Review Article

BIOMEDICAL Journal of Scientific & Technical Research

ISSN: 2574 -1241

DOI: 10.26717/BJSTR.2019.16.002887

Bioterrorism Information System as the Most Effective Tool in Management of Bioterrorism

Leila Shokrizadeh Arani[1], Hamid Moghaddasi*[2], Afshin Zarghi[3] and Forough Rahimi[4]

[1]*Faculty of Paramedical Sciences, Kashan University of Medical Sciences, Kashan, Iran*

[2]*Associate Professor of Health Information Management & Medical Informatics, Department of Health Information Technology and Management, School of Allied Medical Sciences, Shahid Beheshti University of Medical Sciences, Tehran, Iran*

[3]*Professor, Department of Pharmaceutical Chemistry, School of Pharmacy, Shahid Beheshti University of Medical Sciences, Tehran, Iran*

[4]*Assistant Professor, Faculty of Paramedical Sciences, Shahid Beheshti University of Medical Sciences, Tehran, Iran*

***Corresponding author:** Hamid Moghaddasi, Associate Professor of Health Information Management & Medical Informatics, Department of Health Information Technology and Management, School of Allied Medical Sciences, Shahid Beheshti University of Medical Sciences, Tehran, Iran

ARTICLE INFO

Received: March 23, 2019

Published: April 01, 2019

Citation: Leila Shokrizadeh Arani, Hamid Moghaddasi, Afshin Zarghi, Forough Rahimi. Bioterrorism Information System as the Most Effective Tool in Management of Bioterrorism. Biomed J Sci & Tech Res 16(4)-2019. BJSTR. MS.ID.002887.

Abbreviations: BIS: Bioterrorism Information System; CDC: Centers for Disease Control; HANAA: Handheld Advanced Nucleic Acid Analyzer; FACTS: FSIS Automated Corporate Technology Suite; BDI: Biological Defense Initiative; LRN: Laboratory Response Network; BL: Biosafety Levels; NLP: Natural Language Processing; DARPA: Defense Advanced Research Projects Agency; NLRN: National Laboratory Response Network; HAN: Health Alert Network; PHIN: Public Health Information Network; NEPHTN: National Environmental Public Health Tracking Network

ABSTRACT

Introduction and Aim: Bioterrorism Information System is for real-time and reliable reporting in order to identify bioterrorism attacks. This system is considered as the most important tool in the management of bioterrorism. A major step in management of these attacks is early identification and subsequent timely response to bioterrorism attacks. The effects of such a system depend on its features and capabilities. This study aims to investigate the features and capabilities of Bioterrorism Information System in effective management of bioterrorism attacks.

Method: To accomplish this review study, 98 articles including the key words of Sentinel Surveillance, Disease Outbreaks, Biosurveillance Bioterrorism and Information Systems were originally derived from the ProQuest, PubMed, Web of Science, Scopus and Google Scholar databases. 98 articles dated 1980-2017 were found of which 58 were analytically identified as the main ones according to the content.

Results: Based on this study, the features and capabilities of Bioterrorism Information Systems were in the top 10 categories. Diverse data resources relying on superior technologies, Environmental surveillance, Laboratory and antimicrobial resistance surveillance, Event-based surveillance, Coding models and vocabulary standard, Robust, automatic, and timely processing and statistical analysis system, Communication networks ,Problem solving methodology and anthology, Information sharing and distribution technologies, Legal and security requirements were found as features and capabilities of the bioterrorism information system in its effective management process.

Conclusion: Early detection of bioterrorism is an important step in managing bioterrorism events. If the Bioterrorism Information System is properly designed, it will more effectively manage bioterrorism attacks by relying on its capabilities and technologies.

Keywords: Information Systems; Bioterrorism; Biosurveillance; Management; Disease Outbreaks

Introduction

One of the most important types of terrorism is bioterrorism which involves illegal and deliberate use of biological agents, poisonous substances or chemical agents causing illness and mortality in humans, animals and plants. The purpose of such materials is to cause great damage while using a small amount of each one is very dangerous [1]. Application of the bioterrorism agents dates back to 1400 BC. Given the various events arisen from these agents, the

history of their application can be divided into two periods. The first pertains to the era before the emergence of microbiology, the World War II, and before the 1925 Geneva Protocol. The blind use of biological agents by the users has been the main characteristic of this era [2]. The second period began from 1925 and lasted until the current time. The onset of this period coincides with the development of microbial genetics and other biological and biomolecular fields. This era resulted in the development of more dangerous biological agents through methods and techniques such as mutation and selection and protoplast fusion. The advancement of human knowledge in the genetics of microbes as well as the progress in aerobiology are other effective means in the modernization of biological weapons in this period [2-4].

