissemination, a crucial distinction, and in predicting the evolution of bioterrorist agents.

Report of the DIMACS Discussion Group on Agriculture and the Food Supply

Group Members[24]

Simon Levin, Princeton University (Facilitator)
Lora Billings, Montclair State University
Michael Boechler, Innovativc Emergency Management (Writer)
Keith Cooper, Rutgers University
Donald Hoover, Rutgers University
Mai Nguyen, Federal Government
Michael Steuerwalt, (NSF Observer)
Stephen Tennenbaum, Cornell University (Rapporteur)

Focus

The discussion of our group ranged across a number of issues associated with protection of the country's agriculture industry. Our definition of the industry was intended to be inclusive of forestry and aquaculture within which we primarily considered issues related to the food supply, as opposed to those that may involve ecosystem damage but not significantly affect the food consumed by humans[25].

Background

Agriculture is a significant component of the economy, accounting for approximately 2% of the nation's gross domestic product[26]. A terrorist attack on it could result in enormous direct effects on the industry targeted, on their dependent consumer markets and throughout the entire food chain resulting in adverse events throughout the entire world economy. The costs of repair responses and *a posteriori* control measures to prevent future attacks would prove high in a possibly panicked atmosphere. Historical records of the massive impact of crop failures with resulting mass starvation and migration are indicative of the potential scale of these problems. Examples of this include the Irish Potato Blight, famines in Ethiopia, and the "dust bowl" of the 1930's.

Such a devastating attack could result in the disruption of normal activities and peace of mind as well as food lines, uncertainty, erosion of public confidence, and fear. These effects could, in turn, result in persistent or permanent changes in domestic culture or international relations[27].

Attacks on agriculture could have major impacts on food availability if aimed at crops or livestock directly, resulting in nutritional problems and increased vulnerability to disease or other forms of attack on humans. Food safety would be compromised if agents were deployed that

[24] The group thanks Mark Thurmond, University of California, Davis, for helpful input.
[25] Attacks on agricultural areas could be easily orchestrated and result in wide-scale, persistent ecological consequences. However, attacks could be just as costly but maintain a low profile, for example the effects of an introduction of weedy species or pests (e.g. Gypsy Moths) could be difficult or impossible to control but have little sensational impact.
[26] http://www.cia.gov/cia/publications/factbook/geos/us.html
[27] For example, if contaminated food were exported.

produced or contained toxins, or if toxins were introduced into the foods directly from within the food processing system. Posing a smaller threat, the possibility of livestock, fisheries or wildlife being used as vectors or secondary hosts for disease transmission to humans also exists.

Current agricultural practices and trends such as the increasing genetic homogeneity of crops, large geographic expanses of monocultures, isolation, as well as difficulties in surveillance and detection, coupled with the potential use of low tech, low cost and self perpetuating biological agents could make agriculture and the food supply a particularly attractive target to terrorists. In addition, as new technologies continue to revolutionize agribusiness, future pressure from these changes could foster targeted forms of ecoterrorism in which particular crop strains are targeted.

Contamination Problems

The most salient example of contamination of an agricultural product is perhaps the occurrence of bovine spongiform encephalopathy, more colloquially known as mad cow disease among European livestock. More recently, British problems with foot and mouth disease have garnered attention in the media which reported on the speed of the contagion, and the difficulties officials encountered in attempting to contain, control, and eradicate the disease.

Posing problems for the beef industry are recurrent incidents of *E. coli*-contaminated ground beef resulting in deaths and large scale recalls, while the contamination of corn crops intended for human consumption by genetically engineered, and toxic, strains did little to further the cause of those who promote the use of genetically modified crops.

Perhaps the most relevant, and notorious, food or drug contamination example involves the Tylenol® tampering that occurred in 1982. Even though only a handful of containers were contaminated with cyanide, large recalls of the product, and public distrust of it, meant large financial losses for the company.

Motivated by these considerations, we turn our attention throughout the rest of this report to some of the attributes of a framework that could be used to prepare for or to counter events in which an agent is used by a terrorist to contaminate food or drug products. This is followed by an identification of the significant challenges for the mathematics and computer sciences communities in implementing such a counterterrorism framework.

