

Toward the Design of a Robust Bioterrorism Information System to Enhance National Security

Leila Shokrizadeh Arani ✉

Ph.D. in Health Information Management, Health Information Management Research Center (HIMRC), Department of Health Information Management, School of allied medical sciences, Kashan University of Medical Sciences, Kashan, Iran.

Email: arani_leila@yahoo.com , ORCID: <http://orcid.org/0000-0002-5586-0580>

Citation: Shokrizadeh Arani L. **Toward the Design of a Robust Bioterrorism Information System to Enhance National Security.** Applied Health Information Technology 2021; 2(1): 51-57.

Received: 01-05-2021

Accepted: 04-03-2021

DOI: 10.18502/ahit.v2i1.6162

Abstract

In an objective sense, security measures the absence of threats to acquired values, whereas, in a subjective sense, it refers to the absence of fear that such values will be attacked. Bioterrorism is a threat. Therefore, any threat to the country's vital goals and security components, such as population, land, and property, is a national security threat.

Establishing a robust information system is critical for detecting Bioterrorism outbreak, which is considered a threat to national security. Real-time surveillance and monitoring, fast communication, data collection, and analysis at the regional and national level are the main functions of this information system.

Early detection of bioterrorism is an important step in national security promotion. If the BIS is appropriately designed based on critical factors such as multidimensional, real-time, manage by the security agency, and have the capability for pattern recognition and detection, it will more effectively manage bioterrorism attacks by relying on its capabilities, features, and technologies. Therefore, this study investigates the features and capabilities of the Bioterrorism Information System (BIS) in national security improvement and promotion.

Keywords: Information systems; Bioterrorism; Bio-surveillance; Security; Disease outbreaks

Security is very important for social development and health planning, the absence of security is the most important obstacle and barrier on the way to moving the country towards its predetermined goals (1,2).

Security has emerged as an important strategic priority and is one of the main goals for the government of any country (3, 4). The national security term was used for the first time in 1945, at the end of World War II (5). According to the definition of national security by the United Nations and the Encyclopedia of Social Sciences, national security is states and conditions in which there is the threat of losing all or part of its population, property, or territory (1, 6).

Copyright: ©2021 The Author(s); Published by Shahid Sadoughi University of Medical Sciences. This is an open-access article distributed under the terms of the Creative Commons Attribution License (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

One of the components of national security is the protection of the people's lives of the country (1). Anything that affects human resources is a security threat (7). Government, population, and land are three components of national security.

Therefore, the threat is against the concept of national security and challenges security (7). Security means no threat, and terrorism is a threat to the population. So terrorism is a threat to national security (6). One of the most important types of terrorism is bioterrorism which involves the illegal and deliberate use of biological agents, chemical agents, or poisonous substances causing illness and mortality in plants, animals, and humans. The purpose of such materials is to cause great damage and using even a small amount of them is very dangerous (6, 8, 9).

Bioterrorism features

Bioterrorism has some features and factors making it a major threat to national security.

That is why terrorists tend to use it more than other weapons of mass destruction (WMD). Biological weapons often are defined as 'cheap weapons of mass destruction, because this is relatively cheap and easy to produce, hide and relocate (8, 10).

In comparison to nuclear weapons, biological agents have no destructive effects (6). Moreover, the bioterrorism agents are more powerful, more conventional, simpler to produce, less costly, less sophisticated but more lethal. There is also a variety of agents for the dissemination of biological substances (6, 8). Intrinsic features of biological agents which influence their potential for use as weapons include infectivity; virulence; toxicity; pathogenicity; incubation period; transmissibility; lethality; and stability. Unique to many of these agents, and distinctive from their chemical counterparts, is the ability to multiply in the body over time and increase their effectiveness. Features of biological agents that influence their effectiveness are presented in Table 1 (6, 8, 9).

Table 1: Features of Effective Biological Agents

Feature	Description
Infectivity	The ability of a pathogen to establish an infection.
Virulence	The ability of a microorganism (pathogen's or microbe's ability) to cause disease in the host.
Toxicity	The toxicity of an agent reflects the relative severity of illness or incapacitation produced by a toxin.
Pathogenicity	Reflects the capability of an infectious agent and the potential ability to produce disease in a susceptible host.
Additional factors	The suitability of a microorganism or toxin as a biological weapon includes easiness of proliferation and production; stability when stored or transported; and ease of dissemination; easiness of proliferation; invisibility during an attack and low traceability in the initial phase of an attack.
Incubation period	The time from the moment of exposure to an infectious agent until signs and symptoms of the disease appear.
Transmissibility	Some biological agents can be transmitted from person-to-person directly.
Lethality	Reflects the relative ease with which an agent causes death in a susceptible population.
Stability	The degree of influence of an agent by various environmental factors, including temperature, relative humidity, atmospheric pollution, and sunlight.