There are different lists of biological agents that can be used as a weapon in bioterrorism wars. These lists have been published by international organizations, research centers, and military experts. The most accepted classification of bioterrorism pathogens pertains to Centers for Disease Control and Prevention (CDC). Based on their hazards, this center categorized the pathogens into three groups [1,2,5-9]. Factors that contributed to this categorization include their profound impact on health, health fears, potential for re-dissemination, availability of protective vaccines or antimicrobial agents, proliferating pathogens, toxins or biomodulators, secondary transmission potential, and public health preparedness [2,5,7]. Each group has its own characteristics. The characteristics and the pathogens are classified and presented in Table 1. Considering the features presented and compared to chemical and nuclear weapons, biological weapons are more lethal, more powerful, less costly, easier to prepare, quitter, and deadlier. In addition, biological agents can be released through a variety of means [1,2,10-12]. According to specific features of biologic agents, their early detection is of great importance for their control.

Table 1: Characteristics and pathogens based on CDC categorization.

Agents	Features of Each Category	Pathogenic Agents of Each Category
Category A	**a)** Can be easily disseminated or transmitted from person to person; **b)** Result in high mortality rates and have the potential for major public health impact; **c)** Might cause public panic and social disruption; and **d)** Require special action for public health preparedness.	Anthrax (*Bacillus anthracis*) Botulism (*Clostridium botulinum toxin*) Plague (*Yersinia pestis*) Smallpox (*variola major*) Tularemia (*Francisella tularensis*) Viral hemorrhagic fevers, including :Filoviruses (Ebola, Marburg) and ,Arenaviruses (*Lassa, Machupo*)
Category B	• Are moderately easy to disseminate; • Result in moderate morbidity rates and low mortality rates; and • Require specific enhancements of CDC's diagnostic capacity and enhanced disease surveillance.	Brucellosis (*Brucella species*) Epsilon toxin of *Clostridium perfringens* Food safety threats (Salmonella species, *Escherichia coli* O157:H7, Shigella) Glanders (*Burkholderia mallei*) Melioidosis (*Burkholderia pseudomallei*) Psittacosis (*Chlamydia psittaci*) Q fever (*Coxiella burnetii*) Ricin toxin from *Ricinus communis* (castor beans) Staphylococcal enterotoxin B Typhus fever (*Rickettsia prowazekii*) Viral encephalitis (alphaviruses, such as eastern equine encephalitis, Venezuelan equine encephalitis, and western equine encephalitis]) Water safety threats (*Vibrio cholerae, Cryptosporidium parvum*)
Category C	Availability; Ease of production and dissemination; and Potential for high morbidity and mortality rates and major health impact.	Emerging infectious diseases such as Nipah virus and hantavirus [2, 6, 9-11] Include emerging and highly pathogenic microorganisms. With the help of genetic engineering and biotechnology, this group can be modified to be used as deadly organisms in biological warfare. These agents are a matter of concern due to the inadequate knowledge on their means of dissemination and their infection and control mechanisms. To confront the agents of this group, research should be directed towards the diagnosis, treatment, and prevention of the resulted infections [2, 6, 10,11]

The specific features of these agents include contagiousness (poisonous), ability to propagate through aerosols and hence covering a large area or the ability to infect water and food supplies ability to cause numerous fatalities, short incubation period and difficult diagnosis in the early stages stable and durable in environmental conditions and capable of retaining properties even after dissemination (especially in the aerosol form), and easy production and dissemination (especially in large quantities) [2,11,13]. Research results have shown that the Bioterrorism Information System (BIS) can systematically and continuously collect, analyse, interpret, and publish the data for early detection of outbreaks caused by bioterrorism. The system emphasizes identifying clinical symptoms based on patient behavior patterns and signs and symptoms from various references. The results of this system can be used in planning, implementation, and evaluation of public health performance to improve the management of bioterrorism events [1,2]. Timely response is another feature of this system, meaning that bioterrorism attacks are reported before the disease cluster is clinically identified [1,14,15].

