Journal of Bioterrorism & Biodefense

Moghaddasi et al., J Bioterror Biodef 2018, 9:2
DOI: 10.4172/2157-2526.1000162

Research Article Open Access

Features of Bioterrorism Information System

Moghaddasi H[1]*, Shokrizadeh Arani L[2] and Zarghi A[3]

[1]Department of Health Information Technology and Management, School of Allied Medical Sciences, Shahid Beheshti University of Medical Sciences, Tehran, Iran
[2]International Branch of Beheshti University of Medical Sciences and Health Services, Tehran, Iran
[3]Department of Pharmaceutical Chemistry, School of Pharmacy, Shahid Beheshti University of Medical Sciences, Tehran, Iran

Abstract

Background and objectives: Bioterrorism Information System has been widely used under different titles for real-time detection, control and evaluation of bioterrorism attacks in various countries. Appling such system, based on various characteristics, leads to reduction of epidemiological effects and reduction of its etiologic factors in the community whose benefits are real-time health response and increasing national security. The effects of such a system depend on its features. This study aims to investigate the features of Bioterrorism Information System.

Method: To accomplish this review study, 150 articles including the key words of Sentinel Surveillance, Biosurveillance, Disease Outbreaks, Bioterrorism and Information Systems were originally derived from the ProQuest, PubMed, Web of Science, Scopus and Google Scholar databases. 150 articles dated 1980-2017 were found of which 79 were analytically identified as the main ones according to the content.

Results: Based on this study, the features of Bioterrorism Information System were classified into five main categories: collection, processing, distribution of data, legal requirements, and Security requirements.

Conclusion: Identifying the features of the Bioterrorism Information System is an important step in its designing. If the Bioterrorism Information System is properly designed and its features are considered in terms of collection, processing, distribution, security and legal requirements, it will more effectively detect bioterrorism attacks.

Keywords: Information systems; Bioterrorism; Sentinel surveillance; Biosurveillance; Disease outbreaks

Introduction

One of the most important types of terrorism is bioterrorism which involves deliberate and illegal use of biological agents, poisonous substances or chemical agents causing mortality and illness in humans, animals and plants. The purpose of such materials is to cause great damage while using a small amount [1-3]. The most important and the most dangerous bioterrorism factors are Anthrax (Bacillus anthracis), Smallpox (variola major) and Viral hemorrhagic fevers(including Filoviruses (Ebola).The most appropriate classification for bioterrorism agents belongs to CDC (Centers for Disease Control and Prevention), which classifies the factors into three categories based on their risk level [4-8]. Potential 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. In comparison to nuclear weapons, biological agents have no destructive effects [9]. The bioterrorism agents are more powerful, simpler to provide, less costly, less sophisticated but more lethal. There is also a diversity of agents for the dissemination of biological substances [10-13]. Bioterrorism weapons are not comparable in terms of diversity and scope of action with other weapons [14]. Concerns related to the spread of a disease caused by bioterrorism in society are much more further than the explosion caused by other war weapons [3,13]. On the other hand, the specific characteristics of biological materials and the development of genetic changes in biological warfare agents, together with other factors, have made it more difficult to identify and recognize these factors, and to treat the diseases caused by them [14-18]. Bioterrorism is a real and significant threat of the 21stcentury [19,20]. Which overshadows stability, national security, economic development, and the development process of countries. This kind of terrorism, more than before, has been considered as a remerging and asymmetric health problem, and is now considered an emergency state of national security for many countries. The solution to this problem is to provide a Bioterrorism Information System [21-24]. Hence a large budget has been allocated to research and development of Bioterrorism Information Systems by different countries [6,12,25]. The effectiveness of the Bioterrorism Information System is based on collection and accurate statistical analysis of data about bioterrorism attacks. The basis of this system is information obtained from patients or suspected cases [6,26,27] that are effective in identifying early bioterrorism attacks. This system helps to identify bioterrorism outbreaks using signs, symptom, laboratory findings and other non-clinical information from various sources before confirming 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, what is more, it leads to preservation and promotion of national security [28-34]. The findings of various studies have shown that Bioterrorism Information System can pursue numerous therapeutic, epidemiological, secure and healthy goals with indicators such as high sensitivity and specificity, timeliness and flexibility. These objectives include: Facilitating the accurate and rapid recognition of bioterrorism-related diseases, improving the speed of analysis and data transmission, providing detailed information for evaluating bioterrorism attacks, assisting in determining exposure sites through

