Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2003 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2003

The Use of Information Management/Information Technology in the War Against Bioterrorism

Russell Smutz
Army Medical Department Center and School

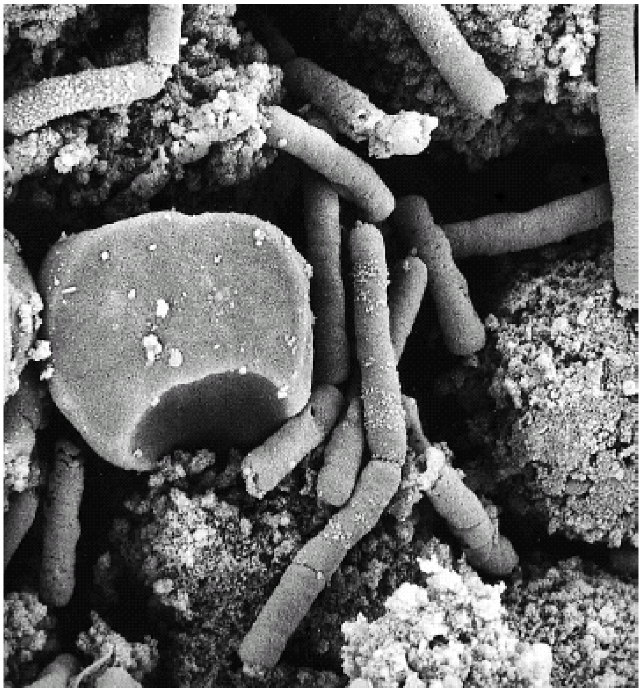
The Use of Information Management/Information Technology in the War Against Bioterrorism

Major Russell P. Smutz
Army Medical Department Center and School
russell.smutz@amedd.army.mil

Abstract

Twenty-five thousand fans crowd a park in New York City to hear a popular rock group give an outdoor summer concert. In all the noise and fun nobody notices two men driving a pickup truck bearing official city markings around the periphery of the park. Mounted on the back of the truck, a fog machine sprays a steady stream of thin vapor into the air. The people in the park have just been exposed to anthrax. The above theoretical scenario has become a frightening possibility. To be able to deal successfully with a covert bioterrorist attack, the medical system must be able to intervene as early as possible. That means they must detect an event that has been designed to be difficult to detect. The key to this detection is syndromic surveillance, the collection and analysis of patient symptom data. Used properly, syndromic surveillance can detect anomalies in the occurrence of key symptoms. Because of its artificial method of spread, a bioterror disease will produce these anomalies. Syndromic surveillance can form the core of a county-wide public health information system. Such a system links hospitals, private physicians, and other health care providers with public health officials, both locally and at the state and federal level. It can aid public health officials in detecting and successfully reacting to a bioterrorist attack. Such a system has the added benefit of aiding the health care system in detecting and successfully reacting to naturally- occurring disease outbreaks.

Introduction



It's Saturday afternoon. Twenty-five thousand fans crowd a park in New York City to hear a popular rock group give an outdoor summer concert. In all the noise and fun nobody notices two men driving a pickup truck bearing official city markings around the periphery of the park. Mounted on the back of the truck, a fog machine sprays a steady stream of thin vapor into the air. Had anyone asked, they would have been told that the men were spraying for mosquitoes to reduce the danger of West Nile Virus disease. By nightfall, the two men, along with the truck and fogging device are in another part of the country. By Tuesday night many people who were at the concert begin to visit their local emergency rooms and their private physicians, complaining of coughs, sore throats, and other symptoms that the patients and their physicians associate with a severe or the flu. The sudden influx of patients, all reporting the same symptoms, is dispersed among the hospitals and clinics throughout the city. No one physician sees enough of an increase over the normal numbers of patients to be able to detect anything out of the ordinary. By Wednesday night, more than 3000 concertgoers have begun to complain of symptoms, and the first signs of respiratory collapse have appeared in the more susceptible patients. Only at this point, four days after the concert, is the medical community becoming aware that something out of the ordinary is taking place. By Thursday night the first deaths have occurred and the first tentative diagnoses of anthrax have been made. By the following Monday, 1276 people have died. The population is in panic, as thousands abandon the city. Tens of thousands crowd local hospitals, demanding prophylactic antibiotics. The city medical and emergency response systems are overwhelmed as doctors struggle to deal with a disease that few have ever encountered in their careers.

Two years ago, the above scenario would have merely been the stuff of some spy novel or action movie. Since that time things have changed dramatically. In the months following the September 11 attacks on the World Trade Center and the Pentagon, the people of the United States awoke to a new danger. Envelopes containing the spores of *Bacillus anthracis*, the causative agent for anthrax, were mailed to members of congress and media offices in New York and Florida in a deliberate attempt to infect people at those locations. Bioterrorism had come to America. Actually, it had been here for some time. In the 1700s the British used smallpox-laced blankets in their wars against the North American Indians (Thornton, 1987). More recently, in 1984 the Oregon-based Rajneeshee cult deliberately infected restaurant salad bars in the town of The Dalles with *Salmonella typhimurium* bacteria. The contamination gave 751 people diarrhea. Their apparent motive was to sicken local voters, keeping them home, and allowing the cult to win a local election and take over the county (W. Seth Carus, 1997).

