Advancing Bio Detection with Biosensors and Nanotechnology for Rapid Interagency Response

by Habi Mojidi

Any effective bio surveillance system must be able to detect the presence of biological agents with sufficient speed and adequate attribution to facilitate an effective interagency response and thwart a crisis. The U.S. currently employs a detection system called BioWatch designed to collect environmental samples in public spaces throughout the country.[1] BioWatch is slow and lacks the ability to provide comprehensive attribution information, which leaves the U.S. population vulnerable to deadly biological agents and contributes to the nation's overall biological unpreparedness and vulnerability. In this article, I argue that the interagency must leverage new technologies, such as nano-biosensors, which bind to and analyze potentially harmful biological materials almost instantaneously, to create a secure, real-time notification system capable of attribution. All of this will enable a rapid and effective interagency response.

Background: Existing Bio defenses

The U.S. currently relies on BioWatch—a program "owned" by the Department of Homeland Security (DHS)—as its first line of detection of deadly pathogens/viruses/bacteria. BioWatch has been defending the U.S. from a biological attack for more than 15 years.[2] The biological surveillance system is actually an improvement on previous response efforts, when the interagency lacked any means of obtaining knowledge of an outbreak or presence of a biological agent. This surveillance system uses more than 600 sensors in over 30 major cities across the U.S., including throughout city transport systems (see Figure 1).[3] The samples are obtained by monitoring the quality of the air via a specialized filter. The filter is tested for pathogens using Polymerase Chain Reaction, which directly identifies pathogenic genes from a list of predetermined highly infectious diseases.[4] The results of the monitoring performed by the Environmental Protection Agency are given, as necessary, to the Centers for Disease Control and Prevention for analysis and finally passed along to the Federal Bureau of Investigation as the lead agency for law enforcement.[5]

U.S. Army Major Habi Mojidi is the Hospital Headquarters Administrator at the United States Army Reserve Center, Fort Meade MD. She holds a M.S. degree in Biotechnology, a MBA degree, and received a M.S. degree in WMD Studies as a National Defense University Countering WMD Graduate Fellow.

Figure 1: BioWatch Surveillance collector[6]

BioWatch is a slow and cumbersome system, and the detection process is far from automated. Not only do individuals have to manually collect air samples from collection containers, laboratory scientists must then perform assays (genetic tests of a biological agent) on these samples to confirm a positive result. If the sample yields a positive result, this result would not be identified immediately: It can take from days to weeks before the U.S government can coordinate an effective interagency response to bioterror events through the unsecured BioWatch portal.[7]

Take, for example, the case of a positive result of tularemia in the city of Houston in 2003.[8] Three days of waiting for a final positive confirmation of preliminary results produced understandably great angst on the part of the city administration and public health officials. While follow-up tests concluded that there was no ongoing biological attack, the image of thousands of individuals that would have remained at risk over the 72 hours while the test were being confirmed is extremely unnerving.

BioWatch can only identify who might be infected in a specific area after a large number of people have passed through the subject area over time. This hardly constitutes a real-time warning of a biological attack. Figure 2 (page 42) illustrates how current biological surveillance tools support diagnosticians and public health officials from the early data collection through the later response phases in a "response pyramid."

BioWatch falls under the first stage—data collection. Data from BioWatch sensors are combined with additional sources of outbreak information at later stages of the pyramid.[9] After the collection and central storage phases, data must be analyzed using algorithms to screen for veracity and robustness in the data repository.[10] Only then can analysts can conduct attribution analysis and identify trends and outbreaks using timing and location data.[11] Then it is possible to develop a picture of the biological incident. This analysis takes precious time away from fighting

