Abstract

Over the past two years, disaster preparedness has become an area of intense national focus. The threat of disease outbreaks, from naturally occurring pathogens or those maliciously introduced, has provoked a major response from the biomedical, public health, defense, and intelligence communities. A new information infrastructure and methods to support real time detection and monitoring of diseases, as well as their diagnosis and treatment, has rapidly emerged. This paper addresses the problems and promise of real time biosurveillance, with a particular focus on the role of informatics.

1. Background

1.1 Germ warfare agents

Faced with the very real threat of bioterrorism, the critical need for early detection of an outbreak has shortened the time frame for major enhancements to our public health infrastructure. The Centers for Disease Control and Prevention (CDC) classifies the group of germ warfare agents most concerning, in terms of how easily they could be disseminated to large numbers of people with the potential for causing a major public health impact, as Category A agents. These agents include anthrax (bacillus anthracis), botulism, plague, smallpox, tularemia, and viral hemorrhagic fevers.

The biological features of Category A agents and the clinical effects on their victims require that urgent efforts be focused on the development of methods for early detection and monitoring. The case of an anthrax attack is illustrative. Anthrax has an incubation period of one to six days. The first signs and symptoms resemble those of influenza and include fever, malaise, and fatigue. Within two to three days, patients become severely ill and develop respiratory distress, septicemia, and in about half of the cases, hemorrhagic meningitis. If antibiotic treatment is not initiated prior to the onset of the acute, severe phase of the illness, survival is not likely. However, antibiotic prophylaxis at the time of exposure or treatment during the early phase of the disease is very effective.\(^1\)

1.2 Detection

It is reasonable to assume that a biological attack on a civilian population will be carried out covertly. Hence, the first indication of an attack may be large numbers or smaller clusters of people developing an influenza-like illness between one and six days after the attack. Ideally, if this surge in people with influenza-like illness were detected at the early possible moment, a large scale public health response would be mobilized to initiate treatment of all those exposed.

A model developed by the Department of Defense Advanced Research Projects Agency (DARPA) and the Johns Hopkins Applied Physics Laboratory projects that fatalities resulting from a covert anthrax attack on the New York City subway system would be reduced by a factor of seven if an active surveillance system was in place. The same study found that with a communicable, highly contagious disease such as smallpox, an active surveillance system might reduce mortality by seven fold.

An infrastructure to support fundamental change in the health care system must therefore include real time information about regional disease patterns, health care processes, and health related behaviors. Current health information systems fall far short of this capability,\(^2\) despite readily available information technology to process patient data. The Federal focus on preparedness for bioterrorism, which was sharpened after the 2001 anthrax mailings, has thrown into greater relief the problems we face when providing health care and protecting the public health in the absence of real time information.\(^3\)
2. Biosurveillance

2.1 Approaches to surveillance

The goal of biosurveillance is to identify biological weapons before they are used or as soon as possible after release. There are five major approaches to biosurveillance for germ warfare attacks including monitoring the environment, animals, agriculture, the citizenry, or patient populations.

Once an attack has occurred, surveillance of the environment provides the earliest possible warning of a germ release into, for example, the ventilation system of an office building. Detection systems such as those employing laser-induced fluorescence and immunologically based bioelectric sensors have been shown to be highly sensitive to germ releases.

Animals and agriculture are prime targets for bioterrorism. The recent extensive outbreak of foot and mouth disease in Great Britain illustrates the devastating economic and social impact that such an attack could have.

The citizenry may be observed, polled, or examined. For example, surveillance video at Carnegie Mellon University is being analyzed to measure the frequency of coughing, a sign of illness and a potential early sign of serious illness, in public places. Telemarketing and the emerging field of consumer informatics enable surveillance of the ever growing population of Internet users.

Behaviors of the citizenry, when their health is affected, may leave imprints on certain data sets. The principal underlying premise of these systems is that the first signs of a covert germ warfare attack will be clusters of victims who change their behavior because they begin to feel ill. When people become sick, they may make purchases such as Kleenex, orange juice, and over-the-counter cold remedies. They may stay home from school or work. The Defense Advanced Projects Agency has had an interest in monitoring the health of the population through “non traditional” data sources, such as grocery sales, sales of over-the-counter medication, and rates of absenteeism.

The next phase of detectable activity is likely to be encounters with the health care system. Patients may phone in to nurses or physicians. They may visit primary care settings and emergency departments. They may be hospitalized. Some may die. All of this activity may precede the first confirmed diagnosis of a germ warfare victim.

2.2 Syndromic surveillance

One recent approach to the problem of how to recognize an attack as soon as possible has been the development of syndromic surveillance systems. Syndromic surveillance relies on data that are available before the diagnosis of the individual patient and would precede recognition that there has been an attack.