The bioterrorist uses organisms or toxins from living organisms to attack people, animals, or crops. They use disease as a weapon to create casualties and to spread panic and social disruption. Biological weapons offer many advantages to the terrorist. The technology required for their production is not especially complicated or bulky. The delayed onset of symptoms from biowarfare diseases makes them ideal for covert attacks. The delay also makes it easy for the attackers to escape undetected. Finally, biological weapons can be extremely effective. A study conducted by the World Health Organization estimated that 50 kilograms of dried anthrax spores, released in an aerosol in a city of one million, would kill at least 36,000 people, and leave another 54,000 incapacitated. Consider that the September 11 attack on the World Trade Center, which killed approximately 2800 people and injured another 2500-3000, required medical and emergency resources from all over the East Coast. A successful biological attack on an American city would overwhelm the medical and emergency infrastructure of the entire region. Even if few people died, the fear and panic caused by this kind of invisible attack would be all that a terrorist could dream of.

Effects of Treatment Delays

In the event of a bioterrorist attack, the medical community's ability to mitigate the effects of the attack will be significantly affected by the speed of its detection and subsequent treatment. Any delay in response and treatment will translate as more casualties and, potentially, more deaths. The window during which intervention will be successful is surprisingly narrow. A biological warfare disease simulation developed by the Office of the Army Surgeon General models the effect on the percentage of exposed soldiers who will become casualties based on how soon after the attack prophylactic antibiotics are initiated. As shown in Figure 1, if the attack was immediately detected and all exposed personnel were administered antibiotics, essentially zero percent would become casualties. However, if the attack was not actually observed or detected by medical monitors, the first indication of exposure would be the appearance of initial symptoms after the disease's incubation period. In the case of anthrax, this generally occurs on the third day after exposure. By the time that symptoms appear, even if prophylactic antibiotics are immediately initiated, 29% of the exposed personnel will become medically significant casualties. If administration of antibiotics to all exposed personnel is delayed by another 24 hours (day 4), the casualty rate will rise to approximately 70%. By day 5, it will rise to 88%. Assuming that symptoms show up on day 3, day 5 will be the soonest that a clinician can confirm an anthrax diagnosis with traditional lab work.

The model shown in Figure 1 was born out by the anthrax attacks in Florida, New York/New Jersey and Washington D.C. during the fall of 2001. Those victims whose exposures were quickly detected, mostly workers in the Senate Office Building, received immediate antibiotic therapy and escaped the development of symptoms. Those victims whose exposures were not immediately detected, mostly workers in post offices, did not receive prophylactic antibiotics prior to the appearance of their symptoms. They became ill and, subsequently, four died. It should be noted that the early detection of the anthrax exposures was largely due to the clumsy nature of the attack, rather than to any attribute of the medical system. The anthrax spores were poured into envelopes and delivered through the mail. When the envelopes were opened, the spores fell out and contaminated whoever happened to be nearby. As the envelopes made their way through the postal system, they also leaked some of the spores, contaminating the postal workers. Once the medical system and the public were alerted to the dangers of these attacks, they became rather easy to detect. But even with this unsophisticated delivery method, the attacks contaminated over a dozen people and killed four. Additionally, they severely hampered the postal delivery system and caused an estimated 30,000 people across the country to receive prophylactic antibiotics, most unnecessarily. In the hands of a more sophisticated terrorist, anthrax, which lends itself easily to aerosol delivery, could infect thousands of people in a single covert attack. Such an attack could prove difficult to detect until victims started reporting symptoms.