Counterterrorism Framework

In order to minimize the risks associated with a terrorist attack two objectives should be accomplished: the probability of the attack should be decreased through deterrence, and the attack's consequences should be minimized. The first objective requires that adequate capability exists to predict the terrorist attack. The second requires that, when the attack occurs, the crisis caused by it, and its consequences, are optimally managed.

Event prediction and deterrence, crisis management and consequence management can all be aided through the use of mathematical models and simulation. Each of these components offers opportunities and challenges to the quantitative modeling community.

Prediction

Minimizing potential impacts of a terrorist attack is accomplished by predicting, then deterring the attack. Prediction depends on intelligence regarding the terrorist's capabilities, motivations, willingness to act and perception of his target's vulnerabilities. This suggests that systematic vulnerability assessments should be done in order to better understand and remedy critical weaknesses in the current agribusiness, food and drug protection infrastructures.

Vulnerability assessments should include assumptions that areas of large monocultures exist and that some crop species are highly inbred, hybrid, or genetically specialized. Plants are particularly vulnerable to pathogens since resistance to disease is often dependent on a handful of genes. This implies that the genetic engineering of pathogens could potentially circumvent innate plant protection. These areas of monocultures and the types of organisms raised within them should be comprehensively catalogued as part of the vulnerability assessment.

Especially contagious or difficult to control diseases should be identified and ranked with respect to risk. Some likely candidates include: Foot and Mouth Disease, Avian Influenza, Newcastle Disease, Bluetongue, African Horse Disease, Tuberculosis, Brucellosis, Potato Blight, Classical Swine Fever, and Mad Cow Disease.

Zoonoses and vector borne diseases may also be of some concern in assessing vulnerability. Some example include: Tuberculosis, West Nile Virus, Dengue Virus, Malaria, Avian Encephalitis, Rocky Mountain Spotted Fever, Lyme Disease.

In terms of terrorist capability, there are a host of potential agents that could be used in an attack. Chemical, biochemical or radiological agents could be employed. Microparasites such as viruses, bacteria, fungi could be used, as could macroparasites such as protozoans, worms and other invertebrates or algae. And, as mentioned above, pests such as weeds, insects, or competitor species could be used.

Finally, it should be assumed that outbreaks dependent on environmental conditions will be of lesser concern as a mechanism for minimizing the consequences of these outbreaks exists naturally and at no cost to the target.

Identifying the terrorists' immediate goals will be important for predicting their actions. Specific terrorist goals might include:

- Death, pain, or disablement of people or entire populations
- Economic damage – Producers of agricultural products face an additional ecoterrorist threat in addition to the background terrorist threat
- Military disablement
- Social disruption
- Coercion
- Diversion
- Social rebellion

A number of analytical techniques should be applied to the problem of predicting an agriterrorism attack. Mapping of monoculture regions and the distribution of crop types can be

aided through the use of geographical information systems (GIS). Risk analytic techniques can be applied to calculate the degree to which various sectors of the food industry are vulnerable to exploitation and at what technological cost to the terrorist.

An examination from the terrorist's perspective might involve application of operations research techniques such as those employed in foraging theory. In this case, they could be applied to the terrorist's choice of attack opportunities. Predator-prey models might be adapted and applied to the 'arms race' between terrorist and counterterrorist strategies. Since these models are primarily descriptive rather than strategic, game-theoretic approaches, modeling the competition between attacker and defender, might be more useful.[28]

Little quantitative modeling and simulation has been done in the areas of persuasion, influence and action initiation. Models of these phenomena could be of use in predicting the antecedents of terrorist action or in decreasing the probability that such action will occur.

Challenges for Prediction:
There are a number of particularly difficult issues that are raised when considering the prediction of terrorist actions. There is the possibility of multiple attacks across large geographic regions. Multiple organisms could be simultaneously targeted in order to synergize the effects of each attack. Attacks could occur with multiple agents, possibly coordinated to specifically compromise detection and/or response systems. New sophisticated models that account for these possibilities will need to be developed.