According to CDC, BIS is the most effective means in the management of bioterrorism. Early detection and prompt response to bioterrorism attacks are one of the hallmarks of this system for reducing mortality [2,16]. In addition, other studies have indicated that implementation of a BIS system is effective in the management of bioterrorism events for the following reasons: collection of data that indicate the early stages of an outbreak, facilitating the identification of cases and case management, identifying and managing outbreaks, launching statistical warnings for users, providing continuous monitoring of the disease, analysing the exact process of the disease, providing timely and appropriate responses at the regional and local levels to facilitate the prevention and control of the outbreak at the national level, providing strong epidemiological information to assist in the long-term health management, planning, and policy-making [2,15-20]. Therefore, the effects of such a system depend on its features and abilities. The present study aimed to investigate the capabilities and features of BIS in effective management of bioterrorism events.

Background

Studies have indicated the importance of BIS in the management of bioterrorism events. BIS is capable of early detection of attacks and thereby can help effectively manage bioterrorism based on five technology groups including detection, communication, diagnosis and clinical management, surveillance, and supporting technology [2,21]. In addition, by introducing the key features of the BIS, studies consider this system as the core of effective management of bioterrorism events. The key features of the system are timeliness and rapid and early detection of the outbreak, high sensitivity and specificity, routine analysis of the data to facilitate decision-making and tracking the outbreak before the final diagnosis and laboratory approvals, using diverse and varied data sources, flexibility, rapid transfer and distribution of information [2,19,22]. Timeliness is critical in the bioterrorism events' management given that the effective treatment of bioterrorism diseases is contingent on its timely identification. High sensitivity is important because the delay in identification of bioterrorism cases is regarded as a failure in its identification. In addition, a low specificity level leads to an increased number of false warnings entailing health costs [18-20,22-24].

Research results have shown that BIS uses a variety of sources to increase accuracy [17]. These data resources are required for timely identification of bioterrorism events [25]. Integration of diverse data from various data resources provides the following advantages for managing bioterrorism events:

a) Simultaneous assessment of numerous health indicators.

b) Comparison of the aberrations to compare the trends of bioterrorism-induced illness.

c) Identification of confounding factors and reducing the system false warnings [2,18].

The results of various studies point out the capabilities and characteristics of BIS in effective management of bioterrorism events. For example, BIS employs the FSIS Automated Corporate Technology Suite (FACTS), which is an integrated information system, to reduce the data redundancy and increase the accuracy, completeness, and timeliness [1,2]. Moreover, BIS can also incorporate the Handheld Advanced Nucleic Acid Analyzer (HANAA) technology capable of identifying the biological agent in less than 30 minutes after the start of its dissemination. Therefore, such features can improve the BIS performance in the management of bioterrorism events [26].

Biological Defense Initiative (BDI) is another feature of this system. This is a national model for identification of bioterrorism events by integrating information from various detectors including BASIS, Portal Shield, RSVP, ESSENSE, and B-Safer [2]. By incorporating laboratory monitoring, the system performance is increased in the management of bioterrorism events. CDC has launched the Laboratory Response Network (LRN) to detect and identify biological agents. The laboratories of this network are categorized in four levels (A-D) according to their capabilities. The Level A laboratory has the minimum facilities to detect the suspicious samples using simple tests. This lab should send suspicious samples to a higher-level lab [2]. In this classification, based on biosafety levels (BL), the low-risk pathogens are placed at BL1 and the high-risk pathogens at BL4 [2,21]. This capability has increased the capacity of quick identification of RODS in the management of bioterrorism events [2,20]. BIS provides the appropriate threshold based on coding models, syndromic classification, risk prediction models, and strong base data. This feature is effective in reducing the errors in decision-making regarding the management of bioterrorism events [2,17].