***Corresponding author:** Moghaddasi H, Associate Professor, 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, Tel: 9038711190; E-mail: Moghaddasi@sbmu.ac.ir

Received May 04, 2018; **Accepted** March 30, 2018; **Published** June 05, 2018

Citation: Moghaddasi H, Arani LS, Zarghi A (2018) Features of Bioterrorism Information System. J Bioterror Biodef 9: 162. doi: 10.4172/2157-2526.1000162

GIS (Geographic Information Systems), facilitating the integration of bioterrorism information through the country, helping to accomplish effective services, such as the process of vaccination and antibiotic therapy, helping to treat early-onset illnesses leading to death quickly, evaluating the success in the inhibition of disease along with reducing its burden in the area, intercepting the chain or the transmission of secondary diseases, providing historical data to be used as a base for statistical comparisons and long-term monitoring of health [32,33,35]. The effects of Bioterrorism Information System depend on its features. Therefore, the purpose of this study is to survey the features of Bioterrorism Information System.

Methods

To conduct this review study, the keywords Sentinel Surveillance, Disease Outbreaks, Bioterrorism, Information systems and Biosurveillance were firstly obtained in 150 articles from databases like Science Direct, Pro Quest, Pub Med, Sid, Springer, Google scholar and Web of Science in the period from 1980 to 2017. After reviewing the titles and abstracts of these articles, 40 were excluded due to non-alignment with the objectives of the study but110 met the requirement of the study. Having analyzed the quality of the articles, the authors identified and used 79 studies as the main ones, based on the contents of the articles and their sources.

Background

Bioterrorism Information System has been widely developed in different countries under different titles for the early detection and rapid control of epidemics as well as their evaluation. One of the features of this system is timely response and reaction. This means that bioterrorism attacks are reported before clinically recognizing the cluster of diseases [36,37]. Bioterrorism Information System with numerous features in the field of data collection and processing, and information distribution, as well as legal and security requirements can reduce epidemiological effects, rate of disease transmission and burden of disease in the community. Finally, more appropriate healthy response and, as a result, an increase in national security are the outcomes of implementation such system [38-40]. Hughes announced that a bioterrorism information system has a real-time surveillance capability and is capable of rapidly exchanging information at the national and regional level, which will help to strengthen the health and security system [32]. In this regard, the Statistics Committee in Defense and National Security (DNS) emphasized the importance of the existence of Bioterrorism Information System because of its secure communication network and power of statistical analysis of incidents [6]. Research results have shown that Bioterrorism Information System, using powerful tools and technologies, new statistical and mathematical models, using GIS, rapid and effective transmission of information to responsible authorities, can help to respond the bioterrorism events [7,13]. Considering the importance of Bioterrorism Information System and its ability for real-time bioterrorism outbreak detection, its development has been prioritized by different countries. For this reason, from 2001 to 2014, there has been an increase in funding for creation and development of such system in security and health organizations of the United States, the United Kingdom and Australia [41-46]. Centers for Disease Control and Prevention (CDC) in America uses various information systems such as Biosurveillance, BioSense, B-SAFER, Biodefend, RSVP and BioStorm to detect and manage bioterrorism events [6,39,47-50]. It should be noted that relying on ontology and problem-solving methods are important features of BioStorm which is also a knowledge-based system [3,50-52]. Equipping the Bioterrorism Information System with advanced detectors based on genome and PCR technologies will increase its validity and sensitivity. Also, the strengths of the Biowatch system include increasing the speed and accuracy of detecting bioterrorism events, and its equipping with robust and highly sensitive detectors [3]. Each of the features of the information system has specific capability. For example, in the data collection phase, FACTS[1] technology (a data integrator system) reduces data redundancy and increases accuracy, completeness and timeliness [46]. The use of diverse data sources increases the power of Bioterrorism Information System in detecting attacks [53]. Also, the results of studies have shown that, in order to increase the accuracy, various systems of bioterrorism surveillance use different data sources [54]. These sources of data are one of the requirements to assess the timely detection of bioterrorism events [55]. Biosurveillance, BioSense, B-SAFER, Biodefend, RSVP in the United States, and Syndromic Surveillance System in England are well known to use the accurate and diverse data sources including Non-clinical data sources such as OTC (Over-The-Counter medicines), school and workplace absenteeism data [37,47-50,54,55]. In Japan and Scotland, the features of the Bioterrorism Information System are based on the clinical and non-clinical data, and also on population-based behavior. The first category includes data such as data based on emergency departments, the cause of death, information from general physicians (GPs), poison centers, and laboratories. In the second part are there information such as: evaluating the searched words from the internet, nurse hotline, social media surveys, school and workplace absenteeism, and OTC data [40,56]. Another important feature of the Bioterrorism Information System is its syndromic Surveillance. The emphasis of this type of surveillance is on the symptom illness. This system compared with traditional disease surveillance that is based on the final diagnosis, requires less time to detect the outbreak of bioterrorism. This feature has been introduced as a real-time detection [40,57]. BioPortal has the attribute of using the reliable and strong prospective and retrospective statistical methodsm [50,58] in the United States. ESSENCE is well known for its robust processing feature using spatial and temporal detection methods and the use of a combination of military and civilian information [50,59,60]. In America, BioSense uses the statistical method of SPC[2] and an exact analysis to detect bioterrorism attacks [54,55]. EpiSPIRE, RODS, and LEADERS in the United States [48-50,57,61,62] and ISS[3] in China work based on a precise and accurate display and dissemination methods such as Dashboards and GIS [63]. NBSSDP[4] and LEADERS[5] in the US have security requirements [31,49,50,64]. Korea's Bioterrorism Information System has an automatic and timely statistical analysis system, produces reports, and creates an automatic notification system to inform specialists .Its other feature is its reliance on emergency department data [65]. Other notable features of the Bioterrorism Information System are that this system has met the validated legal requirements and has the international telecommunication network via connecting to the security centers and following the guidelines developed by these organizations. This feature is in IDSP[6] system in India [7] and RODS in the United States as a factor in expediting outbreak detection [48,50,57,62].

