A Mathematical Model of Bioterrorist Attack Risk Assessment

Radosavljevic Vladan1,2, Belojevic Goran3 and Jovanovic Larisa4*

1Headquarters of The Serbian Medical Corps, Serbia
2Military Academy, Belgrade, Serbia
3Institute of Hygiene and Medical Ecology, School of Medicine, University of Belgrade, Serbia
4University Alfa, Belgrade, Serbia

Abstract

The authors propose a bioterrorism risk assessment model comprising 22 qualitative and 10 quantitative parameters. Scores 0 and 1 refer to low and high probability of a bioterrorist attack, respectively. Vulnerability analysis is related to targets, while feasibility analysis refers to perpetrators, agents and means/media of delivery. The model is applied on the US anthrax attack in 2001. Mathematical modeling is also proposed to express the risk of human losses in a bioterrorist attack. The model may be helpful in predicting and preventing bioterrorist attacks.

Keywords: Bioterrorism; Risk scoring; Epidemiological mathematical modeling

Introduction

A Bioterrorist Attack (BA) may be presented as a 4-component chain model, including perpetrators, agents, means of delivery, and targets [1]. In continuation to this model, here we propose a mathematical method of Bioterrorist Attack Risk Assessment (BTRA), applied on the US anthrax attack in 2001.

We propose three steps of BTRA: Step 1 (vulnerability analysis related to target); Step 2 (feasibility analysis related to other three components of BA: perpetrator, agent and means/mediums of delivery), and Step 3 (general risk assessment analysis, including all four BA components). A total of 32 parameters (22 qualitative and 10 quantitative) are included in the BTRA (Table 1). Qualitative parameters have specific descriptive characteristics, while quantitative parameters have numerical characteristics. None of these parameters itself constitutes a proof of intentional use of a biological agent, but together they can greatly assist in determining if further investigation is warranted. We have developed a simple scoring system for each parameter. Scores 0 and 1 refer to low and high probability of a bioterrorist attack, respectively.

If we try to calculate all possible BA scenarios with 32 parameters and only two possibilities for each of them (0, 1), there would be \(2^{32} \approx 1.000.000.000\) possible BA scenarios. These figures explain the complexity of the problem when trying to predict and prevent a BA [2-8]. Mathematical models may be helpful at least in partly solving this problem.

Methods, Results and Discussion

Vulnerability analysis

Vulnerability analysis should be the first step in biodefense strategy [9-12]. It comprises only target as a component of BA, and eleven corresponding parameters (eight qualitative and three quantitative) (Table 1). For biodefense policy makers the very first step should be the classification of targets. There are “hard” and “soft” targets (parameter importance of targets) and three groups of parameters: qualitative (parameters of control, parameters of protection) and quantitative parameters. We will try to explain this analysis on US anthrax attack in 2001. This attack comprised both types of targets: the Hart Senate building in Washington was a “hard” target and the US Postal Offices were “soft” targets. Probability of both types of targets was high for all types of perpetrators (enemy state, terrorist organizations and individuals), so we scored each of them with 1.

Parameters of control are: intelligence/secrecy (global and local), personal control, control of mediums (air, food and water), and control of services/fomites, for example office equipment, postal letters. Intelligence comprises information provided by using electronic surveillance methods, local intelligence systems and observations of possible targets [13]. These systems were posed only by the state, but functioning was missing or someone employed by government could have passed them, so, we scored with 1 only state as a perpetrator. The impact of secrecy has been evident in the aftermath of the 2001 anthrax letters. Although the US Postal Service and the Center for Disease Control knew that the Brentwood postal facility in Washington, DC was contaminated, they waited for four days before closing the facility and treating workers with antibiotics. By that time, one worker had died of anthrax, another was close to death, and two were gravely ill. Another extreme example is China, where the government denied SARS epidemic for six weeks, causing international alarm and spread of the disease in 2003 [14]. This illustrates that government secrecy presents a persistent jeopardy, leaves the public in ignorance, and allows narrow-minded political agendas to undermine health care goals. For these reasons, we scored with 1 only state as a perpetrator.