For example, RODS use the syndromic classification based on Bayesian classifiers [27]. In addition, this system analyses the bioterrorism outbreaks information using warning detection algorithms and temporal and spatial statistical methods along with Natural Language Processing (NLP) [27-30]. This feature increases the analytical power of the system in the management process. According to studies on the use of communication networks, three requirements should be met to increase the power and capacity of the system in managing bioterrorism events: complying with the data transfer standards, the use of Internet-based communication infrastructures, and compliance with the agreements pertaining to the confidentiality principles when sharing information [2]. The BioWatch dashboard pertains to the information sharing and distribution technologies in BIS [31]. In addition, the use of charts, GIS, and LDAP protocols is mentioned in RODS and BioSense [28,32]. RODS use new software such as ArcIMS package and Map plot screen, which facilitates the update process and allows information to be displayed based on the time, region, and type of syndrome [28,30].

Reliance of the system on timely methods of distribution and display for generation of reports [33] allows rapid assessment of changes to identify the outbreaks quickly [22]. An example of this capability is the timely reporting of aberrations according to the Early Aberration Reporting System (EARS) [22,30]. Provision of option for users is another significant feature of the system. In this feature, users can determine and select a valid method for detecting the aberration and change and modify the threshold of warning sensitivity and specificity [22]. The use of various portals increases the system's power in the distribution and display stages. For example, the ESSENCEII system provides four portals to the users to allow them view raw data and their processing results. These four portals include a map portal which presents the geographical distribution of the data, a warning list portal, a search portal, and a report summary portal [34].

Findings

In general, the capabilities and characteristics of BIS which contributes to the effective management of relevant incidents can be divided into 10 categories [2,33,35-37].

Diverse Data Resources Relying on Superior Technologies

Types of data resources for the BIS are divided into five categories:

i) Data and evidence before the diagnosis of illness such as person's behavior (absenteeism) and OTC sale [30]. These data are timely and non-specific (preclinical with low specificity percentage). An example of this model is the use of data related to the human behavior in the Bio Alert System developed by Defense Advanced Research Projects Agency (DARPA) [2,21]. In addition, the use of keywords on the Internet in Google to identify early outbreaks can also be included in this category [2,20].

ii) Laboratory symptom and orders which are timely and relatively specific (clinical or pre-diagnostic) [2,24].

iii) Final diagnosis of illnesses and results of tests, which though not timely, are specific with a high specificity [2,24].

iv) Data from biological detectors and biosensors that are both timely and have a high sensitivity and specificity [2]. Molecular Recognition-based Real Time Detection [21] and Epidemic Outbreak Surveillance (EOS) are two examples of this type. These systems are capable of an early identification of biological events according to DNA-based advanced technologies [2]

v) Data from security agencies based on the presence of a biological agent at a specific location and time [2].

Environmental Surveillance

In this system, continuous sampling reveals the presence of biological agents in various environments. Examples of these systems include remote identification systems such as radar and doppler radio as well as point detection systems such as EpiSPIRE and BioWatch [20].

Laboratory and Antimicrobial Resistance Surveillance

In this case, timely collection, analysis, and reporting of important antibiotic-resistant pathogens are carried out to identify biological agents [21]. Studies have shown that the sensitivity of these systems are 76-100% [23]. As a specific ability, it can identify unusual organisms such as anthrax, smallpox, and Ebola, as well as known and antibiotic-resistant organisms [38].

Event-Based Surveillance

Although many BISs continuously collect, analyse, and report data, some systems are intended for short-term use. These systems are known as event-based or drop-in systems [20] and are built following specific events such as Super Bowl. The bioterrorism syndromic surveillance system, which was created after September 11th, 2001 in New York for 30 days in 15 emergency units, is an example of this model [17,27,39].

Coding Models and Vocabulary Standard

BISs use classification systems in the form of four categories: classification systems, core vocabularies, cross reference ontology, and messaging standard in public health [30,37,40-42].

Robust, Automatic, and Timely Processing and Statistical Analysis System

This feature is based on Strong Outbreak Recognition Algorithms and robust, reliable, and flexible prospective and retrospective statistical methods for changing the threshold of sensitivity and specificity indices with respect to time and place [1,2,22,34,36,43-46].

Problem Solving Methodology and Anthology

BioStorm is the most prominent example of this system and a type of knowledge-based BIS [24,30]. Problem solving methods in this system are directed based on knowledge adjusted by anthology [24,30,47].