Panic and fear related to the spread of a disease caused by bioterrorism in society are much intense than the explosion caused by other war weapons (11, 12). On the other hand, the development of genetic changes in biological warfare agents and specific characteristics of biological materials, in addition to other factors, has made it more difficult to identify and recognize these factors, and to treat the diseases caused by them (6, 8, 13).

Bioterrorism Information System (BIS) involves early detection of disease due to bioterrorist activity. The attributes of the bioterrorism agents can affect their detection. So the design of BIS depends on the properties of the bioterrorism agents

BIS properties and national security

The October 2001 anthrax attacks and the outbreak of the virulent Severe Acute Respiratory Syndrome (SARS) 2004, and increased awareness that terrorist groups may be capable of releasing life-threatening

biological agents have stimulated and prompted efforts to improve the nation's preparedness and response for bioterrorism.

Bioterrorism is a real and significant threat of the 21st century (8, 14, 15) which affects stability, national security, and economic development. Bioterrorism is a reemerging and asymmetric health problem and is now considered as an emergency state of national security for many countries. The solution for this problem is to provide BIS (6, 8, 9).

BIS is based on the collection and accurate statistical analysis of data about bioterrorism attacks. This system is the monitoring of a wide range of pre-diagnostic and diagnostic data to enhance the ability of the public health infrastructure to detect, investigate, and respond to bioterrorism disease outbreaks. The basis of this system is information obtained from patients or suspected cases (6, 8, 9). As shown in Figure 1, the BIS connects national security and public health threats.

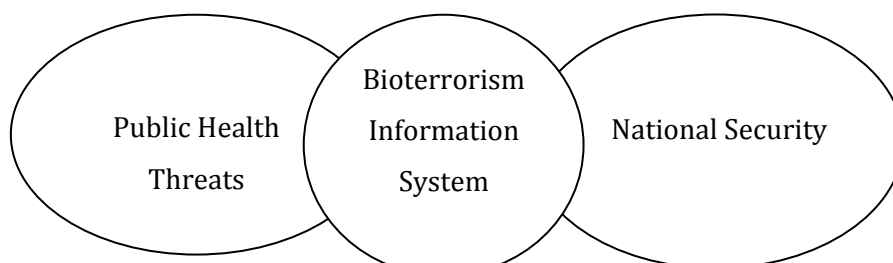


Figure 1: The connections among BIS, national security, and public health threats.

BIS helps to identify bioterrorism outbreaks using signs, symptoms, laboratory findings, and other non-clinical information from various sources before confirming a final diagnosis. It is also designed to monitor bioterrorism events and to reduce mortality as well as illness. On the other hand, this system is possible to improve the method of response and communication to obtain the clinical details of diseases caused by Bioterrorism (6, 8, 9, 16).

BIS can:

- Facilitate the accurate and rapid recognition of Bioterrorism-related diseases
- Improve the speed of analysis and data transmission
- Provide detailed information for evaluating Bioterrorism attacks
- Assist in determining exposure sites through GIS (Geographic Information Systems)
- Facilitate the integration of Bioterrorism information through the country

- Help to accomplish effective services, such as the process of vaccination and antibiotic therapy
- Help to treat early-onset illnesses leading to death quickly
- Provide historical data to be used as a base for statistical comparisons and long-term monitoring of health (6, 8, 9). Therefore, a bioterrorism information system is necessary for health threats. Besides, the strength of this system in responding to threats depends on the characteristics of the system.

Method

For this review study, 25 articles including the keywords of sentinel surveillance, bioterrorism detection, disease outbreaks, bio-surveillance, bioterrorism, national security, and information systems were originally derived from the ProQuest, PubMed, Web of Science, Scopus, and Google Scholar databases. In the reviewed articles, the existence of bio-terrorism information system features has been considered. Publications throughout 2005–2020 in English and Persian languages were selected for this work.

The steps involved to identify relevant e-resources for the review were searching, screening, eligibility, and inclusion. Searching was conducted using the key terms listed above. Next, the documentations were thoroughly screened to eliminate non-relevant records by reading the titles, abstracts, and finally, the full texts, based on the set inclusion/exclusion criteria. This work was done by two researchers separately.

After the screening activity was completed, the selected articles were checked for

completeness and retained for the review work. Eventually, 30 articles were found eligible for the present review. By analyzing the retrieved articles, the features of the BIS were extracted and its relationship with national security was discussed.

Results

A bioterrorism attack is a public health emergency. Completion of the following five phases of activities before an incident is essential for a successful response to a bioterrorist attack:

1. Preparedness Phase
2. Early Warning Phase
3. Notification Phase
4. Response Phase
5. Recovery Phase

Early detection is the key to contain such attacks. The role of the BIS is critical in the early warning phase. Overall, the characteristics of the BIS can be divided into five general categories according to the methodological steps and main functions of the system, i.e., features of the BIS in the data collection, processing, and distribution phase. Furthermore, features of the BIS are related to legal and security requirements (6, 8, 9).