Results and Discussion

In general, the characteristics of the Bioterrorism Information System (Table 1) can be divided into five general categories according to the methodological steps and main functions of the system [28,57,63,66].

[1] FSIS Automated Corporate Technology Suite (FACTS)
[2] Statistical Process Control
[3] Electronic surveillance system (ISS)
[4] National Bioterrorism Syndromic Surveillance Demonstration Program
[5] Lightweight Epidemiology Advanced Detection and Emergency Response System
[6] Integrated Disease Surveillance Project

Features of the Bioterrorism Information System in the data collection phase

The integration of diverse data obtained from various data sources [33,35,54] Examples include the use of clinical and non-clinical data, such as school absenteeism data [29] and OTC [50].

The Acquisition of essential data in real time using accurate and timely collection methods [66] such as the use of biological detectors, accurate and sensitive biosensors, and data integrator technology [67,68].

Use of Data verification in order to reduce data redundancy, increase the accuracy, completeness and timeliness of data using the advanced technology such as FACTS[7] [46].

The Acquisition and collection of data from security agencies related to bioterrorism events.

Features of Bioterrorism Information system in the processing phase

The features of classification, organization, analysis and detection of bioterrorism attack are found in this group.

Using coding systems and vocabulary standards [50,69-71].

Using a robust and timely processing system [50,59,66] especially using the prospective and retrospective statistical methods that are valid and flexible to modify sensitivity and specificity thresholds based on time and place [31,50,53,58,64].

Automatic statistical analysis system [65].

Knowledge-based, ontology-based and using the problem-solving methods [50-52].

Features of Bioterrorism Information System in the Distribution Stage

This feature is relevant to reporting and disseminating information.

Relying on a timely distribution and display method for reporting [63] such as real-time reporting based on the EARS method (Early Aberration Reporting System) [50,53].

Creating an automatic message sending system to inform specialists [65].

The use of information dissemination technology based on time and place such as the use of GIS, dashboards as well as accurate and rapid alert systems [50-52] to increase efficiency for data dissemination. An example for this feature is "use of dashboards in BioWatch" [72].

Using the network to facilitate sharing of data, such as the use of crisis information sharing platform technology (CRISP), Public Health Information Network (PHIN), and National Food Safety Laboratory System (NFSLS) [3,46,63].

Using the alert system for bioterrorism events such as National Bioterrorism Security Advisory System from severe threat (red) to low threat (green) [30].

Features of Bioterrorism Information System related to security requirements

It includes secure and valid coding, acquisition, collection, transmission, storage and delivery of information, with emphasis on maintaining the main attributes of data security such as integrity, availability, and confidentiality [71,73].