Communication Networks to Facilitate Data Sharing

BISs use communication networks to increase interoperability and provide accurate and timely reports [2]. The most common communication networks used in BISs are:

National Laboratory Response Network (NLRN): Aiming to establish a secure network for providing standard diagnostic protocols for bioterrorism laboratories [2,20,48].

Epidemic Information Exchange (Epi-X): Aiming to facilitate the secure communication between epidemiologists for rapid analysis and reporting [2,48-50].

CDC's Health Alert Network (HAN): Aiming to facilitate communication and sending messages to health professionals [50]. This health alert network pertains to the provision of early warnings in response to bioterrorism events [2,21].

Public Health Information Network (PHIN): Aiming at proper and secure exchange of information related to BIS in five performance fields of identification, surveillance, data analysis, knowledge management, health warning, and response [37,51-53].

National Environmental Public Health Tracking Network (NEPHTN): The BIS pertaining to identification of environmental threats communicates with this network [2,21].

Information Sharing and Distribution Technologies: In this feature, spatial- and temporal-based information distribution technologies such as GIS, dashboard, and rapid and precise warning system are used [24,30,47] for the productivity of information distribution. Other BIS capabilities in this category include use of specific portals, automatic message sending system to inform specialists [54] and use of alert system for bioterrorism events in the form of the National Bioterrorism Security Advisory from severe threat (red) to mild threat (green) [1,2,55].

Legal and Security Requirements

Regarding legal requirements, the two following requirements can be pointed out:

a. Compliance with General Standards of ASTM, HL7, and ISO [49,53,56-58].

b. Compliance with the specific standards of BIS, such as Pandemic and All-Hazards Preparedness Act (PAHPA) [50] and Resolution 1540 of the United Nations Security Council, and compliance with security requirements and connection to security centers such as the FBI [20,28,30,37].

As its point of strength, BIS complies with the security requirements in the following five areas in the management of bioterrorism events: security management and policy making of BIS, system software security, security in the field of human resources, security in the field of equipment and hardware, security in the field of data collection and processing, and storage, transmission, and distribution of information [1,2]. Each BIS has specific features, each of which uses one or more technology groups that are effective in the three stages of management. All features discussed in the Table are effective with varying intensity and strength in three stages of prevention, response, and recovery in the bioterrorism events' management (Table 2).

Table 2: Capabilities of BIS based on technology groups in the management of bioterrorism events.

	Capabilities of BIS	IT Categories					System	References
		Supporting technology	Communication	Diagnosis and clinical management	Surveillance	Detection		
1	Diverse data resources	*				*	BASIS, Portal Shield, RSVP, ESSENSE, B-Safer	[2]
2	Environmental surveillance	*				*	Biowatch EpiSPIRE	[20]
3	Laboratory and antimicrobial resistance surveillance	*		*		*	RODS	[2]
4	Event-based surveillance	*				*	Drop-in surveillance 1	[37]
5	Coding models and vocabulary standard	*			*	*	RODS	[2]
6	Robust, automatic, and timely processing and statistical analysis system		*			*	BioPortal	[30,57]
7	Problem solving methodology and anthology	*				*	BioStorm	[24,30,47]

8	Communication networks to facilitate data sharing			*	*	*	RODS	[2]
9	Information sharing and distribution technologies			*	*	*	BioWatch	[31]
10	Legal and security requirements			*	*	*	NBSSDP[2] RODS	[20,28,30,37,45,58]

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

2-National Bioterrorism Syndromic Surveillance Demonstration Program

Conclusion

BIS is considered as the main element in all stages of the bioterrorism events' management, namely the prevention, response, and recovery stages. By designing and implementing the system based on the features and capabilities presented in this paper, the system will be able to play an active and effective role in the triple stages of bioterrorism events management. Focusing on management and technical features and abilities in all three stages will help manage the bioterrorism events effectively. Enhancing each of the BIS features will improve the system power in different stages of management. Finally, effective management of bioterrorism events will increase the social security and health.