Deterrence
The best way to respond to a terrorist threat is to deter the threat from reaching its destructive potential. Preventive measures to protect agricultural products should be implemented so that the adverse consequences of any terrorist attack can be minimized. One of the best ways to deter the action is to decrease the amount of damage that it can cause. In the present case, this means that agricultural methods should be adopted so that food crops are less susceptible to disease outbreaks or pest infestations.

Some of the *a priori* preventive measures that might be considered include encouraging genetic heterogeneity in crops,[29] intercropping and diversifying crop types at the landscape level, using buffer zones between genetically similar crops or reserves, or by reducing the mobility of crops and animals by requiring an observation/quarantine period before transport.

These preventive measures could be made more effective if a more complete understanding of the conditions that precede and compel terrorist activity was obtained. Such an understanding would suggest additional strategies that might take advantage of the *a priori* measures that have been implemented.

Challenges for Deterrence:
The measures we have suggested for reducing the damage that can be sustained in an attack would, in many cases, represent a significant and costly departure from current agricultural

[28] In these models, we might assume that the perpetrator of an attack will also consider our response to his actions.
[29] Costs, such as profit loss, might be offset by government payments to farmers and agribusinesses.

practice. Determining the cost effectiveness of the economic solutions needed in order to implement these *a priori* measures would require a significant amount of modeling. In addition, accurate and useful models of terrorist beliefs and behaviors would require a great deal of modeling.

Crisis Management

The well-organized management of a complex crisis such as an agricultural terrorist attack depends on the timely receipt of accurate information. This information needs to be obtained and transmitted quickly once the event starts and must be made available in an understandable format so that decision makers can best act upon it.

The information systems employed should allow decision makers to simulate possible event outcomes and to explore the expected effects of different response strategies on these outcomes. These systems should also be able to maintain false positive identification of threats at a low level in order to maintain credibility and to prevent civic disruption by the system itself.

In addition, in cases of response resource shortfalls, decision makers should beble to optimally allocate scarce materials or personnel. Such a set of integrated surveillance and response systems would represent a significant increase in our capability to minimize the negative consequences of agricultural terrorist attacks.

The group thought that it was necessary to focus at a system level in order to best manage any response to a terrorist attack and made the following observations regarding the design and characteristics of a planning, surveillance and response system.

An effective and coordinated surveillance system for reporting, response and decision making would be designed for redundancy and would screen and categorize suspicious events triggering more intense surveillance.

The design should allow hierarchical system responses, much like an immune system model, in which distinctions would be created between global versus local response, and a diversity of response options, that allow for the evolution of a strategy to best meet the need of a given situation, would be available. This feature would likely involve the incorporation of adaptive behavior into the system and should allow analysts to find the most appropriate levels of flexibility and robustness in the system.

Modeling for an effective response should be done at the system level but should also incorporate disparate high resolution models in order to increase realism. Various biological, physical, economic, demographic, social and transportation system models should be integrated in the design, modeling and analysis of this proposed adaptive surveillance system.

One of the first steps toward building such a system is a clear description of each threat it is expected to detect. All known pathogens and pests should be described with respect to transmission characteristics, incubation times, dose-response characteristics, and early signs and symptoms of infection. The acquisition of this information could be facilitated by employing several disease subject matter experts for each agent. These experts, who should be willing to

provide uncertainty estimates for their opinions, can provide the biological insight and facts to indicate the limitations of our knowledge.

These experts should also be able to help conceptualize the key questions, provide estimates for some parameter values and provide an understanding of the general shape of distributions or functions that are relevant. They also can provide a comprehensive list of colleagues who can further elaborate on the expert opinion database where objective, empirical data are lacking or insufficient for modeling.

The proposed system should contain a map for each agent indicating the 'farm-to-fork' pathway, including sites or opportunities for food supply contamination. This would involve elucidating the steps, locations, contacts, vehicles, and people involved in moving food or water from the ground to the kitchen. Population maps, including GIS and other spatial distributions of population and food sources, should be incorporated, as should topographical maps showing streams and tributaries that contribute to domestic water supplies, and maps of underground water tapped by wells.