Security management and policy making for the Bioterrorism Information System, including risk management [identifying and prioritizing the existing security threats to the Bioterrorism Information System] and security policy management (determining the sanction policy for non-compliance requirements and determining how the information system is accessed by authorized members).

Software system security, with an emphasis on maintaining the basic concepts of security, including integrity, availability, and confidentiality [71,73].

Security in human resources domain [skills, training and experience] such as informing users about the legal consequences of disclosure.

Security in hardware and equipment domain, such as damage assessment (regular scanning of network systems and its infrastructure), ensuring the continuous update of equipment and the existence of instructions to ensure the physical safety of equipment [50,57,59,66].

Security in the collection, processing, storage, transmission and dissemination of information through the use of encryption methods in the data collection phase [60]. Also, compliance with security standards for transmission messages and information in the Bioterrorism Information System [50,57], use of secure communication networks such as Epi-X (CDC's Epidemic Information Exchange (Epi-X)and BIOTOX and compliance with applicable security laws such as HIPAA and also the use of security technologies like SSL[8] [40,57,74-77].

Features of Bioterrorism Information System related to legal requirements

Following general standards such as ASTM, HL7, ISO [49,78,79]

Following specific standards of Bioterrorism Information System, such as the PAHPA[9] [22] and UN Security Council Resolution 1540, and compliance with security requirements and connection to security centers such as the FBI (Federal Bureau of Investigation) [48,50,57,62].

Each Bioterrorism Information System has specific features. But in some of these systems, a feature has been introduced as a significant feature in bioterrorism outbreaks detection.

Conclusion

In general, Bioterrorism Information System in the world is presented in two simple and complex models. The fundamental difference between these two models is related to the time when bioterrorism attacks are identified, so that more sophisticated and more complex systems are more successful and effective in detecting early outbreak. The use of advanced technology varies according to the financial and scientific progress capacity in countries. Its history dates back to September 11, 2001, simultaneously with the release of envelopes containing anthrax spores. Considering the17-year history of the system and advanced technology in the United States, it has increased its capabilities and facilities.

The features of this system that have led to the prominence of this system include:

– Being equipped with biological detectors and biosensors as data sources

[7] FSIS Automated Corporate Technology Suite (FACTS)

[8] Secure Socket Layer

[9] Pandemic and All-Hazards PreparednessAct (PAHPA

Row	Recourses	The country where the system was first developed	The name of the Information System	The main features of the Bioterrorism Information System based on the five phases				
				Legal requirements and system ownership	Security requirements and strong infrastructure	Distribution	Processing	Data collection
1	(50-52)	America and Canada	BioStorm				√	
2	(50)	America	BioPortal				√	
3	(6, 39)	America	Biosurveillance					√
4	(50)	America	Biodefend					√
5	(50)	America	EARS			√		
6	(50)	England	NHS Direct SSS[10]					√
7	(50, 69, 70)	Southeast Asian countries	EWORS				√	
8	(50)	America	B SAFER			√	√	√
9	(61)	America	EpiSPIRE			√		
10	(48)	America	BioSense					√
11	(50, 59)	America	ESSENCE				√	
12	(63)	China	ISS			√		
13	(7)	India	IDSP		√			
14	(50)	Japan	NIID				√	
15	(48, 50, 57, 62)	America	RODS	√		√		
16	(49)	America	LEADERS		√	√		
17	(49)	America	RSVP					√
18	(29, 50, 64)	America	NBSSDP[11]	√	√		√	

Table 1: Remarkable and significant characteristics of well-known Bioterrorism Information Systems in World related to real-time detection of bioterrorism outbreaks.

[10]NHS Direct Syndromic Surveillance system
[11]National Bioterrorism Syndromic Surveillance Demonstration Program

– The use of advanced technologies such as FACTS to integrate data

– Being connected and to security centers and using their data to anticipate bioterrorism events.

However, in developing countries where this system has recently been developed, it has shown that these systems are emergency–based surveillance in the early stages of creation, and, over time, they enhance and expand their data resource.

It can also be concluded that, due to ownership, the subsystems of Bioterrorism Information System have different legal and security requirements. RODS, as the provider of a bioterrorism information system operating under the control of the army, has much stricter security requirements.