Suggestions

a) It is suggested that various data sources be used in designing the National Bioterrorism Information System. Equipping the system with biological detectors and biosensors as well as using information related to the threats of bioterrorism attacks obtained from intelligence and security organizations have led to a real-time and accurate detection of bioterrorism outbreaks.

b) It is recommended that coding systems and national vocabulary systems be used for every region for an accurate and real-time bioterrorism outbreak detection.

c) It is suggested that localization in the classification of biological agents based on the demographic and epidemiological features of a country for National Bioterrorism Information System be considered.

d) It is recommended that policy and security priorities based on environmental surveillance, Laboratory and antimicrobial resistance surveillance and event-based surveillance be considered in strategy selection for system performance.

e) It is recommended that flexible and advanced statistical methods be used at data processing phase. Geographic features of the region, demographic characteristics, classified system selection, epidemic diseases, determination of syndrome groups, and attention to the season and time of the event are significant points in order to determine threshold in data processing phase.

f) It is suggested that security policies of each country, the extent and the impact of the bioterrorism event be considered for information sharing and distribution technologies in National Bioterrorism Information System.

Competing interests: The authors declare that they have no competing interests.

References

1. Moghaddasi H, Shokrizadeh Arani l, Zarghi A (2018) Features of Bioterrorism Information System. Journal of Bioterrorism & Biodefense 9(2): 1-6.
2. Shokrizadeh Arani L (2018) Providing Architecture Model of National Bioterrorism Information System with Database Approach for Iran. Tehran: Shahid Beheshti University of Medical Science.
3. Barras V, Greub G (2014) History of biological warfare and bioterrorism. Clinical Microbiology and Infection 20(6): 497-502.
4. Hadian B, Moghassemi A (2017) Bioterrorism, a threat to general health. Lorestan University of MedicalScience Quarterly Yafteh 19(3): 33-40.
5. Pappas G, Panagopoulou P, Akritidis N (2009) Reclassifying bioterrorism risk: are we preparing for the proper pathogens? Journal of infection and public health 2(2): 55-61.
6. Zare Bidaki M, Balali Mood M (2015) Bioterrorism and Biological Warfare, from Past to the Present: A classic review. Journal of Birjand University of Medical Sciences 22(3): 182-198.
7. Evans S, Kleinman K, Pagano M (2018) Statistics in Defense and National Security: Bioterrorism and Biosurveillance.
8. Pinto VN (2013) Bioterrorism: Health sector alertness. Journal of Natural Science, Biology, and Medicine 4(1): 24-28.
9. CDC (2018) Bioterrorism Agents/Diseases USA: CDC.
10. Balali Mood M, Moshiri M, Etemad L (2013) Medical aspects of bio-terrorism. Toxicon 69: 131-142.
11. Plianbangchang S (2005) Strategies of Preparedness against the Threat of Biological W eat of Biological W eat of Biological Warfare and Bioterrorism in South-East Asia. Asian Biotechnology and Development Review 8(1): 77-98.
12. Graham B, Talent J (2009) Bioterrorism: redefining prevention. Mary Ann Liebert, Inc. 140 Huguenot Street, 3rd Floor New Rochelle, NY 10801 USA.
13. Joshi D, Kumar D, Maini AK, Sharma RC (2013) Detection of biological warfare agents using ultra violet-laser induced fluorescence LIDAR. Spectrochimica Acta Part A: Molecular and Biomolecular Spectroscopy 112: 446-456.
14. Ansaldi F, Orsi GB, Altomonte F, Bertone G, Parodi V, et al. (2008) Emergency department syndromic surveillance system for early detection of 5 syndromes: a pilot project in a reference teaching hospital in Genoa, Italy. Journal of preventive medicine and hygiene 49(4): 131-135.
15. Buehler JW, Berkelman RL, Hartley DM, Peters CJ (2003) Syndromic surveillance and bioterrorism-related epidemics. Emerging infectious diseases 9(10): 1197-1204.
16. Chang M-h, Glynn MK, Groseclose SL (2003) Endemic, notifiable

bioterrorism-related diseases, United States, 1992-1999. Emerging infectious diseases 9(5): 556.

17. Uhde KB (2003) Bioterrorism syndromic surveillance: A dual-use approach with direct application to the detection of infectious disease outbreaks. USA: University of South Florida.

18. Pavlin JA, Mostashari F, Kortepeter MG, Hynes NA, Chotani RA, et al. (2003) Innovative surveillance methods for rapid detection of disease outbreaks and bioterrorism: results of an interagency workshop on health indicator surveillance. American Journal of Public Health 93(8): 1230-1235.