The system would include descriptions of the available diagnostic tests and testing procedures for each pest or pathogen, including the sensitivity and specificity of each test.[30]

The vaccination (or other prophylactic measure) options for protecting vulnerable species should be systematically described in terms of efficacy, cost and availability[31], time to immune response and protection, and duration of protection.

The various organizational structures, plans, and procedures of the State and Federal agency programs responsible for monitoring and surveillance of food safety should be described such that modeling of governmental response can be addressed. [32] A detailed analysis of current response plans and procedures might involve operations research methods such as the program evaluation and review technique (PERT)**,** which can be used to streamline critical processes employed during the response to an outbreak.

Finally, expert knowledge of agribusiness industry operations and food safety biology would be critical to assuring that the knowledge base of the proposed surveillance and response system is complete, and that the systems that fall within these domains are adequately described.

Challenges for Crisis Management:

A number of methodological hurdles must be overcome during the design of the proposed system. For example, the statistical methods to detect outliers require refinement - predicting rare events is difficult, predicting events that have never occurred is even more so.

[30] That is, the probability of correctly identifying a disease if present, and the probability of falsely identifying the presence of disease if truly absent, respectively.

[31] The time required to manufacture and distribute the vaccines would be quite useful.

[32] This model would contain the strategic nodes identified for typical food safety problems as well as those used in response to a terrorist attack.

The source reconstruction problem exists as it does when considering response to biological weapons directed at humans. This problem becomes thornier when multiple release sources and times are considered. This implies that more sophisticated spatiotemporal models will need to be developed.

Assembling models to build a hierarchical 'immune' system would be a particularly complex task. Although the times allowed to make decisions are longer during an agriterrorism crisis than during, say, a terrorist attack involving nerve agents, the complexity of the surveillance and response system would be great enough that the computing resources needed to implement the system would bear close examination and planning.

Crisis management involves a great many logistical problems of manpower, inventory, distribution, and scheduling. Traditional operations research methods need to be modified to apply to bioterrorist crisis management.

Finally, although conceptual frameworks for human decision making under stress exist within the social sciences, adequate quantitative models do not. Suboptimal decision making behavior occurred during the recent biowarfare exercises TOPOFF and Dark Winter, implying that information is not being processed effectively by those responsible for coordinating and directing official responses to a biowarfare attack. Faithfully capturing these decision making processes and optimizing them will be an important challenge.

Consequence Management

A more complete and accurate estimate of the potential consequences of an agricultural attack must be obtained in order for the proposed system to be of any utility. Anticipated consequences such as contamination, disease outbreaks, displacement, as well as economic and psychological impacts should be incorporated into the system as outcome variables, and should be used as indicators of decision making performance during policy and response exercises.

Once these currencies for optimizing decisions have been specified, adequate consequence management planning will require the use of scenarios that take into account the geographic and spatial aspects of the incident, pathogen or pest persistence and evolution/co-evolution of the pathogen and host, in addition to the considerations discussed above.

Approaches currently exist for countering invading species and would likely be most representative of those used to deal with the aftermath of a terrorist attack targeting agricultural products. They include the following types of control: chemical, biological control, mechanical and habitat-based. The cost effectiveness of each type of control measure available to decision makers should be examined, as should the development of new control options.

Challenges for Consequence Management:

More options for consequence management need to be generated – destroying large amounts of agricultural products in order to halt an advancing pathogen is wasteful and disruptive.

The important dimensions on which planning scenarios are based should be developed. If these dimensions are chosen carefully, a comprehensive set of scenarios could be derived in a manner that assures adequate representation of the relevant policy and planning space.

Bringing in Human Factors

One of the most significant long term challenges to the mathematics and modeling community, is the problem of constructing the types of human behavior models that are needed for the proposed system. To date, no comprehensive mathematical treatment of the transmission of ideas has been offered, although some initial thoughts on the properties accounted for by such theory have been expressed by Dennett[33]. A mathematical treatment of the spread of culture was developed by Boyd and Richerson[34] in a manner familiar to population biologists, while Lumsden and Wilson[35] have examined gene-culture coevolution mathematically, and Feldman and Cavalli-Sforza[36] have also taken an evolutionary point of view, but this work needs to be extended and modified to suit the needs of the range of new problems facing the country.