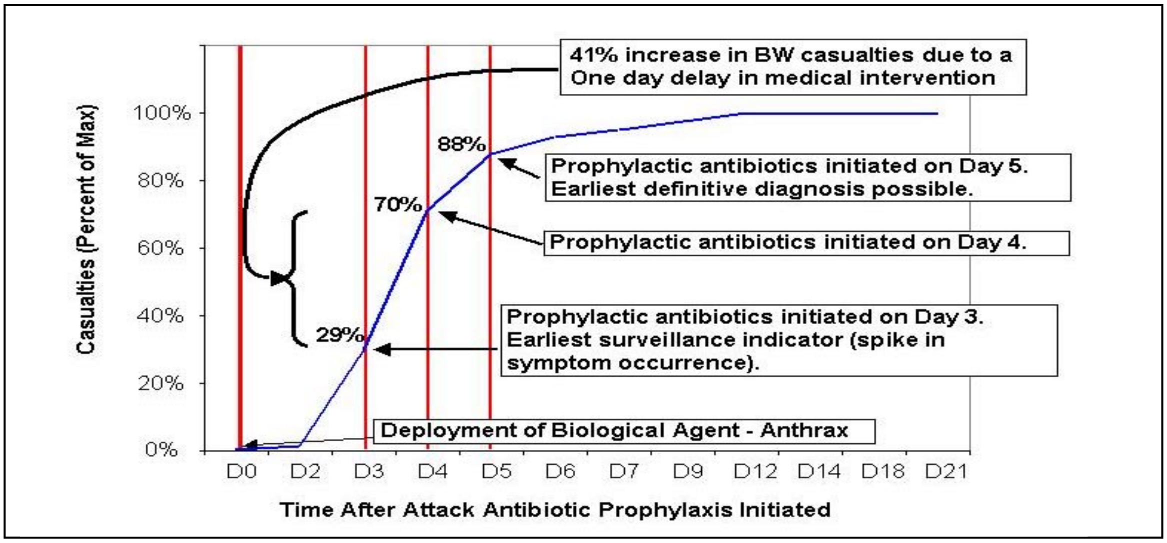


Figure 1. Affects of Medical Intervention Delay on Biological Warfare Casualty Rate
(modified from Schnelle, 2001)

Obviously, to provide optimal care, the medical community must detect a bioterrorism attack as early as possible. It must not only determine the time and location of an attack, but also determine those facts quickly enough to make a difference. Once it has been recognized that an unusual medical event has occurred, the medical community must accomplish the following (Giovachino & Carey):

- Obtain lab confirmation of a possible bio-warfare disease
- Poll other medical treatment facilities to determine whether cases have occurred
- Determine the affected population (determine time and place of the exposure)
- Advise public officials
- Quickly provide prophylaxis for emergency workers
- Set up telephone and internet information systems to keep the public informed
- Set up mass prophylaxis sites
- Identify and locate homebound people who need prophylaxis or treatment
- Determine what, if any, decontamination might be required
- Determine any special requirements for the elderly or very young

Unfortunately, the early symptoms of anthrax, like those of many other potential biowarfare agents, are largely indistinguishable from those of common illnesses, such as the flu or other relatively minor respiratory ailments. Few clinicians are experienced in recognizing, let alone treating, most of the diseases that are likely to be used by a bioterrorist. The medical community is faced with the choices of a) waiting until definitive symptoms of a biological warfare disease appear before taking action, b) treating every patient as a potential biowarfare victim and administering prophylactic antibiotics whenever there is the slightest doubt as to the origin of the disease, or c) developing a surveillance system to differentiate between naturally-occurring diseases and bioterrorism. Choice a) will result in a delayed response to an actual bioterrorism attack, with the consequential increase in sick and/or dead. Choice b) could potentially reduce the number of sick or dead, but at the price of many people receiving unneeded antibiotics. This indiscriminate use of antibiotics would be expensive, would increase the risks of side reactions, and could eventually reduce the efficacy of the antibiotics. Only choice c) offers the potential of a timely and appropriate reaction to a bioterrorism event.

Medical Surveillance

The problem of detecting a bioterrorism attack can be divided into two time periods; the period from the moment the attack occurs until symptoms appear in the victim population, and the period after symptoms begin to appear. Detection during the first period will depend on biological detectors, indicators collected by the law enforcement community, and indicators collected by the medical community. Biological detectors are devices, mostly developed by the military, which gather air or water samples and test for the presence of specific disease pathogens. They are a direct indicator of a bioterrorism attack. Unfortunately, their efficacy is limited by their placement. An air sampler must be in the path of a cloud of wind-borne pathogens to be able to detect them. The detector must also be sensitive to the particular pathogen used in the attack to be effective. Despite these limitations, biological detectors will become increasingly important in protecting our population centers from bioterrorism attacks. Indicators collected by law enforcement officials include eyewitness accounts of the attack and physical evidence such as discarded equipment. Evidence of this nature is especially valuable in the subsequent search for those responsible for a bioterrorism attack. Finally, indicators of a bioterrorism attack collected by the medical community include such items as increases in the numbers of sick and dead animals seen by veterinarians, sudden increases in school and work absenteeism, and sudden increases in the sales of non-prescription drugs. These indicators are based on the facts that for many diseases small animals serve as an early warning, and that most people will attempt to treat themselves with rest and non-prescription drugs prior visiting a doctor or emergency room. This is especially true for diseases whose early symptoms are relatively minor.

Naturally Occurring Disease Patterns

The problem of detecting a bioterrorism attack after symptoms begin to be reported to the medical community is one of differentiating between the early symptoms of a bioterrorism disease and those of common ailments. While the symptoms for an individual exposed to a biological warfare agent are often difficult to discern from those of a naturally occurring illness such as the flu, the pattern of symptoms seen in a bioterrorism attack does not look like the pattern of symptoms seen in a naturally occurring disease epidemic. Figure 2 shows the pattern of respiratory symptoms for a notional influenza outbreak. As the outbreak starts, the numbers of new cases each day builds rapidly and then remains fairly steady. This is because the influenza virus is present over a fairly long period of time; so new victims are infected over a fairly long period of time. Eventually, the disease begins to die out in the population, and the number of new cases tapers off.