19. Henning KJ (2004) What is syndromic surveillance? Morbidity and Mortality Weekly Report 53: 5-11.

20. Kman NE, Bachmann DJ (2012) Biosurveillance: a review and update. Advances in preventive medicine, p. 1-9.

21. US GAO America (2003) Bioterrorism: Information Technology Strategy Could Strengthen Federal Agencies' Abilities to Respond to Public Health Emergencies. In: United States General Accounting Office, editor. Washington, DC, USA.

22. Hutwagner L, Thompson W, Seeman GM, Treadwell T (2003) The bioterrorism preparedness and response early aberration reporting system (EARS). Journal of Urban Health 80(2Supply1): 89-96.

23. Bravata DM, McDonald KM, Smith WM, Rydzak C, Szeto H, et al. (2004) Systematic review: surveillance systems for early detection of bioterrorism-related diseases. Annals of Internal Medicine 140(11): 910-922.

24. Buckeridge DL, Graham J, O'Connor MJ, Choy MK, Tu SW, et al. (2002) Knowledge-based bioterrorism surveillance. Proceedings of the AMIA Symposium American Medical Informatics Association, p. 76-80.

25. Asatryan A, Benoit S, Ma H, English R, Elkin P, et al. (2011) Detection of pneumonia using free-text radiology reports in the BioSense system. International journal of medical informatics 80(1): 67-73.

26. D'Amico W, Mugavero R (2013) Bioterrorism and public health service: Defining management and treatment systems. Biosafety 2: 110.

27. Tsui F-C, Espino JU, Dato VM, Gesteland PH, Hutman J, et al. (2003) Technical description of RODS: a real-time public health surveillance system. Journal of the American Medical Informatics Association 10(5): 399-408.

28. Espino JU, Wagner M, Szczepaniak C, Tsui F, Su H, et al. (2004) Removing a barrier to computer-based outbreak and disease surveillance-the RODS open source project. Morbidity and Mortality Weekly Report 53: 32-39.

29. Moore KM, Edgar BL, McGuinness D (2008) Implementation of an automated, real-time public health surveillance system linking emergency departments and health units: rationale and methodology. Canadian Journal of Emergency Medicine 10(2): 114-119.

30. Yan P, Chen H, Zeng D (2008) Syndromic surveillance systems. Annual review of information science and technology 42(1): 425-495.

31. Cheng CK, Ip DK, Cowling BJ, Ho LM, Leung GM, et al. (2011) Digital dashboard design using multiple data streams for disease surveillance with influenza surveillance as an example. Journal of medical Internet research 13(4): 85.

32. Loonsk JW (2004) BioSense-a national initiative for early detection and quantification of public health emergencies. Morbidity and Mortality Weekly Report 53: 53-55.

33. Yan W, Palm L, Lu X, Nie S, Xu B, et al. (2013) ISS-an electronic syndromic surveillance system for infectious disease in rural China. PLoS One 8(4): e62749.

34. Lombardo JS, Burkom H, Pavlin J (2004) ESSENCE II and the framework for evaluating syndromic surveillance systems. Morbidity and Mortality Weekly Report 53(Supply): 159-165.

35. Reis BY, Mandl KD (2004) Syndromic surveillance: the effects of syndrome grouping on model accuracy and outbreak detection. Annals of emergency medicine 44(3): 235-241.

36. Lober WB, Karras BT, Wagner MM, Overhage JM, Davidson AJ, et al. (2002) Roundtable on bioterrorism detection: information system–based surveillance. Journal of the American Medical Informatics Association 9(2): 105-115.

37. Mandl KD, Overhage JM, Wagner MM, Lober WB, Sebastiani P, et al. (2004) Implementing syndromic surveillance: a practical guide informed by the early experience. Journal of the American Medical Informatics Association 11(2): 141-150.

38. Parker JT, Juren A C, Lowe L, Santibañez S, Rhie G e, Merlin TL (2017) Enhancing laboratory response network capacity in South Korea. Emerging infectious diseases 23(Suppl 1): 126.

39. Wagar E (2016) Bioterrorism and the role of the clinical microbiology laboratory. Clinical microbiology reviews 29(1): 175-189.