Personal control comprises physical control of people (their health status) and behavioral control (CV reviewing, control of suspected behavior, control of contacts). In this case, a microbiologist employed in the US Government was a suspected perpetrator again, so we scored with 1 state as a perpetrator.

Control of water comprises use of bottled water and permanent functioning was missing or someone employed by government could have passed them, so, we scored with 1 only state as a perpetrator. The impact of secrecy has been evident in the aftermath of the 2001 anthrax letters. Although the US Postal Service and the Center for Disease Control knew that the Brentwood postal facility in Washington, DC was contaminated, they waited for four days before closing the facility and treating workers with antibiotics. By that time, one worker had died of anthrax, another was close to death, and two were gravely ill. Another extreme example is China, where the government denied SARS epidemic for six weeks, causing international alarm and spread of the disease in 2003 [14]. This illustrates that government secrecy presents a persistent jeopardy, leaves the public in ignorance, and allows narrow-minded political agendas to undermine health care goals. For these reasons, we scored with 1 only state as a perpetrator.

Control of water comprises use of bottled water and permanent functioning was missing or someone employed by government could have passed them, so, we scored with 1 only state as a perpetrator. The impact of secrecy has been evident in the aftermath of the 2001 anthrax letters. Although the US Postal Service and the Center for Disease Control knew that the Brentwood postal facility in Washington, DC was contaminated, they waited for four days before closing the facility and treating workers with antibiotics. By that time, one worker had died of anthrax, another was close to death, and two were gravely ill. Another extreme example is China, where the government denied SARS epidemic for six weeks, causing international alarm and spread of the disease in 2003 [14]. This illustrates that government secrecy presents a persistent jeopardy, leaves the public in ignorance, and allows narrow-minded political agendas to undermine health care goals. For these reasons, we scored with 1 only state as a perpetrator.

Methods, Results and Discussion

Vulnerability analysis

Vulnerability analysis should be the first step in biodefense strategy [9-12]. It comprises only target as a component of BA, and eleven corresponding parameters (eight qualitative and three quantitative) (Table 1). For biodefense policy makers the very first step should be the classification of targets. There are “hard” and “soft” targets (parameter importance of targets) and three groups of parameters: qualitative (parameters of control, parameters of protection) and quantitative parameters. We will try to explain this analysis on US anthrax attack in 2001. This attack comprised both types of targets: the Hart Senate building in Washington was a “hard” target and the US Postal Offices were “soft” targets. Probability of both types of targets was high for all types of perpetrators (enemy state, terrorist organizations and individuals), so we scored each of them with 1.

Parameters of control are: intelligence/secrecy (global and local), personal control, control of mediums (air, food and water), and control of services/fomites, for example office equipment, postal letters. Intelligence comprises information provided by using electronic surveillance methods, local intelligence systems and observations of possible targets [13]. These systems were posed only by the state, but functioning was missing or someone employed by government could have passed them, so, we scored with 1 only state as a perpetrator. The impact of secrecy has been evident in the aftermath of the 2001 anthrax letters. Although the US Postal Service and the Center for Disease Control knew that the Brentwood postal facility in Washington, DC was contaminated, they waited for four days before closing the facility and treating workers with antibiotics. By that time, one worker had died of anthrax, another was close to death, and two were gravely ill. Another extreme example is China, where the government denied SARS epidemic for six weeks, causing international alarm and spread of the disease in 2003 [14]. This illustrates that government secrecy presents a persistent jeopardy, leaves the public in ignorance, and allows narrow-minded political agendas to undermine health care goals. For these reasons, we scored with 1 only state as a perpetrator.

Vulnerability analysis should be the first step in biodefense strategy [9-12]. It comprises only target as a component of BA, and eleven corresponding parameters (eight qualitative and three quantitative) (Table 1). For biodefense policy makers the very first step should be the classification of targets. There are “hard” and “soft” targets (parameter importance of targets) and three groups of parameters: qualitative (parameters of control, parameters of protection) and quantitative parameters. We will try to explain this analysis on US anthrax attack in 2001. This attack comprised both types of targets: the Hart Senate building in Washington was a “hard” target and the US Postal Offices were “soft” targets. Probability of both types of targets was high for all types of perpetrators (enemy state, terrorist organizations and individuals), so we scored each of them with 1.