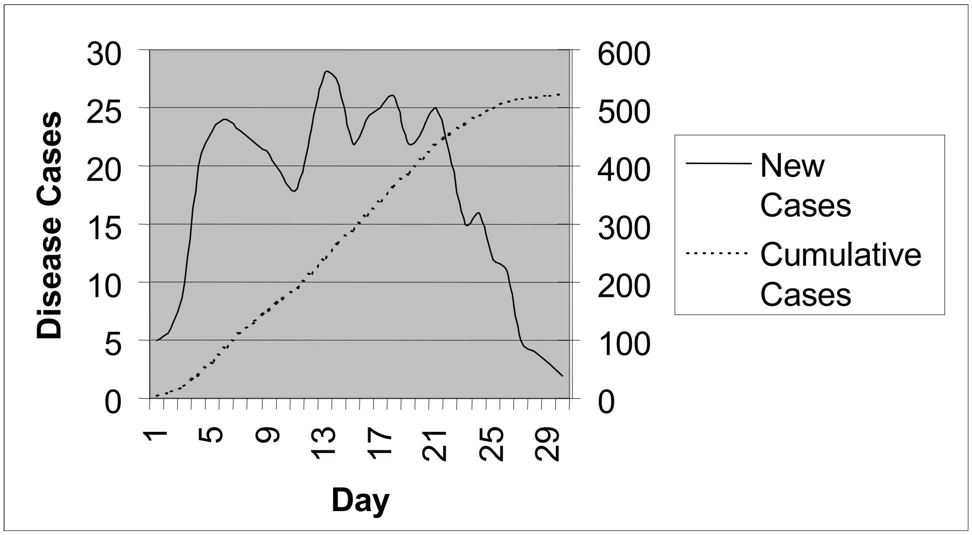


Figure 2. Pattern of New Complaints of Respiratory Symptoms (Notional Influenza Outbreak)

In a naturally occurring outbreak, the dispersion of victims is random. Figure 3 shows a city map on which the residents of our flu victims are shown as red stars. The stars are spread all over the city. They clump in residential areas, but are spread all over the city. When the victim's work locations or recent movements are mapped, no definitive pattern emerges. There may be clumps seen at locations where people tend to gather, such as work places, malls and transportation hubs. These are locations where, because many people gather in close proximity, it is easy to become infected. However, the overall dispersion pattern is still fairly diffuse.