Developing and maintaining an effective BIS is the first essential step in preparedness and response to bioterrorism attacks. Also, it is important in helping promote and upgrade national security.

The designer for BIS must examine how quickly bioterrorism outbreaks need to be detected and characterized. It must be able to design a system that can meet these requirements by real-time collecting data.

Table 2: Capabilities of BIS Based on Main Phase and Technology Groups

Main phase	Main architectural features	Capabilities	IT Categories					System	References
			Detection	Surveillance	Diagnosis and clinical management	Communication	Supporting technology		
Early Warning Phase	Data collection	Diverse data resources	*				*	BASIS, Portal Shield, RSVP, ESSENSE, B-Safer	(6, 9)
		Environmental surveillance	*				*	BiowatchEpiSPIRE	(17)
		Laboratory and antimicrobial resistance surveillance	*		*		*	RODS	(6, 9)
		Event-based surveillance	*				*	Drop-in surveillance 1	(18)
	Processing	Coding models and vocabulary standard	*	*			*	RODS	(6, 9)
		Robust, automatic, and timely processing and statistical analysis system	*			*		BioPortal	(19, 20)
		Problem-solving methodology and anthology	*				*	BioStorm	(6, 9, 19, 21)
	Distribution	Communication networks to facilitate data sharing	*	*	*			RODS	(6, 9)
		Information sharing and distribution technologies	*	*	*			BioWatch	(22)
	Security requirements	Security requirements and strong infrastructure	*	*	*			NBSSDP2, RODS	(17-19, 23-25)
	Legal requirement	Legal requirements and system ownership	*	*	*			NBSSDP2, RODS	(6, 9, 26)

1. Drop-in Bioterrorism surveillance system for World Series 2002in Phoenix, Arizona

2. National Bioterrorism Syndromic Surveillance Demonstration Program

The BIS must have the following features to maintain and enhance national security:

- Various data sources should be used in designing the National Bioterrorism Information System. Equipping the system with biosensors and biological detectors as well as using information related to the threats of bioterrorism attacks must be obtained from security and intelligence organizations. Besides, the use of clinical and non-clinical data and technologies in designing will increase the accuracy and reduce the redundancy of data and finally enhance the performance of this system.
- Localization in the classification of biological agents based on the demographic and epidemiological features of a country should be considered.
- Advanced and flexible statistical methods ought to be used in the data processing phase.
- Geographic features of the region, epidemic diseases, demographic characteristics, classification system selection, determination of syndrome groups, and attention to the season and time of the event are significant points recommended to be applied to determine the threshold in the data processing phase.
- Using the alert system in the design of BIS-based security policies of each country.
- International and national infrastructure security guidelines must be used during the development and implementation phase in designing BIS.
- Ensuring adequate epidemiologic and laboratory capacity nationwide are prerequisites to effective bioterrorism information systems.
- Communication and coordination links also need to be strengthened to minimize response time, especially when exposed for the first time. Also, when response time is shortened, the possibility of apprehending perpetrators increases.

- Many agencies and organizations must work collaboratively to ensure national preparedness against bioterrorist attacks. Intelligence ministry and the health ministry are well-positioned to provide leadership in several areas.

Enhancing the public health infrastructure will improve Iran's ability to respond to any infectious disease outbreak and provide added value in the event of bioterrorist events. In this manner, national security can be promoted. BIS could further strengthen national institute abilities to respond to public health emergencies.

The Nation's capacity to respond to bioterrorism depends in part on the ability of public health officials to manage bioterrorism events. BIS has the potential to aid public health officials to respond and react effectively to a bioterrorist attack.

Conclusion

This paper discusses several features and properties in the development of an effective bioterrorism information system. Four critical factors for national security are that BIS must be multidimensional, managed by a security agency, provide real-time good and sufficient warning, and have the capability for pattern recognition and detection that will quickly identify an alarm the threshold value.

Disclaimer Statements

Conflict of Interests: None

Financial Support or sponsorship: This study is part of the Ph.D. thesis was approved by the Shahid Beheshti University of Medical Sciences.

Protection of Human and Animal Subjects: Not Applicable.