Parameters of control are: intelligence/secrecy (global and local), personal control, control of mediums (air, food and water), and control of services/fomites, for example office equipment, postal letters. Intelligence comprises information provided by using electronic surveillance methods, local intelligence systems and observations of possible targets [13]. These systems were posed only by the state, but functioning was missing or someone employed by government could have passed them, so, we scored with 1 only state as a perpetrator. The impact of secrecy has been evident in the aftermath of the 2001 anthrax letters. Although the US Postal Service and the Center for Disease Control knew that the Brentwood postal facility in Washington, DC was contaminated, they waited for four days before closing the facility and treating workers with antibiotics. By that time, one worker had died of anthrax, another was close to death, and two were gravely ill. Another extreme example is China, where the government denied SARS epidemic for six weeks, causing international alarm and spread of the disease in 2003 [14]. This illustrates that government secrecy presents a persistent jeopardy, leaves the public in ignorance, and allows narrow-minded political agendas to undermine health care goals. For these reasons, we scored with 1 only state as a perpetrator.

Personal control comprises physical control of people (their health status) and behavioral control (CV reviewing, control of suspected behavior, control of contacts). In this case, a microbiologist employed in the US Government was a suspected perpetrator again, so we scored with 1 state as a perpetrator.

Control of water comprises use of bottled water and permanent functioning was missing or someone employed by government could have passed them, so, we scored with 1 only state as a perpetrator. The impact of secrecy has been evident in the aftermath of the 2001 anthrax letters. Although the US Postal Service and the Center for Disease Control knew that the Brentwood postal facility in Washington, DC was contaminated, they waited for four days before closing the facility and treating workers with antibiotics. By that time, one worker had died of anthrax, another was close to death, and two were gravely ill. Another extreme example is China, where the government denied SARS epidemic for six weeks, causing international alarm and spread of the disease in 2003 [14]. This illustrates that government secrecy presents a persistent jeopardy, leaves the public in ignorance, and allows narrow-minded political agendas to undermine health care goals. For these reasons, we scored with 1 only state as a perpetrator.

Control of water comprises use of bottled water and permanent functioning was missing or someone employed by government could have passed them, so, we scored with 1 only state as a perpetrator. The impact of secrecy has been evident in the aftermath of the 2001 anthrax letters. Although the US Postal Service and the Center for Disease Control knew that the Brentwood postal facility in Washington, DC was contaminated, they waited for four days before closing the facility and treating workers with antibiotics. By that time, one worker had died of anthrax, another was close to death, and two were gravely ill. Another extreme example is China, where the government denied SARS epidemic for six weeks, causing international alarm and spread of the disease in 2003 [14]. This illustrates that government secrecy presents a persistent jeopardy, leaves the public in ignorance, and allows narrow-minded political agendas to undermine health care goals. For these reasons, we scored with 1 only state as a perpetrator.
Quantitative parameters comprise the number and distribution of people at a target and location of a target. Since overcrowded targets are at highest risk, people must be advised to avoid them (e.g. some manifestations). Potential targets should be safely organized, well protected, located out of a dense urban area, and with easily accessed roads. For each perpetrator they had the same importance, and did exist at the time of attack and therefore scored with 1.

Parameters of protection can be physical, chemical or immunological. One form of physical protection of people is the advice to remain indoors in response to biological attack alarm. This will simply prevent transmission of biological agents. Another example is the use of air conditioning systems, or system of increasing air pressure in different parts of buildings [16]. Furthermore, UV radiation sources may be used as physical protection. Chemical protection refers to use of antibiotics, which is a great logistic challenge, since it provides protection only against classic agents (e.g. anthrax or plague), for as long as the available stocks last. Mass immunization program requires careful consideration to assess potential risks and benefits. Nation wide smallpox vaccination campaign, carried out in November 2002 in the USA, was based on the idea of smallpox-infected Iraqis invading America. It resulted in 145 serious adverse events among civilians (hospitalization, permanent disability, life-threatening illness, and at least three death cases [17]. Above mentioned measures of protection were not applied, they did not exist at the time of attack and therefore scored with 0.