A number of mathematical approaches might be incorporated into a comprehensive treatment of human communication and behavior. Epidemiological models might be used to model the spread of an idea much like that of a disease. Belief systems might be considered as immune systems – for example, particular belief systems may be quite resistant to the incorporation of new information, especially if that information conflicts with the belief system. Epidemiological models would be best applied when examining questions that are applicable at the group or population level

Other group-level phenomena that need to be addressed are those associated with decision making within bureaucracies. Responding to the types of threats discussed in this report requires the coordination of many governmental agencies embedded within a national to local hierarchy that is responsive to public opinion and the influence of special interests. Network models adapted from the computer sciences might be used to address this aspect of the problem.

On the other hand, models borrowed from information theory would most likely have a place within the mathematical framework when analysis of individual-level communication of ideas is needed. Other mathematical models of individual choice from the econometrics tradition might be similarly applicable for modeling at this level, as may those borrowed from the cognitive sciences in order to link ideas to behavior.

Human language and behavior are among the most complex systems observed. There is no compelling reason to expect that a simple elegant mathematical model of these phenomena exists. The construction of a rigorous framework to explain or predict observed patterns of idea diffusion will likely be a lengthy, difficult endeavor. However, since so much of the complexity present in the real world relevant to the problem of defense against agriterrorism is due to human

[33] Dennett, D. 1995. *Darwin's dangerous idea*
[34] Boyd, R and Richerson, P. 1976. *Culture and the evolutionary process*
[35] Lumsden, C. and Wilson, E. O. 1981. *Genes, mind and culture: the coevolutionary process.*
[36] Feldman, M.W., and Cavalli-Sforza, L.L., 1989, *Evolutionary theory*.

behavior, any comprehensive end-to-end treatment of the problem will be insufficient until such a mathematical structure is complete.

Summary of Challenges for the Mathematical Sciences

- Develop ways to model multiple attacks across large geographic regions.
- Develop models for predicting the impact of attacks by multiple agents and for detecting such attacks.
- Apply risk analysis to calculate the degree to which various sectors of the food industry are vulnerable to agriterrorist attack.
- Develop game-theoretic models for the competition between attacker and defender.
- Develop mathematical models to determine the cost effectiveness of deterrence strategies that depart from current agricultural practice.
- Apply simulation methods to information systems designed to aid decision makers in crisis management.
- Find new statistical methods to detect outliers, to be used in models predicting rare events.
- Create more sophisticated spatio-temporal models for the source reconstruction problem when multiple release sources and times are considered.
- Adapt operations research methods of scheduling, manpower, inventory, and distribution.
- Develop quantitative models to aid human decision making under stress.
- Modify quantitative methods for determining the cost-effectiveness of alternative control measures.
- Adapt network models from computer science to address problems of coordination among multiple government agencies.

Report of DIMACS Discussion Group on Agent-based and Differential Equation Models for Transition Dynamics

Group Members

Fred Brauer, University of Wisconsin
Derek Cummings, The Johns Hopkins University
Robert V. Duncan, University of New Mexico
Mac Hyman, Los Alamos National Labs (facilitator)
Tom Kepler, Santa Fe Institute
Shailendra Raj Mehta, Purdue University
Roseanna M. Neupauer, University of Virginia
Ira B. Schwartz, Naval Research Labs
Carl Simon, University of Michigan
Eduardo Sontag, Rutgers University

Goals of Modeling

A major goal of modeling in epidemiology and public health is to understand and provide feasible forecasts for:

- Estimating the degree to which a disease will spread;
- Understanding the early history of an outbreak;
- Assessing the impact of proposed interventions;
- Optimizing the impact of prevention strategies;
- Improving our understanding of risk factors;
- Assessing the effectiveness of partial protection.

In addition, models provide a solid mathematical framework for analysis and prediction. Moreover, they can be used to improve the design of surveillance systems.

Modeling Techniques

Modeling techniques in epidemiology can be distinguished in various ways: Are they continuum or agent-based? Are they deterministic or stochastic? What is the degree of heterogeneity (space, age, risk, susceptibility, infectivity, contact structure, …). Are they single resolution or multiresolution?