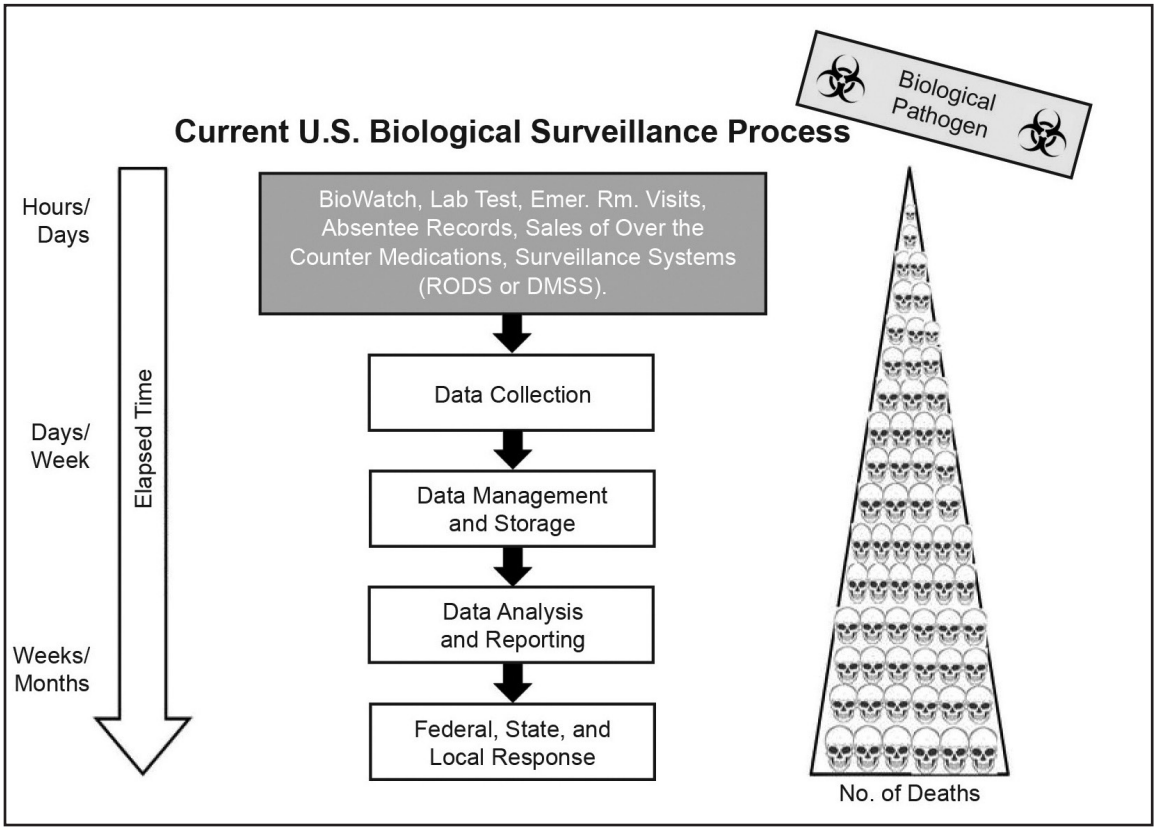

Figure 2: BioWatch Surveillance "Pyramid"

the disease in its early stages of outbreak and hinders a rapid, efficient, interagency response.

Not only is BioWatch part of an incredibly slow processing stream, it is also quite vulnerable.[12] The BioWatch portal is hosted electronically on an .org rather than a .gov domain.[13] The .org domain does not have the same security requirements as the .gov domain, making the data an easier target for potential hackers.[14] Hacking into the BioWatch portal could provide access to the location of the sensors, or sensors could be disabled before an attack, leaving the population vulnerable.[15]

Although current surveillance tools and systems constitute the early event detection of a biological disease, the term "early" is vague. There are many modeling tools to predict the spread of chemicals or nuclear plumes, accurately predicting the spread of biological agents is more difficult. Using the Hazard Prediction and Assessment Capability program, a Department of Defense (DoD) modeling tool to predict the path of a biological pathogen in the direction of the prevailing winds, in conjunction with nano-biosensors can predict the most likely areas where the infections would spread very rapidly. Failing to rapidly identify biological weapons leaves U. S. citizens helpless to a biological attack. If an enemy creates a biological weapon with the intent to kill, the weapon would likely have increased morbidity and enhanced evasive properties.[16]

New Technologies: Leveraging Nanotechnology

Advanced notice from a sensing device that could provide healthcare providers and experts the time and relevant information to save lives is an essential part of any effective biological response plan. Advances now being made in

nano-biosensor technology offer the potential to allow healthcare providers to develop a course of treatment to facilitate a full interagency response to a biological weapons attack within acceptable time parameters. In practical terms, nanotechnology aimed at bio surveillance could take the form of the subcutaneous injection of biosensors. Current medical research allows nanoparticle design to be smaller and more sensitive than conventional drugs.[17] Nanotechnology can be carriers for targeted drug delivery or therapeutic treatments.[18] Current methods of detection do not have the ability to identify novel biological weapons created to evade detection; however, developing specific nano-biosensors to identify biological weapons could provide a remarkable advantage to the U.S. during a catastrophic biological event. A nano-biosensor network would allow for rapid detection in determining the type and spread of a pathogenic organism before infected individuals present with symptoms.

Nanotechnology, precisely nano-biosensors, could potentially identify subtle changes between naturally-occurring micro-organisms and biological weapons. Whether a designer biological weapon or a deadly, naturally-occurring microbe causes a pandemic, most infectious agents trigger an immune response from the infected organism. Based on an intelligent design, nano-biosensors could use the interaction with the immune system to identify specific genetic or molecular signatures and determine which are probably naturally-occurring and which would be a potential biological weapon. It is possible that nano-biosensors residing in infected individuals could provide this early detection—essentially the "canary in the coal mine" for clinicians at the forefront of a potential catastrophic biological attack. This type of technology is expected to become available within the next decade. Currently, the DoD is investing in nanotechnology and is becoming increasingly more reliant on nanomaterials in general. Just as the internet progressed from the strict military application to a daily tool used by almost every person on the planet, nanotechnology could become similarly ubiquitous.

Current methods and technologies used to detect a biological agent are actually far from early warning sensors.