## Table 1: A model of bioterrorism risk scoring.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>State or state supported</th>
<th>Disaffected/terrorist groups</th>
<th>Individuals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Importance of target</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Intelligence</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Secrecy</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Personal control</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Control of means/mediums</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Physical protection</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Chemical protection</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Immunological protection</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Number of people in target</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Distribution of people in target</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Location of target</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Perpetrator</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sophistication</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Motivation</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Ability</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Capacity</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Intelligence</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Secrecy</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Number of perpetrators</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Accessibility to sources of agent</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Accessibility to targets</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Agent</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A category</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>B category</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>C category</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Emerging agent</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Amount of the available agent</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Means/media of delivery</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Air</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Food</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Water</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fomites</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Munition</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Delivery systems</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Dispersion systems</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>21</td>
<td>9</td>
<td>9</td>
</tr>
</tbody>
</table>

* 1 = High probability of a bioterrorist attack (BA)
0 = Low probability of a BA

Total Scores:
1-8 - BA is lowly probable
9-16 - BA is possible
17-24 - BA is highly probable
25-32 - BA is imminent

condition systems should also be developed and applied (biosensors). These measures of control were insufficient by State and scored with 1.
This was an example of a retrograde _vulnerability analysis_. But, if we know some parameters of any target we can calculate anticipating _vulnerability analysis_ (risk of a successful attack, possible losses, priorities in bio-defense, costs, improvement of resource management).

**Feasibility analysis**

_Feasibility analysis_ may have dual use (anticipating and retrograde analysis). Anticipating analysis could be used for risk assessment, e.g. as guidelines for biosecurity and biodefense measures [18-20]. It comprises three components (perpetrator, agents and means/mediums of delivery) and corresponding parameters for a BA. Total number of parameters is 21 (14 qualitative and 7 quantitative). Retrograde analysis could be used for finding out a perpetrator and reconstruction of a BA [21].

Three types of perpetrators may exist: government organized and supported perpetrators (institutions and organizations), terrorist organizations and individuals. Other qualitative parameters are _sophistication_ and _motivation_. Highly sophisticated perpetrators use highly dangerous agents (category A agents or emerging agents) [22], attack without suicidal tendencies, keep themselves unknown, and try to attack "hard" targets. Such perpetrator(s) carried out the USA anthrax attack in 2001. Al-Qaeda was the main suspect the very first day of the attack. But, so high sophistication, ability, capacity, intelligence, secrecy and repeated attacks might have not be expected from Al-Qaeda. _Intelligence_ presents _ability_ to get a true and on- time information on global and local level related to biological attack. _Secrecy_ comprises _capacity_ to keep activities unobserved before an attack, and to keep perpetrators unknown after the attack. Because of that we scored only _State_ with 1. One highly motivated perpetrator was sufficient for all types of perpetrators, so we scored the _Number_ parameter with 1 for all of them. _Distribution_ affects the _accessibility_ of bioterrorist to sources of infectious agents and to their targets. _Accessibility_ of bioterrorists to sources of agent was possible only at the top-secret military labs in Fort Dietrick, so, one point for _State_. _Accessibility_ of bioterrorist to the targets was possible for everyone through USPS, so we scored all types of perpetrators with 1.

_Bacillus anthracis_ strain used in US attack 2001 was highly specific and stolen from top-secret military labs. Then, only State should be pointed with 1. Also, a repeated attack with this highly selected and sophisticated strain available during longer period of time request solid amount of it. Because of that, we scored only the State with 1. B, C, and emerging agents were not used and were pointed by 0.

Fomites (postal letters) and delivery system (USPS) were used, and could be used by all types of perpetrators, so we scored all of them with 1. Other means/mediums of delivery were not used, and were scored with 0.

This was an example of a retrograde _feasibility analysis_. But, if we know some parameters of these three components we can make an anticipating _feasibility analysis_ (risk of successful attack, possible losses, priorities in bio-defense, costs, improvement of resource management).

**General BA risk assessment**

_General BA risk assessment_ may helps in finding out perpetrator, as well as in estimating potential losses due to BA.