The group emphasized the distinction between continuum and agent-based models and discussed their positive and negative features in general and in the bioterrorism context.

Agent-based models are formulated in terms of the characteristics of and interactions among individuals. The resulting emergent behavior of the system determines the course of the epidemic and the effectiveness of control strategies.

Continuum models are formulated in terms of a dynamical system describing the distribution of a (possibly heterogeneous) population. The resulting emergent behavior of the system again determines the course of the epidemic and the effectiveness of control strategies.

Features of Continuum Models

The positive features of continuum models are:

- Analyzable (based on a rich theoretical foundation)
- Sensitivity Analysis (forward and backward) is readily performed
- Model is defined in terms of available population based parameters
- Efficient prediction of mean behavior in the presence of low amplitude noise

The negative features are:

- Severe limitation on the dimension of the state space (age, risk, susceptibility…)
- Poor information about low probability events (tails of distributions)
- Model cannot handle individual level behavior

Features of Agent-based Models

The positive features of agent-based models are:

- Few limitations on the dimension of the state space (age, risk, susceptibility…)
- Good information about low probability events (tails of distributions)
- Model directly incorporates individual level behavior

The negative features are:

- Few analytical tools (nascent theoretical foundations)
- No backward sensitivity analysis
- Individual level data often has to be derived from population level data
- Computationally less efficient than continuum model

In a bioterrorist context, the positive features, such as incorporating individual level behavior, could be important. But the paucity of analytical tools and the inefficiency of existing computational methods provide challenges to mathematical scientists in order to make these types of models useful in the bioterrorist context, at least in the response phase when response time is critical.

Challenges for the Mathematical Sciences

Such models are already widely used in understanding the spread of various kinds of diseases. Modification of them in a bioterrorist context will require the development of special features. However, it should not require the development of fundamentally new modeling tools. Still, there are some important specific challenges for the mathematical sciences:

- Develop improved tools for understanding geographic spread
- Find ways to mutually calibrate agent-based and continuum models

- Improve significantly the efficiency of computational methods (both software and hardware) for using these models.
- Develop new techniques to evaluate and establish confidence in simulations.
  - Forward sensitivity analysis using techniques such as tangent linear methods
  - Backward sensitivity analysis to answer "how come" questions.
- Develop probabilistic models to improve our capabilities of predicting epidemics where there are only a few infected people.
- Design new approaches to quantify the uncertainty and suitability of models for the transmission of infectious diseases.

In order for these types of tools to become useful in a bioterrorist context will require improved communication between the mathematical sciences community and the public health community on the role of models.

Appendix I

DIMACS Working Group Meeting on Mathematical Sciences Methods for the Study of Deliberate Releases of Biological Agents and their Consequences

First meeting, March 22 - 23, 2002
DIMACS Center, Rutgers University, Piscataway, NJ

March 22:

8:00 - 8:50 Breakfast and Registration

8:50 - 9:10 Opening Remarks

Fred Roberts
Director of DIMACS and co-Chair of meeting

James Flanagan
Vice President for Research, Rutgers University

John Tesoriero
Executive Director, NJ Commission on Science and Technology

Carlos Castillo-Chavez
Cornell University and co-Chair of meeting

Talks: all talks are 15 minutes, with 5 minutes for discussion

Talk Session I (Modeling):

9:10 - 9:30 Ellis McKenzie, NIH
Making Models Make Sense to Policy-makers

9:30 - 9:50 Peter Merkle, Defense Threat Reduction Agency
Biological Modeling and Support to Operations

9:50 - 10:10 John Glasser, CDC
(Joint presentation with M. Reynolds, M.I. Meltzer, B. Schwartz, J.M. Lane, S.O. Foster, J.D. Millar and W.A. Orenstein)
Optimal Response to Deliberate Reintroduction of Smallpox: Design via Mathematical Modeling

10:10 - 10:30 Lone Simonsen, National Institute of Allergy and Infectious Diseases (NIAID), NIH
The Need for Mathematical Models to Make Better Public Health Decisions: A Few Examples from the World of Influenza Pandemic Planning