40. Lober WB, Trigg L, Karras B (2004) Information system architectures for syndromic surveillance. Morbidity and Mortality Weekly Report 53: 203-208.

41. Siswoyo H, Permana M, Larasati RP, Farid J, Suryadi A, et al. (2008) EWORS: using a syndromic-based surveillance tool for disease outbreak detection in Indonesia. BMC proceedings 2(Supply3): 3.

42. Chretien JP, Blazes D, Mundaca C, Glass J, Lewis SH, et al. (2006) Surveillance for Emerging Infection Epidemics in Developing Countries: EWORS and Alerta DISAMAR. Wiley & Sons 30: 367-396.

43. Platt R, Bocchino C, Caldwell B, Harmon R, Kleinman K, Lazarus R, et al. (2003) Syndromic surveillance using minimum transfer of identifiable data: the example of the National Bioterrorism Syndromic Surveillance Demonstration Program. Journal of Urban Health 80(2Supply1): 25-31.

44. Zeng D, Chen H, Tseng C, Chang W, Eidson M, et al. (2005) BioPortal: A case study in infectious disease informatics. Proceedings of the 5th ACM/IEEE-CS joint conference on Digital libraries.

45. Yih WK, Caldwell B, Harmon R, Kleinman K, Lazarus R, et al. (2004) National bioterrorism syndromic surveillance demonstration program. Morbidity and Mortality Weekly Report 53(Supply): 43-49.

46. Wang S, Han H, Ki M (2005) Development of a Comprehensive Bioterrorism Information System in Korea. Prehospital and Disaster Medicine 20(Supply1): 97.

47. Crubézy M, O'Connor M, Pincus Z, Musen MA, Buckeridge DL (2005) Ontology-centered syndromic surveillance for bioterrorism. IEEE Intelligent Systems 20(5): 26-35.

48. Koplan J (2001) CDC's strategic plan for bioterrorism preparedness and response. Public health reports 116(Suppl 2): 9-16.

49. Kun LG, Bray DA (2002) Information infrastructure tools for bioterrorism preparedness. IEEE engineering in medicine and biology magazine 21(5): 69-85.

50. Ali S Khan, Alexandra M Levitt (2000) Biological and chemical terrorism: strategic plan for preparedness and response. MMWR 49: 1-14.

51. Siswoyo H, Permana M, Larasati RP, Farid J, Suryadi A, et al. (2008) EWORS: using a syndromic-based surveillance tool for disease outbreak detection in Indonesia. BMC proceedings 2(Supply3): 3.

52. Broome CV, Loonsk J (2004) Public Health Information Network-improving early detection by using a standards-based approach to connecting public health and clinical medicine. Morbidity and Mortality Weekly Report 53(Supply): 199-202.

53. Morris T, Cicchinelli M, McGarvey S, Johnson J, Conn LA, et al. (2005) PHIN Preparedness: Outbreak Management. AMIA Annual Symposium Proceedings, pp. 1176.

54. Wang S, Han H, Ki M (2005) Development of a Comprehensive

Bioterrorism Information System in Korea. Prehospital and Disaster Medicine 20(Supply1): 97.

55. Bravata DM, McDonald K, Owens DK, Wilhelm ER, Brandeau ML, et al. (2004) Regionalization of bioterrorism preparedness and response. Evidence report/technology assessment (Summary).

56. Buckeridge DL, Burkom H, Campbell M, Hogan WR, Moore AW (2005) Algorithms for rapid outbreak detection: a research synthesis. Journal of biomedical informatics 38(2): 99-113.

57. Tseng C, Lynch C, Gotham I, Eidson M, Chang W, et al. (2005) BioPortal: A case study in infectious disease informatics. Proceedings of the 5th ACM/ IEEE-CS Joint Conference on Digital Libraries (JCDL'05); IEEE.

58. Platt R, Bocchino MC, Caldwell B, Harmon R, Kleinman K, et al. (2003) Syndromic surveillance using minimum transfer of identifiable data: the example of the National Bioterrorism Syndromic Surveillance Demonstration Program. Journal of Urban Health 80(Sapply1): 25-31.

ISSN: 2574-1241

DOI: 10.26717/BJSTR.2019.16.002887

Hamid Moghaddasi. Biomed J Sci & Tech Res