_Finding out perpetrator_. Total number of parameters in Table 1 is 32 (22 qualitative and 10 quantitative). In the US anthrax attack in 2001, (Enemy) _State_ had 66% of the maximum possible number of points, while _terrorist organization_ and _individuals_ each had 28%, respectively. This difference clearly indicates that someone close to _State_ stayed behind the BA. The risk of BA decreases with increase of the number of known parameters, and the probability of discovering the perpetrator increases with increase of the number of known parameters.

_Estimating potential losses_ and _costs_ is crucial for public health preparedness for a BA. US anthrax attack in 2001, recognized both types of targets: the Hart Senate building in Washington was "hard" and the US Postal Offices were "soft" targets. Losses are known (direct: five dead, 22 ill and 32.000 under antibiotics therapy; indirect: the estimated cost of decontaminating parts of the Hart Senate building in Washington, DC was $23 million ("hard" economic target). The economic impact of a biological attack involving potential exposure to anthrax was estimated at $26.2 billion/100000 persons exposed ("soft" economic target). The cost and resources needed to decontaminate the environment should be added to this [23], as well as losses due to psychological effects [24].

Risk is usually defined as the product of the damage (loss) and probability of its occurrence:

\[
R = p \cdot L
\]

\(p\) – probability

\(L\) – damage (loss)

In the case when the damage (loss) occurs as a result of different causes, the risk is presented as the sum of partial risks:

\[
R = \sum_i p_i L_i
\]  

(4.1)

Passing to the limit (when the size of the damage / loss depends on a continuous parameter \(\tau\)) one obtains the following formula:

\[
R = \int_{\tau_0}^{\tau} p(\tau) L(\tau) d\tau
\]  

(4.2)

Using more detailed mathematical modeling, the risk of human losses due to biological attack can be expressed as follows:

\[
R = E(N) = \int \int_{\tau_0}^{\tau} p(\tau) \psi(x, y) f(x, y, \tau) d\tau dx dy
\]  

(4.3)

Here:

\(R\) – risk = mathematical expectation of the human losses (\(E(N)\))

\(P\) – probability of biological attack (accident etc.)

![Figure 1: Expected risk vs. probability of BA - efficacy of protection depends on the knowledge of the characteristics/parameters.](image-url)
$S$ – area of integration (e.g. territory of the city, district, state,...)

$\tau$ – a parameter characterizing the harmful effects (concentration, intensity of the agent)

$\tau_0, \tau_1$ – minimum and maximum values of the parameter $\tau$

$p(\tau)$ – the probability of illness/death, depending on the intensity of $\tau$

$\psi(x,y)$ – density of population in the observed area

$f(x,y,\tau)$ – density distribution of the parameter $\tau$ at the point $(x,y)$ from $S$

If one takes into account the time factor $t$ (for example, due to changes in the concentration of agent $\tau$, or taking into account the incubation time), the formula gets the form:

$$R = E(N) = E\left[\int \int \left( \int \int p(\tau, t) \psi(x,y,t) f(x,y,\tau) d\tau \right) dx dy dt \right]$$

(4.4)

It should be noted that the effective determination of probability is complex and difficult task. It may be estimated on the basis of available statistical data. If the measures of protection/security are taken, the risk reduction is expected. More efficient protection leads to greater risk reduction. Efficacy of protection depends on the knowledge of the characteristics/parameters of the problem: if the larger number of parameters $N$ is known - protection is more efficient (Figure 1).

Curve $\Gamma_N$ corresponds to the case when $N$ parameters are known. We identified $\Gamma_N$ with a hyperbola $y = \frac{d_0}{x}$ where $a_0 > a_1 > a_2 > ...$

The simplest and the cheapest preventive measure in BTRA is vulnerability analysis of the target. It is an independent feasible and useful analysis. Each country could denote its own potential targets as “hard” and “soft” and perform vulnerability analysis.

Conclusion

This paper presents a mathematical model of BTRA that includes vulnerability analysis of targets and feasibility analysis of perpetrators, agents and means/media of delivery. It is also used to express the risk of human losses in a bioterrorist attack. The model may helpful in predicting and preventing BAs.

Acknowledgment

This study has been financially supported by the Serbian Ministry of Education and Science, through projects No. 175078, III47009 and III43009. The authors state that they have no conflict of interest in this study.

References