10:30 - 10:50 BREAK

Talk Session II (Biosurveillance):

10:50 - 11:10 Richard Heffernan, NYC Department of Health
Syndromic Surveillance of Emergency Department Visits, New York City

11:10 - 11:30 Teresa Hamby, NJ Department of Health & Senior Services
Challenges in NJ's Ongoing Surveillance: A Discussion of Current Activities

11:30 - 11:50 Marcello Pagano, Harvard University
(Joint presentation with Marco Bonetti, Karen Olson and Kenneth D. Mandl)
Analyzing Bio-surveillance Data to Increase Vigilance to Bio-terrorism

11:50 - 12:10 Henry Rolka, CDC
Data Mining in Public Health: Issues and Challenges

12:10 - 12:30 David Madigan, Rutgers University
Some Aspects of Adverse Events Detection

12:30 - 1:30 LUNCH

Talk Session III (Biosurveillance, continued):

1:30 - 1:50 Jim Koopman, University of Michigan
Basing Surveillance On Infection Transmission System Theory Rather Than Sampling Theory

1:50 - 2:10 Ira B. Schwartz, Naval Research Laboratory
Mathematical Problems in Biological and Chemical Sensors

Talk Session IV (Mathematical Sciences Tools and Approaches):

2:10 - 2:30 Gary Strong, NSF
The Role of Computer Science in the Defense Against Bioterrorism

2:30 - 2:50 Edward Kaplan, Yale University
(Joint presentation with David Craft and Larry Wein)
Modeling Bioterror Response Logistics: The Case of Smallpox

2:50 - 3:10 Karl Hadeler, University of Tuebingen
The Role of Migration and Contact Distributions in the Spread of Deliberately Released Infectious Agents

3:10 - 3:30 Simon Levin, Princeton University
Mathematical Challenges Posed by Bioterrorism

3:30 - 3:50 Mac Hyman, Los Alamos National Lab
Comparing and Combining Agent Based and Differential Equation Models for the Spread of Epidemics

3:50 - 4:10 BREAK

4:10 - 6:30 Discussion Group Session I
Discussion groups meet separately

Discussion Groups:

The meeting will start with short talks on Friday morning. By late afternoon, we plan to break into "brainstorming groups" to discuss the role of methods of the mathematical sciences in the defense against bioterrorist attacks. The groups will continue their discussions on Saturday morning, drafting brief "white papers" on their topic. We will then ask each group to summarize their conclusions to the entire meeting.

Discussion Group List: Group Topics and Leaders:

Design of Control Strategies
(Combined Modeling Control and Design of Isolation and Vaccination Strategies via Mathematical Modeling)
Leader: Ellis McKenzie and John Glasser
Location: Seminar Room (4th Floor, CoRE 431)

Modeling and Evaluating Bioterrorism Emergency Response Logistics

Leader: Ed Kaplan
Location: Conference Room (4th Floor, CoRE 433)

Biosurveillance
Leader: Marcello Pagano
Location: CoRE A (3rd Floor, CoRE 301)

Modeling Transmission Dynamics with Agent-Based and Differential Equations Models
Leader: Mac Hyman
Location: CAIP 601 (6th Floor, CoRE)

Challenges for Computer Science
Leader: Fred Roberts
Location: CAIP 626 (6th Floor, CoRE)

Agriculture and Food Supply
Leader: Simon Levin
Location: CAIP 726 (7th Floor, CoRE)

Evolution
Leader: James Koopman
Location: Office 404 (4th Floor, CoRE)

6:30 Reception at DIMACS

7:15 Banquet at DIMACS

March 23:

8:00 - 8:40 Breakfast

Talk Session V (Networks, Ideologies, Game Theory, Discrete Math):

8:40 - 9:00 David Banks, FDA
Risk Analysis and Game Theory

9:00 - 9:20 Alun L. Lloyd, Institute for Advanced Study
(Joint presentation with Ira Schwartz, Naval Research Lab and Lora Billings, Montclair State University and NRL)
Disease Spread on Networks: Analogies Between Biological and Computer Viruses

9:20 - 9:40 Carlos Castillo-Chavez, Cornell University
Core Groups, Cooperative Behavior and Peer Pressure: The Dynamics of Fanaticism by Ultra-ideologically Driven Individuals

9:40 - 10:00 Fred S. Roberts, DIMACS, Rutgers University
Challenges for Discrete Mathematics and Theoretical Computer Science

10:00 - 10:15 Break

10:15 - 12:15 Discussion Group Session II

Discussion groups meet, prepare drafts of white papers and prepare presentations to the full group. Same meeting rooms as before.