Suggestions

- It is suggested that various data sources 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 obtained from security and intelligence organizations have led to a real and accurate detection of bioterrorism attacks. In addition, the use of clinical and non-clinical data and technologies such as FACTS in designing will increase the accuracy and reduce the redundancy of data and finally will enhance the performance of this system.

- To design the National Bioterrorism Information System, localization in the classification of biological agents based on the demographic and epidemiological features of a country should be considered.

- It is recommended that advanced and flexible statistical methods be used at 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 in order to determine threshold in data processing phase.

- Determining alert system in the design of Bioterrorism Information System depends on the security policies of each country, the extent and the impact of the bioterrorism event. Therefore, it is recommended to use different alert and notification systems based on end-user levels. Dashboard system for high-level managers, color-coded alerts system for the public (red, orange, yellow, blue and green for severe, high, elevated, guarded to low) and email or telephone notification system for epidemiologists.

- Any possible threat or attack on this system, such as unauthorized access to the network and destruction of data, should be considered. Therefore, it is recommended to follow international and national infrastructure security guidelines during the development and implementation phase in designing Bioterrorism Information System.

References

1. Pedersen C (2017) Reflecting back on the Ebola outbreak and the future of bioterrorism. Pepperdine Policy Review 9: 2.
2. Barras V, Greub G (2014) History of biological warfare and bioterrorism. Clin Microbiol Infect 20: 497-502.
3. Krishan K, Kaur B, Sharma A (2017) India's preparedness against bioterrorism: Biodefence strategies and policy measures. Current Science 113: 1675-1682.
4. Pappas G, Panagopoulou P, Akritidis N (2009) Reclassifying bioterrorism risk: Are we preparing for the proper pathogens? J Infect Public Health 2: 55-61.
5. ZareBidaki M, Balalimood M (2015) Bioterrorism and biological warfare, from past to the present 58: A classic review. Journal of Birjand University of Medical Sciences 22: 182-198.