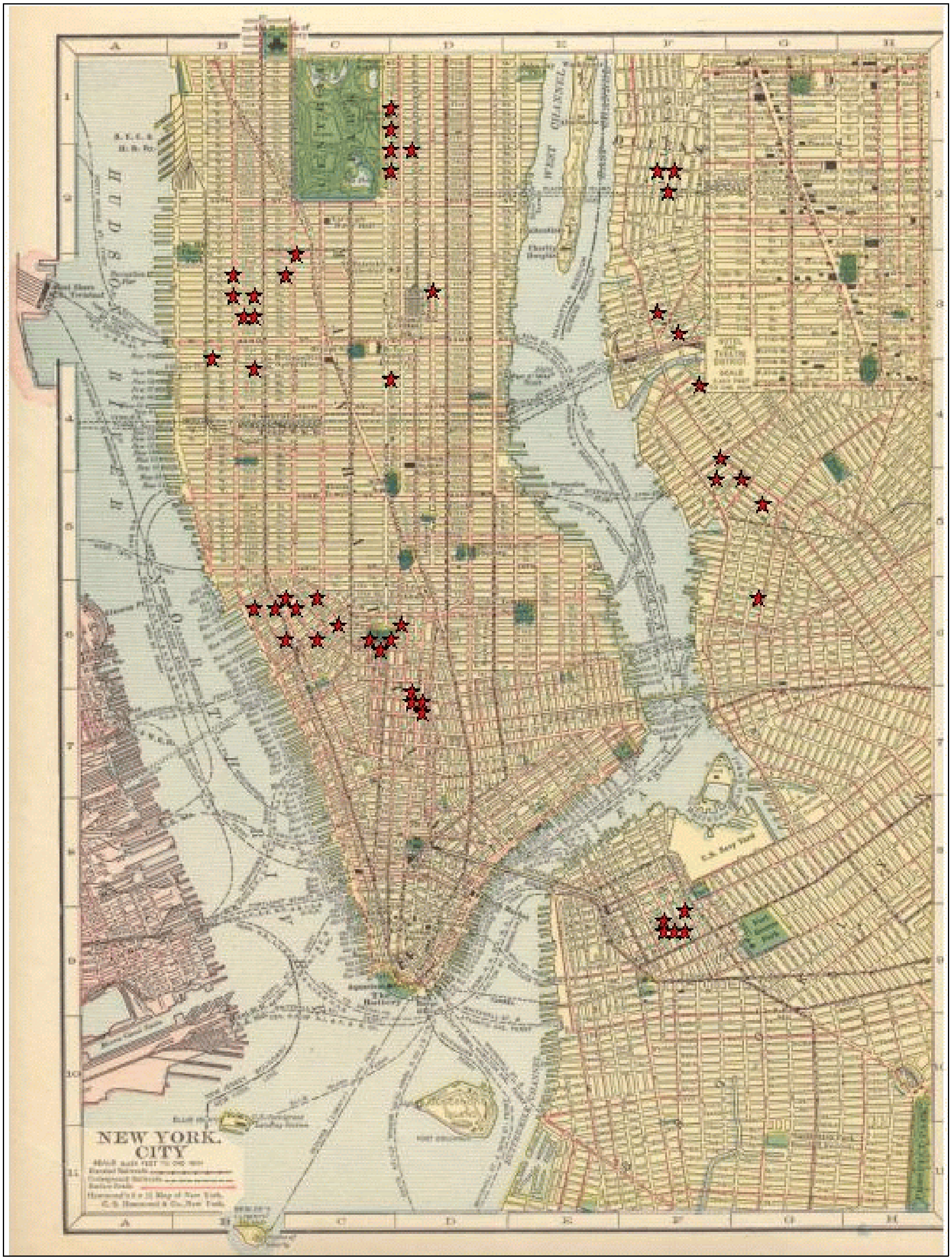


Figure 3. Pattern of Symptoms in a Naturally Occurring Disease Outbreak

Bioterror Disease Patterns

The pattern of new victims seen in a bioterrorism attack is quite different. While in a naturally occurring disease outbreak people are exposed to the disease over a relatively long period of time, in a bioterrorism attack all of the victims are exposed at the same time. While some victims will be more susceptible to the disease, and others less, most will become ill at about the same time and will all seek medical aid over a relatively short period. Thus, even if the symptoms of the bioweapon are similar to normal diseases, the medical community will experience a sudden significant spike in new patients. Figure 4 shows the pattern of respiratory symptoms for a notional bioterrorism attack using anthrax as the bioweapon. The chart assumes a background level of respiratory symptoms from naturally occurring diseases. After the incubation period following the attack on day 10, the number of patients presenting respiratory complaints spikes very dramatically, holds for a short period, and then drops back to the normal background level.

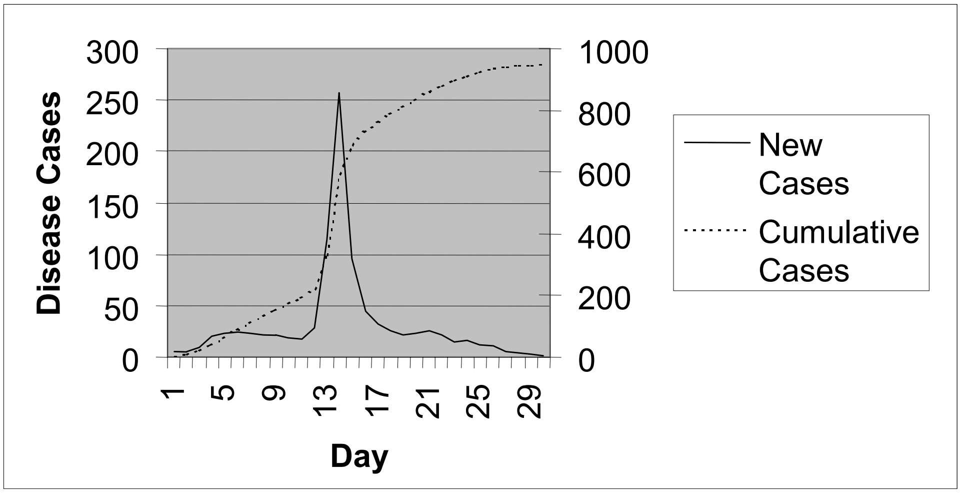


Figure 4. Pattern of New Complaints of Respiratory Symptoms (Notional Anthrax Attack)

The pattern of victim dispersion in a bioterrorism attack is also quite different from that seen in a naturally occurring disease. By its very nature, a biological warfare agent is a point weapon. To be effective, it has to be released at a location where there are people to infect. To get the maximum effect the location selected should be where many people gather. Depending on the location of the attack (in a residential area, a local mall, a commercial area, etc.), mapping the victim's residences could produce a dispersion pattern similar to that seen in a naturally occurring disease. However, tracing the victim's recent movements will eventually disclose a common location and a dispersion pattern similar to that shown in figure 5. In our notional anthrax attack the strike occurred in a city park, during a concert.

It should be noted that the symptom and victim dispersion patterns shown in figures 2 through 5 make several assumptions. For both the natural epidemic and the bioterrorism attack it was assumed that the disease was not contagious. Secondary infections in either a natural epidemic or bioterrorism attack produce a pattern that is much less clear. The symptom and victim dispersion patterns for the anthrax attack also assume a single attack, at a single location, on a single day. Multiple attacks, especially if they are conducted over multiple days, will make the symptom spike much wider and will produce several dispersion clusters on the map.