12:15 - 1:15 LUNCH

1:15 - 4:00 Plenary Session: Discussion Group Presentations

Each group will have 10 minutes to present its draft white paper and then there will be 10 minutes for discussion.

4:00 - 4:05 Closing Remarks
Conference Chairs

Discussion of follow-up meeting(s) and projects

Appendix II

Participants in the DIMACS Working Group Meeting on Mathematical Sciences Methods for the Study of Deliberate Releases of Biological Agents and their Consequences

First meeting, March 22 - 23, 2002
DIMACS Center, Rutgers University, Piscataway, NJ

Jean Marie Arduino, Merck Research Laboratories

Douglas Arnold, Institute for Mathematics and its Applications, University of Minnesota

David Banks, FDA

Sankar Basu, IBM

Lora Billings, Montclair State University

Michael Boechler, Innovative Emergency Management, Inc.

John Bombardt, IDA

Marco Bonetti, Harvard University

Fred Brauer, University of Wisconsin

Adam Buchsbaum, AT&T Labs Research

Donald Burke, Johns Hopkins University

Carlos Castillo-Chavez, Organizer, Cornell University

Alok Chaturvedi, Purdue University

Keith Cooper, Rutgers University

Derek Cummings, Johns Hopkins University

Stephen DiPippo, Center for Communications Research

Joseph DiPisa, Rutgers University

Robert Duncan, University of New Mexico

Richard Ebright, Rutgers University

Irene Eckstrand, NIH

James Flanagan, Rutgers University

John Glasser, CDC

Karl Hadeler, University of Tuebingen

Teresa Hamby, NJ Department of Health & Senior Services

Drew Harris, UMDNJ

Richard Heffernan, NYC Department of Health

Carlos Hernandez Suarez, University of Colima

Donald Hoover, Rutgers University

Mac Hyman, Los Alamos National Lab

Sorin Istrail, Celera Genomics

Mel Janowitz, Rutgers University

Edward Kaplan, Yale University

Thomas Kepler, The Santa Fe Institute

Jon Kettenring, Telcordia Technologies

Mark Koch, Sandia National Labs

James Koopman, University of Michigan

Moshe Kress, Ctr. for Military Analyses (CEMA)

Simon Levin, Princeton University

Alun Lloyd, Institute for Advanced Study

David Madigan, Rutgers University

Ellis McKenzie, NIH

Shailendra Raj Mehta, Purdue University

Peter Merkle, Defense Threat Reduction Agency

William Mills, Federal Government

S. Muthukrishnan, Rutgers University

Roseanna Neupauer, University of Virginia

Mai Nguyen, Federal Government

Rafail Ostrovsky, Telcordia Technologies

David Ozonoff, Boston University

Marcelo Pagano, Harvard University

Manish Parashar, Rutgers University

David Pennock, NEC Research

Fred Roberts, Organizer, Rutgers University

Henry Rolka, CDC

David Rosenbluth, Telcordia Technologies

Estelle Russek-Cohen, University of Maryland

Ira Schwartz, Naval Research Lab

Larry Shepp, Rutgers University

Carl Simon, University of Michigan

Lone Simonsen, NIAID – NIH

Annette Sobel Sandia National Labs

Eduardo Sontag, Rutgers University

Alfred Steinberg, MITRE

Mike Steuerwalt, NSF

Gary Strong, NSF

Stephen Tennenbaum, Cornell University

John Tesoriero, NJ Commission on Science and Technology

Michael Trahan, Sandia National Labs

David Waltz, NEC Research

Daniel Wartenberg, University of Medicine and Dentistry of NJ

Peter Winkler, Bell Labs