6. Evans S, Kleinman K, Pagano M. Statistics in Defence and National Security: Bioterrorism and Biosurveillance.
7. Pinto VN (2013) Bioterrorism: Health sector alertness. J Nat Sci Biol Med 4: 24.
8. https://emergency.cdc.gov/agent/agentlist-category.asp
9. Michailiuk B (2016) Threat of biological weapons. Securitologia 1: 59-75.
10. Graham B, Talent J (2009) Bioterrorism: Redefining prevention. Biosecurity and Bioterrorism: Biodefense Strategy, Practice and Science 7: 125-126.
11. Hatami H (2002) Principles of Medical & Health of Bioterrorism. The two-day training seminar bioterrorism and public health strategies to deal with it; Tehran: Beheshti University of Medical Sciences: 5-20.
12. Rashidi Jahan H, Rezaei Rad M, Tavakoli R (2004) Preventive actions to reduce biological damage. Journal of Military Medicine (Summer 2004) 6: 129-141.
13. Plianbangchang S (2005) Strategies of Preparedness against the Threat of Biological Warfare and Bioterrorism in South-East Asia 8: 77-98.
14. Tawakoni HR, Sarafpour R, Samadi M (2005) Water and food bioterrorism. Journal of Military Medicine Spring 7: 75-82.
15. Pejmankhah S, Pejmankhah S, Mirhaghi A (2012) Effect of bioterrorism training through lecture and educational pamphlet on knowledge medical staff in hospitals of Iranshahr. Health System Research 8: 1255-1262.
16. Balali-Mood M, Moshiri M, Etemad L (2013) Medical aspects of bio-terrorism. Toxicon 69: 131-42.
17. Balali-Mood M (2012) Medical aspects of bioterrorism. Toxicon 60: 98.
18. Saraf Poor R, Faraj Zadeh D (2010) An overview of the biological weapons as a threat to drinking water sources. Ann Mil Health Sci Res Winter 299-307.
19. Kshirsagar MM, Dodamani AS, Vishwakarma PY, Dodamani GA, Jadhav HC, et al. (2017) 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 57-60.
20. Allen L (2016) Biosecurity and non-communicable diseases.
21. Sabur B (2012) The need to respect the principles of passive defense in the health system. Journal of Clinical Research in Medical Sciences 1.
22. Anathallee M, Curphey A, Beeching N, Carley S, Crawford I, et al. (2007) Emergency departments (EDs) in the United Kingdom (UK) are not prepared for emerging biological threats and bioterrorism. J Infect 54: 12-17.
23. Chauhan SS (2008) Bioterrorism and biosecurity practical solutions. Journal of Biotechnology 136: S764.
24. Masumi M (2011) Terrorism social foredoom and national security (Islamic Republic of Iran) Daneshnameh Quarterly 80: 207-235.
25. Moshtagh Eshgh Z, Aghaei N, Alavi Majd H (2007) Review of nurses' knowledge and attitudes in relation to bioterrorism in hospitals affiliated of Sari, Mazandaran University of Medical Sciences. Beheshti Faculty of Nursing and Midwifery 57: 33-38.
26. Parks LI (2004) Security and HIM. Appendix B: Syndromic Surveillance Systems in Bioterrorism and Outbreak Detection. AHIMA 75.
27. Johnson J, Scott-Waldron C, Romalewski C, Mott J. Syndromic Surveillance for the State of Louisiana. Louisiana Office of Public Health, Infectious Diseases Epidemiology Section.
28. Reis BY, Mandl KD (2004) Syndromic surveillance: The effects of syndrome grouping on model accuracy and outbreak detection. Annals of Emergency Medicine 44: 235-241.
29. 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: 910-922.
30. Bravata DM, McDonald K, Owens DK, Wilhelm ER, Brandeau ML, et al. (2004) Regionalization of bioterrorism preparedness and response. Evidence Report/ Technology Assessment 96.
31. 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: 43-49.
32. Hughes JM (1999) The emerging threat of bioterrorism. Emer infect Dis 5: 494-495.
33. Pavlin JA, Mostashari F, Kortepeter MG, Hynes NA (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: 1230-1235.
34. Pavlin JA, Kelley PW (2005) Department of Defense Global Emerging Infections System Programs in Biodefense. Biological Weapons Defense. Springer 361-385.
35. Asatryan A, Benoit S, Ma H, English R, Elkin P (2011) Detection of pneumonia using free-text radiology reports in the biosense system. Int J Med inform 80: 67-73.
36. 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. J Prev Med Hyg 49: 131-135.
37. Buehler JW, Berkelman RL, Hartley DM, Peters CJ (2003) Syndromic surveillance and bioterrorism-related epidemics. Emerg Infect Dis 9: 1197-1204.
38. Van den Wijngaard C, van Pelt W, Nagelkerke N, Kretzschmar M, Koopmans M (2011) Evaluation of syndromic surveillance in the Netherlands: Its added value and recommendations for implementation. Euro Surveill 16: 1-8.
39. Tsui FC, Espino JU, Dato VM, Gesteland PH, Hutman J, et al. (2003) Technical description of RODS: A real-time public health surveillance system. J Am Med Inform Assoc 10: 399-408.
40. Omoe H (2010) Syndromic surveillance-toward the early detection of infectious disease epidemics. NISTEP Science & Technology Foresight Center 1349-3663.
41. Australian Government Department of the Prime Minister and Cabinet (2015) Review of the Australian's counter-terrorism machinary. In: Department of the Prime Minister and Cabinet (ed) Australia: Commonwealth of Australia 2015.
42. Australia-New Zealand Counter-Terrorism Committee. National Counter-Terrorism Plan.In: Department of the Prime Minister and Cabinet (ed) Australia: Commonwealth of Australia 2017.
43. Australia-New Zealand Counter-Terrorism Committee. National Counter-Terrorism Plan (NCTP). In: Attorney General's Department (ed) Commonwealth of Australia 2012.
44. National Counterterrorism Committee (2005) National Counter-Terrorism Plan. Australia (2003): 1-29.
45. Attorney General's Department National Counter-Terrorism Plan. Australia: Commonwealth of Australia.
46. USGAO Government Accountability Office, America USo (2003) Bioterrorism: Information Technology Strategy Could Strengthen Federal Agencies' Abilities to Respond to Public Health Emergencies. Washington DC.
47. Chang MH, Glynn MK, Groseclose SL (2003) Endemic notifiable bioterrorism-related diseases, United States, 1992-1999. Emerging Infectious Diseases 9: 556-565.
48. Kman NE, Bachmann DJ (2012) Biosurveillance: A review and update. Advances in Preventive Medicine 1-9.
49. Kun LG, Bray DA (2002) Information infrastructure tools for bioterrorism preparedness. IEEE Engineering in Medicine and Biology Magazine 21: 69-85.
50. Yan P, Chen H, Zeng D (2008) Syndromic surveillance systems. Annual Review of Information Science and Technology 42: 425-495.
51. Crubézy M, O'Connor M, Pincus Z, Musen MA, Buckeridge DL (2005) Ontology-centered syndromic surveillance for bioterrorism. IEEE Intelligent Systems 20: 26-35.
52. 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.
53. Hutwagner L, Thompson W, Seeman GM, Treadwell T (2003) The bioterrorism preparedness and response early aberration reporting system (EARS). J Urban Health 80: i89-i96.
54. Uhde KB (2003) Bioterrorism syndromic surveillance: A dual-use approach with direct application to the detection of infectious disease outbreaks: University of South Florida.
55. Velsko S, Bates TA (2016) Conceptual architecture for national biosurveillance: Moving beyond situational awareness to enable digital detection of emerging threats. Health Secur 14: 189-201.