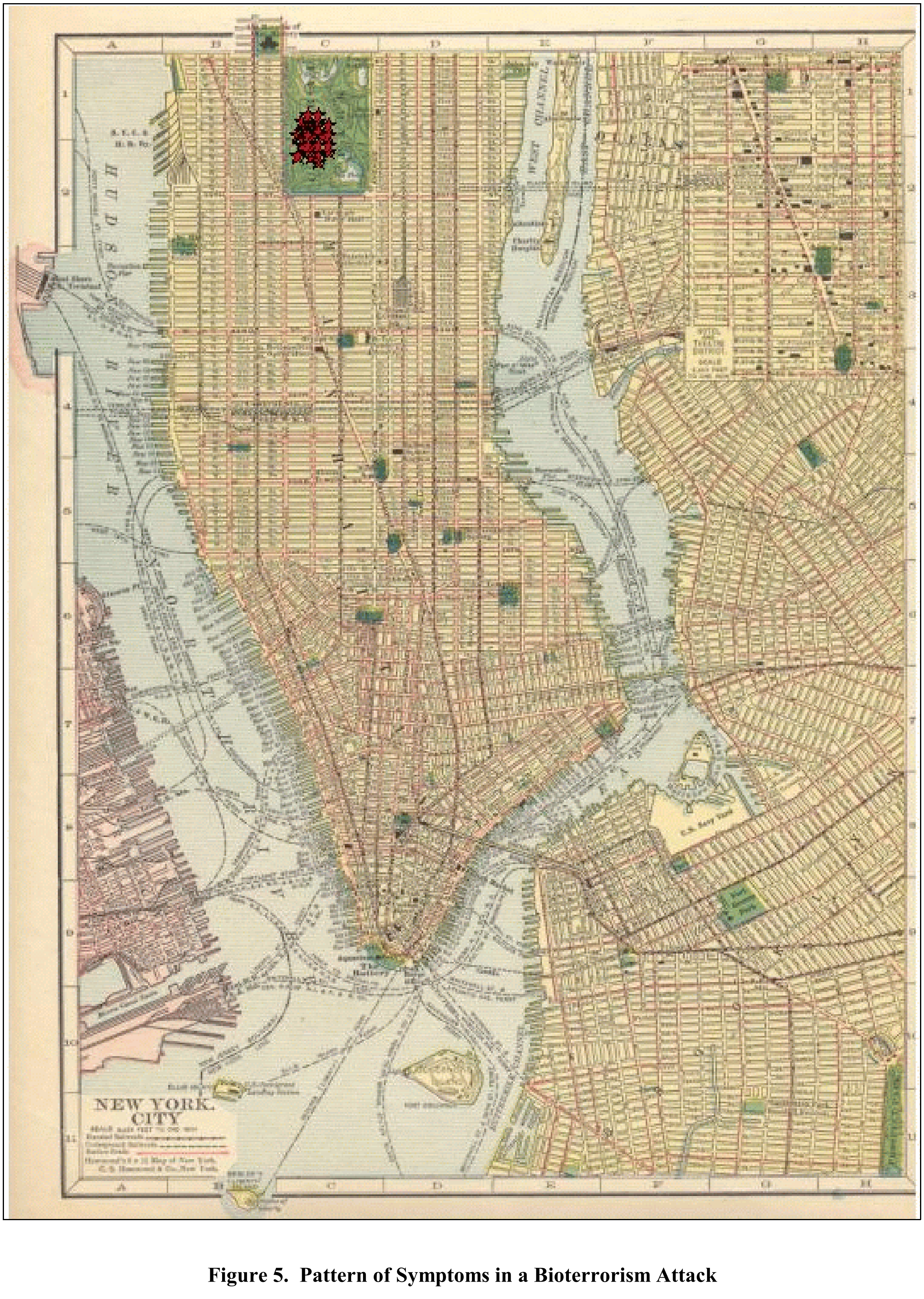


Figure 5. Pattern of Symptoms in a Bioterrorism Attack

Information Management/Information Technology

Syndromic Surveillance

The role of information management and information technology in the fight against bioterrorism is in bringing together all of the available information in a form that allows the medical/public health system to detect the presence and extent of a bioterrorism event and to intervene in a timely manner. The graphs and maps of symptom data shown above are not possible at this time. While current public health regulations require hospitals and clinics to report certain diseases including those most likely to be used in bioterrorism, these reports are based on diagnoses. Hospitals and private practices report by diagnosis primarily because that is how they bill. As shown in figure 1 and the 2001 anthrax attacks, by the time that a definitive diagnosis can be made, it is too late to help many of the victims. Medical surveillance by diagnoses also suffers from the problem that different medical practitioners may diagnose a given collection of symptoms as several different conditions. A more useful method of medical surveillance is syndromic surveillance, the search for trends and patterns in the occurrence of symptoms (Thompson, 2003). While effective treatment of a bioterror disease in an individual does require a diagnosis, detection of the possible presence of the disease in a population can be done more efficiently by symptoms. Syndromic surveillance offers several advantages.

- Syndromic surveillance is timelier than diagnoses surveillance, allowing the medical system to intervene earlier, with the potential of saving more lives.
- While the formation of a diagnosis requires a physician, the detection of symptoms does not. This allows data collection from sources such as school nurses, factory clinics, pharmacies, and self-reporting by the victims themselves.
- The reporting of symptoms is less subjective than the formation of diagnoses.
- The sharing of anonymous symptom occurrence data does not create the same privacy law issues as the sharing of individual diagnosis data.