These victims may initially have behavioral patterns, symptoms, signs, or laboratory findings that can be tracked. If the germ warfare attack involved anthrax, a syndromic surveillance system looking for evidence of a surge in influenza-like illness could provide an early warning and a tool for monitoring an ongoing crisis. By detecting a surge in patients with flu-like symptoms, a public health authority can be warned early of an anthrax attack, enabling prompt case identification and treatment.

One approach to syndromic surveillance of emergency department populations has been drop-in surveillance as practiced by the CDC. Drop-in surveillance was implemented by the CDC at the World Trade Organization Ministerial (Seattle, Washington) in 1999, and at the Super Bowl (Tampa, Florida) and World Trade Center Attacks (New York, NY) in 2001. Drop-in surveillance is accomplished by staffing the emergency departments around an area thought to be at high risk of an attack. Health care providers use a paper form to indicate whether each patient fits a particular syndrome of concern. At the World Trade Center, the syndromes tracked were anxiety, asthma, botulism-like, death, gastrointestinal, inhalation, neurological, rash, respiratory, sepsis, and trauma.

There are limitations to drop-in surveillance as it has recently been practiced. The very nature of the method assumes that the time and location of an attack can be predicted. Furthermore, reliance on manual processes produces incomplete and at times inaccurate data.

There has been substantial recent success in developing systems to enable automated data collection for real time syndromic surveillance in Boston, Pittsburgh, Indiana, Seattle, New York and other metropolitan areas. These systems exploit data from hospital information systems, pharmacies, emergency medical services, and other sources. However, designing automated systems and interpreting their output poses substantial methodological challenges.

3. Methodological challenges

3.1 Data quality

The quality of the data used in automated systems varies. Establishing new manual data entry processes to collect new data (effectively, relying on human intelligence) is difficult and costly. Therefore, the most successful syndromic surveillance systems to date rely on information collected for other purposes.

The Joint Commission on Accreditation of Healthcare Organizations requires emergency departments to record
diagnostic data, including chief complaints (the patient-reported reason for the health care encounter). International Classification of Disease (ICD) codes are universally used for billing. When stored electronically, chief complaints and ICD codes often become available in databases during or shortly after a patient’s visit, in a time frame that can support real time surveillance.

Codes are grouped together into categories consistent with syndromes of interest. For example, a chief complaint of cough would be included in an influenza-like illness syndrome group. The mapping of these codes to syndromes of interest is imprecise. The degree of imprecision is, however, measurable against a gold standard such as a physician chart review of the case.13, 14

Another issue is the timeliness of the data. To support real time detection, data must be available immediately. Chief complaints, when stored electronically, are generally available instantaneously. ICD codes may not be assigned to patient visits for hours, days or weeks, depending on the specifics of the visit and the local practices at the hospital.

There are also important issues with the quality of geographical location data. Geographical information system (GIS) software can translate an address into precise latitude and longitude coordinates. In general, in the health care system, the only address reliably collected is the home address. Ideally, a surveillance system should have access to data about where each individual works, goes to school, and has been recently. If an attack were to occur at a baseball game, for example, the home address may not be the most salient geographical feature of the patients, but rather a cluster of patients who had attended the game might be identified.

Even the home address may be entered inaccurately, making geocoding a challenging task. In hospital information systems, new patient addresses may permanently overwrite older ones, making the historical geographical patient distributions difficult to reconstruct. Also, the accuracy of geocoding results is far from perfect.15

3.1 Data standards

A problem that plagues health care information technology generally, and bioterrorism surveillance specifically, is a lack of universal standards for storage and communication of medical information.16, 17 Chief complaints are a good example. If they are even stored electronically, they may be stored as free text or as codes. Coding systems might be developed locally or might attempt to follow a more universally agreed upon coding systems such as ICD codes, which while universal, are not particularly well suited to describing chief complaints. Sharing information across systems requires a standardized method for describing data and their organization. Models for data exchange are being developed for health care,18 emergency medicine,19, 20 and public health.21 The National Electronic Disease Surveillance System (NEDSS) is a standards-based approach to connect public health and clinical medicine. As its implementation proceeds, NEDSS will help standardize and facilitate the transfer of information needed for public health from clinical information systems.

3.2 Disease Modeling

To recognize a cluster in time or space, a thorough understanding of the normal patterns of disease is required. Figure 1. Daily emergency department visit rates at a single institution over 10 years

Having several years of historical data at the surveillance sites is quite useful in this regard. Many health care datasets show regular and predictable periodicities. For example, annual periodicities in daily emergency department visit rates, with peaks in the winter, are shown in Figure 1. More detailed analysis revealed several periodicities, related to month and day of the week.22, 23 External variables, such as the weather have an impact as well.