Authors' contributions: None

References

1. MovahediNia J. Principles of passive defense. 1th ed. Tehran: Malek Ashtar University Press; 2008 Winter:10-15.

2. Azghandi A, Kafi M. Study on national security of the Islamic Republic of Iran from the perspective of constructivism theory. *Political Science Quarterly*. Winter 2013; 8(21):205-31. [In Persian]
3. Minaei H, Zohdi Y. Examining the impact of social cohesion and demographic change on I.R. Iran's national security. *Defense Strategy*. Fall 2013; 10(39):73-112. [In Persian]
4. Alizadeh A, PishgahiFar Z. Environmental security and the evolution of the concept of security in the 21st century. *Journal of Geographical perspective of human studies*. 2011; 14(6):107-19.
5. Tahaei S. Review the national security doctrine Foreign Relations Spring 2013;10(39):73-112. [In Persian]
6. ShokrizadehArani L. Providing Architecture Model of National Bioterrorism Information System with Database Approach for Iran. Thesis: Tehran: Shahid Beheshti University of Medical Science.2018:25-100.
7. Jajarami K, Pishgahifard Z, Mahkuei H. Assessment of environmental and Biological threats on the national security in Iran. *Strategy Quarterly*. Summer 2013; 22 (67):193-230. [In Persian]
8. Moghaddasi H, ShokrizadehArani L, Zarghi A. Features of Bioterrorism Information System. *J Bioterror Biodef*. 2018; 9(162): 2:1-6.
9. ShokrizadehArani L, Moghaddasi H, Zarghi A, Rahimi F. Bioterrorism Information System as the Most Effective Tool in Management of Bioterrorism. *history*. 2019;16(4):1-8.
10. Michailiuk B. Threat of biological weapons. *Securitologia*. 2016; 1(23): 59-75.
11. Krishan K, Kaur B, Sharma A. India's preparedness against bioterrorism: biodefence strategies and policy measures. *Current Science*. 2017; 113(9):1675-1682.
12. Graham B, Talent J. Bioterrorism: redefining prevention. Mary Ann Liebert, Inc. 140 Huguenot Street, 3rd Floor New Rochelle, NY 10801 USA; 2009. 125-126.
13. Balali-Mood M, Moshiri M, Etemad L. Medical aspects of bio-terrorism. *Toxicon*. 2013; 69:131-142.
14. Kshirsagar M, Dodamani A, Vishwakarma P, Dodamani G, Jadhav H, Bhandari R. Assessment of knowledge and attitude of dentists toward bioterrorism awareness in dhule (maharashtra, india): A cross-sectional survey. *Journal of Indian Association of Public Health Dentistry*. 2017;15(1):57-60.
15. Allen L. Biosecurity and non-communicable diseases. *Journal of Bioterrorism & Biodefense*. 2016;7(2):1-4.
16. Shmueli G, Burkom H. Statistical challenges facing early outbreak detection in biosurveillance. *Technometrics*. 2010;52(1):39-51.
17. Kman NE, Bachmann DJ. Biosurveillance: a review and update. *Advances in preventive medicine*. 2012; Volume 2012, Article ID 301408: 1-10.
18. Mandl KD, Overhage JM, Wagner MM, Lober WB, Sebastiani P, Mostashari F, et al. Implementing syndromic surveillance: a practical guide informed by the early experience. *Journal of the American Medical Informatics Association*. 2004;11(2):141-50.
19. Yan P, Chen H, Zeng D. Syndromic surveillance systems. *Annual review of information science and technology*. 2008;42(1):425-95.
20. Tseng C, Lynch C, Gotham I, Eidson M, Chang W, Chen H, et al., editors. *BioPortal: A case study in infectious disease informatics*. Proceedings of the 5th ACM/IEEE-CS Joint Conference on Digital Libraries (JCDL'05); 2005: IEEE.
21. Crubézy M, O'Connor M, Pincus Z, Musen MA, Buckeridge DL. Ontology-centered syndromic surveillance for bioterrorism. *IEEE Intelligent Systems*. 2005;20(5):26-35.
22. Cheng CK, Ip DK, Cowling BJ, Ho LM, Leung GM, Lau EH. Digital dashboard design using multiple data streams for disease surveillance with influenza surveillance as an example. *Journal of medical Internet research*. 2011;13 (4):e85.
23. Espino JU, Wagner M, Szczepaniak C, Tsui F, Su H, Olszewski R, et al. Removing a barrier to computer-based outbreak and disease surveillance—the RODS open source project. *Morbidity and Mortality Weekly Report*. 2004 Sep 24;53:32-9.
24. Yih WK, Caldwell B, Harmon R, Kleinman K, Lazarus R, Nelson A, et al. National bioterrorism syndromic surveillance demonstration program. *Morbidity and Mortality Weekly Report*. 2004:43-6.
25. Platt R, Bocchino MC, Caldwell B, Harmon R, Kleinman K, Lazarus R, et al. Syndromic surveillance using minimum transfer of identifiable data: the example of the National Bioterrorism Syndromic Surveillance Demonstration Program. *Journal of Urban Health*. 2003;80(1):i25-i31.
26. Yan W, Palm L, Lu X, Nie S, Xu B, Zhao Q, et al. ISS-an electronic syndromic surveillance system for infectious disease in rural China. *PloS one*. 2013; 8(4): e62749.