A robust syndromic surveillance would be one in which symptom occurrence data is collected from hospitals, clinics, private practices, school and factory nurses, nursing homes, and nurse telephone triage systems throughout a region. The data would be aggregated and a normal baseline occurrence for each of the reportable symptoms would be established. A running average for each symptom would be maintained and monitored for deviations from the background norm. If a deviation were to exceed a set parameter, the regional public health officials would launch an investigation to look for further evidence of a bioterrorism event. This would begin with looking at the geographic distribution of the reports that constituted the spike. If the geographic distribution did not appear to be random, the public health officials would then contact the medical personnel who reported the data to obtain further information about their patients. At some point in this investigation, the surveillance would transition from surveillance of anonymous aggregated symptom data to specific personal health data. The medical privacy laws allow for this type of inquiry and loss of confidentiality in the event of a perceived public health threat. As the evidence of a bioterrorism event built, the public health officials would be able to use the symptom dispersion data to help determine the population at risk. This would be important in the event that a decision was made to dispense prophylactic treatment. The events of fall, 2001 showed that the medical community would be faced with the challenge of separating out those who truly need prophylaxis from a much larger population of "worried well" who have not been exposed and do not require prophylaxis.

Preliminary work has been done on the development of syndromic surveillance systems. The National Electronic Disease Surveillance System (NEDSS) (**www.cdc.gov/nedss/about/organization.htm**) is an initiative that promotes the use of data and information system standards to advance the development of efficient, integrated, and interoperable surveillance systems at federal, state and local levels. It is a cooperative effort between the Centers for Disease Control and Prevention and many state and local public health systems. While a good start, most communities do not currently possess any sort of community-wide medical surveillance system. With the creation of the Department of Homeland Security and the restructuring of much of the government to make it more responsive to homeland security issues, new emphasis and financial support has been placed behind the creation of local surveillance systems, and the linkage of these systems to state and federal information networks.

Public Health Information Systems

Need and Architecture

While the development of a local medical surveillance system is important, it is only part of the solution. As discussed earlier, syndromic surveillance only comes into affect once victims begin to present symptoms. Prior to that point there can be other indicators of a potential attack, collected by the law enforcement and medical community. The public health and medical systems need both sources of information to perform there mission effectively. They need the pre-symptom indicators to give them as early a warning as possible, and they need the syndromic data to further develop that warning and to help them determine the population at risk. Once it has been determined that a bioterrorism has or even may have occurred, the same information system should link to the local emergency response systems so that responding personnel have all information required to react in a coordinated and appropriate manner. Finally, the locally collected data should feed public health systems at the state and federal level so that any response by state or federal emergency response agencies is well coordinated with the local efforts and to determine whether the local situation is part of a larger problem. To accomplish all of these tasks each community needs to develop a public health information system that gathers pre and post-symptom data, presents this data in a form that facilitates analysis and decision making, links with the emergency response community, and links to higher level public health information systems at the state and federal level. Figure 6 shows the high level architecture of such a system.