To establish normal patterns of spatial relationships among patients, one must account for local variations as well as secular trends in population density, hospital catchment areas, and shifting referral patterns.

Detecting abnormal signals using temporal methods may rely on classical time series modeling (autoregressive moving average models), dynamic Bayesian clustering models to identify change points,24 and on tools from the quality control discipline, such as the CUSUM method.

Detecting abnormal clusters in space poses substantial challenges. In classical geographical cluster detection for public health and epidemiology, a specific cluster is often being investigated, and the goal is to identify a point source, such as a toxic waste dump causing an excess number of cases of leukemia.25 Diseases such as leukemia have excellent case definitions and cases may accumulate over years to form a cluster. In syndromic surveillance, detection is less straightforward. In general, one looks widely for...
abnormality, perhaps with no hypothesis about where the outbreak will occur. By their nature, syndromic surveillance systems are very noisy, given the imprecision in case definitions. And rather than looking for cases in a region over years, the syndromic systems monitor rapidly shifting distributions of patients within an ill-defined window of hours to days.

3.3 No training data

Fortunately, few people have been infected with germ warfare agents although there are notable exceptions such as the people of Sverdlovsk exposed in 1979 during an accidental release of anthrax from a weapons plant, and those involved in the Florida, New York and Washington DC mail attacks in 2001. However, with few actual cases, syndromic surveillance systems cannot “learn” to detect bioterrorism with real world data. Nor can systems be benchmarked by their ability to detect actual attacks. These systems must be trained with non-bioterror related events or simulated events instead.

The performance of a syndromic surveillance system can be evaluated by measuring its ability to detect signal (disease outbreak) against a background of noise (normal variation in baseline disease rates in the region). To benchmark performance, training and validation data containing signal and noise are required. These data can be samples of authentic regional data, simulated data, or a combination of both.

3.4 Tuning for a particular attack

Attacks may produce signals in the data that have different shapes. For example, in a syndromic surveillance system that tracked the daily emergency department rates illustrated in Figure 1, an attack might be characterized by a short high spike, a sustained low and flat signal, or an exponentially increasing high amplitude signal. Different methods, and different applications of methods, such as using varying temporal filters, may strongly influence detection capabilities. Therefore, a host of distinct methods may ultimately need to be simultaneously applied to the same data streams to enable the detection of all possible forms of attack.

3.5 Signal Integration

Obviously, a detection system with poor sensitivity, one that fails to detect most attacks, is not acceptable. However, in determining alarm thresholds, one must trade off sensitivity against specificity, ensuring that most alarms are real. Consequently, the more attacks one aims to detect, the more false alarms one must accept. Multiple false alarms can be detrimental, however, depending on what actions are taken when an alarm is triggered.

Using more than one signal stream may help to reduce false alarms. For example, if visits for influenza syndrome increase, but so do actual cases of influenza, there may not be a cause for alarm. If the two signal streams diverge, however, there may be more cause for concern.

Ideally, a regional or national command center would act based upon an interpretation of multiple streams of data, whether they come from completely different sources (e.g. hospital visits, school absenteeism, sales of over-the-counter medication) or from different models of a single data source.

Substantial work is needed to develop methods for such signal integration. Integration must be accomplished for: signals from same data using multiple methods, signals from separate but potentially correlated data streams, signals from overlapping geographical regions, and signals from remote geographical regions.

3. Conclusions

The precise role and efficacy of biosurveillance in public health has yet to be determined. Syndromic surveillance systems as they existed to date in the New York City and Washington DC areas failed to detect the anthrax attacks of 2001. While these attacks affected only a small number of people, they nonetheless are a cause for humility for anyone attempting to predict with certainty when, where, and how bioweapons will be used. Astute clinicians will always play a role in the accurate diagnosis and treatment of patients as well as in the identification of public health emergencies. However, biosurveillance is another modality that clearly has the ability to detect certain kinds of events. The work to be done over the coming months and years is to build our data integration infrastructure, develop and refine our methods, and estimate to the best of our ability, the promise and limits of our technology.

Acknowledgements

This work was supported in part by Contract 290-00-0020 from the Agency for Health Care Quality and Research as well as by Contract N01-LM-9-3536 from the National Institutes of Health, National Library of Medicine )Next Generation Internet Initiative)

References

1. U.S. Army Medical Research Institute of Infectious Diseases. USAMRIID’s Medical
15. Olson KL, KD. M. Use of geographical information from hospital databases for real time surveillance {abstract}. Pediatric Research. 2002;51((No 4 Pt 2)):94a.
22. Reis BY MK. Characterizing the relationships between seasonal components of pediatric ED volume {abstract}. Pediatric Research. 2002;51((No 4 Pt 2)):95a.