56. Meyer N, Menamin JMc, Robertson C, Donaghy M, Allardice G, et al. (2008) A multi-data source surveillance system to detect a bioterrorism attack during the G8 Summit in Scotland. Epidemiol Infect 136: 876-885.

57. Mandl KD, Overhage JM, Wagner MM, Lober WB, Sebastiani P, et al.(2004) Implementing syndromic surveillance: A practical guide informed by the early experience. J Am Med Infor Assoc 11: 141-150.

58. 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 ACM.

59. Lombardo JS, Burkom H, Pavlin J (2004) ESSENCE II and the framework for evaluating syndromic surveillance systems. MMVR 53: 159-165.

60. Lombardo J, Burkom H, Elbert E, Magruder S, Lewis SH, et al. (2003) A systems overview of the electronic surveillance system for the early notification of community-based epidemics (ESSENCE II). J Urban Health 80: i32-i42.

61. Li CS, Aggarwal C, Campbell M, Chang Y, Hill M, et al. (2004) Site-based biosurveillance. MMWR Morb Mortal Wkly Rep 53: 249.

62. 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. MMWR 53: 32-39.

63. 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: e62749.

64. 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. J Urban Health 80: i25-i31.

65. Wang S, Han H, Ki M (2005) Development of a comprehensive bioterrorism information system in Korea. Prehospital and Disaster Medicine 97.

66. Lober WB, Karras BT, Wagner MM, Overhage JM, Davidson AJ, et al. (2002) Roundtable on bioterrorism detection. J Am Med Inform Assoc 9: 105-115.

67. Lim DV, Simpson JM, Kearns EA, Kramer MF (2005) Current and developing technologies for monitoring agents of bioterrorism and biowarfare. Clin microbiol Rev 18: 583-607.

68. Radke SM, Alocilja EC (2005) A microfabricated biosensor for detecting foodborne bioterrorism agents. IEEE Sensors Journal 5: 744-750.

69. 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 Proc BioMed Central 3: s3.

70. Chretien JP, Blazes D, Mundaca C, Glass J, Happel Lewis S, et al. (2007) Surveillance for emerging infection epidemics in developing countries: EWORS and Alerta DISAMAR. Disease Surveillance 369-396.

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

72. 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. J Med Internet Res 13: e85.

73. Stallings W, Brown L (2012) Computer Security Principles and Practice. 2nd edn. PEARSON (ed).

74. Workgroup P (2000) Biological and chemical terrorism: Strategic plan for preparedness and response. MMWR 49: 1-14.

75. Koplan J (2001) CDC's strategic plan for bioterrorism preparedness and response. Public Health Rep 2: 9-16.

76. Binder P, Attre O, Boutin JP, Cavallo JD, Debord T, et al. (2003) Medical management of biological warfare and bioterrorism: Place of the immunoprevention and the immunotherapy. Comp Immunol Microbiol Infect Dis 26: 401-421.

77. Purtle J, Field RI, Hipper T, Nash-Arott J, Chernak E, et al. (2018) The impact of law on syndromic disease surveillance implementation. J Public Health Manag Pract 24: 9-17.

78. Morris SA, Kellogg R, Perry S, Meyer RF, Bray DA, et al. (2003) Detecting Bio-Threat Agents: The Laboratory Response Network.

79. Buckeridge DL, Burkom H, Campbell M, Hogan WR, Moore AW (2005) J Biomed Inform 38: 99-113.