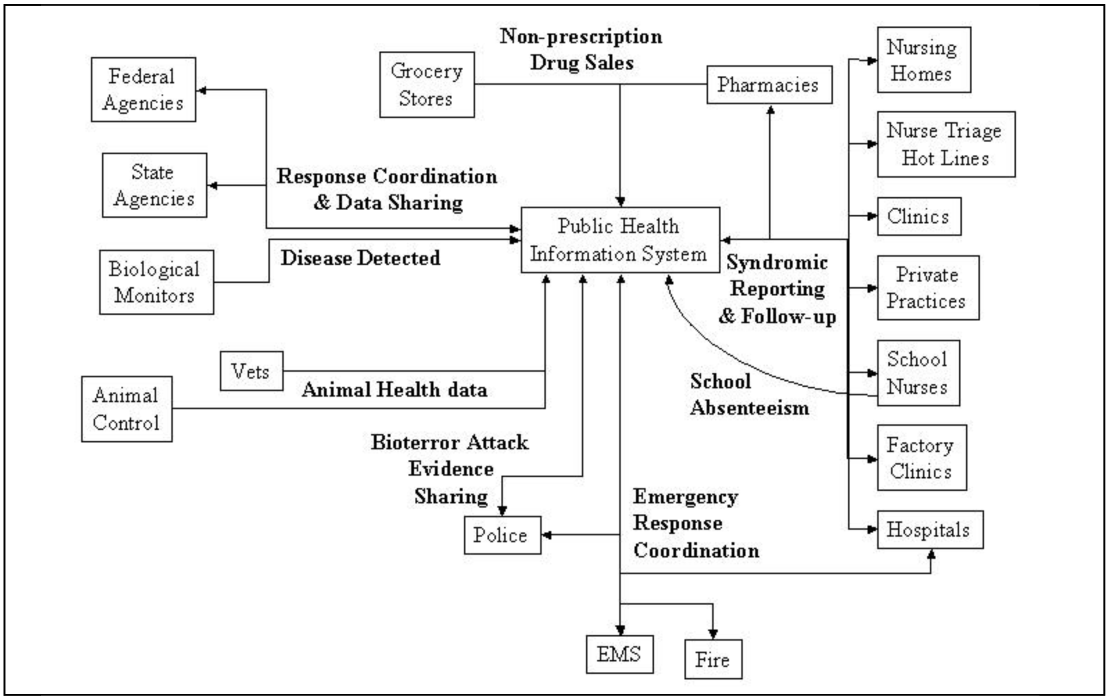


Figure 6. Public Health Information System Architecture

Operation of a Public Health Information System

In the above architecture all hospitals, clinics, private practices, school nurses, factory clinics, nurse triage hot lines, nursing homes, and pharmacies in the county report syndromic surveillance data to the central syndromic surveillance system maintained by the county public health officials as part of its public health information system. Simultaneously, pharmacies and grocery stores report the daily sales for non-prescription drugs, local veterinarians and animal control personnel report the occurrence of sick or dead animals, and school nurses report the number of absent students. The public health information system takes all of this data and determines the normal background rates for each reportable symptom, sales of non-prescription medications, animal illnesses and deaths, and school absenteeism. Biological monitors in areas of high population sample the environment, searching for indications of diseases and report to the health information system. As the system operates long enough, variations for such things as seasons and weather fluctuations will occur and can be included in the model that is emerging. These normal rates are shared with state and federal agencies where they can be integrated into larger scale models.

If a bioterrorism attack occurs there will be a spike in some of the data collected. Depending on the disease used animals might start to die off at a faster rate. Victims will begin to feel ill and will start purchasing more non-prescription medications. School age victims will start missing school. A sudden rise in any of these parameters should alert public health officials that something is going on. Messages can be sent to all clinicians to advise them of the possibility of a bioterrorism event. As victims begin to report to their physicians or emergency rooms, the medical system has already been placed on alert and is better prepared to detect clinical evidence of a bioterror disease and to begin treatment. Once reports of increases in relevant symptoms begin to come into the public health information system, public health officials can analyze the data to determine whether it supports a decision to order the release of prophylactic antibiotics. Obviously, if a biological monitor detects the presence of a disease or law enforcement personnel collect direct evidence of an attack, the level of alert will rise from a suspected attack to a confirmed attack. Once an attack has been confirmed, the information system will alert clinicians and emergency workers throughout the county. It will also pass the alert on to state and federal agencies, as well as to law enforcement officials. Public health officials will use the system to coordinate the actions of the area hospitals, emergency workers and, if they become involved, state and federal assets.

An added benefit of this system is its use in naturally occurring disease outbreaks. While not as sudden and dramatic as that seen in a bioterrorist attack, a natural disease outbreak can still produce a spike in reportable symptoms. Public health officials can use this same system to search for, detect, and react to natural outbreaks such as West Nile Virus, Influenza and, more recently, Severe Acute Respiratory Syndrome (SARS).

Technical Requirements of a Public Health Information System

The main function of a public health information system is to gather, analyze, and disseminate health data, and to support the making decisions based on that analyzed data. As such, the main requirement for such a system is connectivity. The system must be able to collect data from the myriad entities shown in the architecture and to send it where needed. In all cases, the data collection must be as near real-time as possible. The window for effective intervention following a bioterrorism attack is too narrow to allow for the use of daily or weekly aggregated data.

The connections between the various nodes must be capable of operations independent of the public communications systems. This is particularly true of the links between the health information system and those nodes involved with emergency response. The events of 9/11 demonstrated that during emergencies normal communication systems stop working. Cellular phone networks become overwhelmed and fail as the public begins to react to the emergency. Redundant communications must exist between all critical nodes.

The links between all nodes must also be secure. The decisions made with the data collected by the system can affect the lives of thousands of individuals. There must be no doubt that the data received is from proper sources and accurately reflects the current situation.

Required Research

The problems presented in building a public health information system are, at a minimum, how to link and integrate the various existing databases, how to pull out the relevant data and how to decide which data is relevant to each player in any given scenario, how to display the data in a manner most useful to each player, how to transport data to where it is needed with the smallest bandwidth bill possible, and how to do all the above while maintaining data security and not imposing too great an additional burden on busy medical providers and staffs. Research into any of these issues will involve coordination with all of the varied players involved.

Conclusions

The war on terrorism is largely a war of information. This is especially true in the fight against bioterrorism. The modern health-care system is capable of dealing successfully with almost any disease outbreak, but only if it has the time to react. Any delays in the mobilization of the medical response to an attack will result in an increase casualties and deaths. The generally covert nature of a bioterrorist attack is designed to deny the medical community that time. The only successful counter to this covert nature is effective medical surveillance.

References

Carus, W.S., “The Threat of Bioterroism,” National Defense University Strategic Forum, (127), Sept 1997.

Giovachino, M, and Carey, N, “Modeling the Consequences of Bioterorism Response,” Military Medicine (166, 11), Nov 2001, pp. 925-930.

Schnelle, D.D., Unpublished model, Office of the Army Surgeon General, Washington, DC, 2001.

Thompson, L., “Technology and Bioterrorism, Using Information Technology to Detect and Respond to Biological Weapon Attacks,” Proceedings of the 2003 HIMSS Conference, San Diego, CA

Thornton, R., American Indian Holocaust and Survival: A Population History Since 1492, Norman, University of Oklahoma Press, 1987, pp. 78-79.