Current methods and technologies used to detect a biological agent are actually far from early warning sensors. Leveraging new technology can only improve upon the infection-detection lag and allow for an improved and coordinated interagency response. Nano-technology contains the ability to send a short radio signal once the biosensor detects a targeted biological agent.[19] An electrochemical biosensor designed to identify specific antigens, such as the methods used in immunohistochemistry, would be an improvement. An example of a currently available product that represents an advance along the lines described above is the FreeStyle Libre.™ The device is an implantable, continuous, glucose-monitoring capability that is factory-calibrated.[20] This calibration occurs as part of the sensor manufacturing process under specific laboratory guidelines.[21] As more wearable medical devices become commonplace, it will soon become possible for use in nanotechnology to both cure diseases and quickly detect the spread of diseases, thus shortening the timeline for the detection of potentially large-scale biological outbreaks.[22] This is so because nano-biosensors are able to monitor physiological differences in individuals in real time, Nanotechnology also contains the ability to send a radio signal once the biosensor detects a targeted biological agent.

Biosensors are an analytical tool that can detect a signal from an analyte (i.e., a substance whose chemical constituents are being identified

and measured). An analyte for a biological sensor can be any aspect that researchers have determined to be a viable substrate to bind to an enzyme, antibody, cell receptor, or a microorganism. Once the biological receptor recognizes the analyte, a nano-device can act as a signal transducer.[23] A signal transducer translates the physiochemical reaction that occurs because of the release of heat, light, change in mass, or pH.[24] These forms of energy can be captured by nanotechnology, allowing for rapid, near real-time identification of the small change in the local environment. This small but measurable change signal can initiate a response to a biological event within minutes or hours.[25] Nano-biosensors designed to interact with antigens or immunoglobulins decrease the response time, providing public health officials valuable time to respond to a potential biological threat. This defense against biological agents calls for rapid identification and communication of a positive signal, without the need for human laboratory analysis.

Using individuals as "canaries" would allow the interagency to rapidly identify infected individuals and the time and location of the disease outbreak.

Using these newer sensors and hosting their data on a secure platform could make for substantial improvements over the existing system. By monitoring select individuals in various geographic areas and streamlining data collection and integration across the interagency, these nano-biosensors could facilitate the automated appearance of data on a properly-secured system in real time. Not only do nano-biosensors shorten the duration of the response period, they can provide higher-resolution information. When there is a disease outbreak, epidemiologists must make assumptions regarding the dates and locations when the infection might have occurred using data that has been analyzed. Using nano-biosensors, however, epidemiologists can access real-time information about changes in the host's immune system that would signal the body is fighting an infection.

Real-time data is particularly helpful because infection resulting from a weaponized version of a pathogen progresses faster and in a different pattern than that of naturally-occurring disease. Using individuals as "canaries" would allow the interagency to rapidly identify infected individuals and the time and location of the disease outbreak. Thus, nano-biosensors can decease time required to identify a potential outbreak from days to hours—potentially saving many lives and preventing disease outbreaks from reaching epidemic proportion.

The use of nanotechnology would provide other societal benefits as well. Uncertainty about disease progression and the unknowns regarding the origins of the disease can also wreak havoc on hospitals and the economy, due to fear and panic. People will fear going to social gatherings or even to work if they are unsure if the outbreak is contained. With the use of nanotechnology, vital information becomes available in hours instead of days or weeks, thus boosting confidence in the ability of government to manage the situation.

Nanotechnology: Facilitating Interagency Response

In the event of an intentional attack, interagency cooperation is paramount in preventing others from getting infected, while at the same time attributing the outbreak. Current bio-surveillance tools provide only historical data on disease transmission and the efforts of multiple government agencies, including those involved in and overseeing healthcare, food, and transportation. In April 2018, DHS acknowledged that technology upgrades are necessary for BioWatch to better address a wider range of bioterrorism threats, provide real-time data, and enhance information-sharing among

operators at the federal, state, and local levels.[26] While the specifics for the upgrades have not been released, this new approach to bio-surveillance at least moves toward the goal of real-time data in a specific area to provide better predictions regarding the spread of a pathogen over space and time.[27]

An effective response against a biological attack or epidemic must involve a coordinated interagency effort. A pre-arranged interagency response expedites resource requirements when responding to a biological incident, while minimizing the response time and enhancing the efficacy of a response effort provides a greater opportunity to save lives.

Nano-Biosensors: Deterring Adversaries, Saving Lives

Developing a biological weapon simply requires an actor with the knowledge, desire, and skillset to create a biological weapon that the human body has not evolved to combat. Since there is no way to ensure total elimination of biological weapons, the Biological and Toxin Weapons Convention (BWC) was created with the hope of prohibiting the development, production, and stockpiling of bacteria and toxins as weapon.[28] Unfortunately, its existence does not guarantee compliance with the prohibitions. Moreover, while the BWC binds states, it has no way to guarantee that individuals will not engage in efforts to produce bioweapons. Hence, an effective means of bio-detection remains essential to protect U.S. citizens from a biological weapon.[29] Continued research regarding these systems and technologies will make nano-biosensors as common as today's computers, decreasing the cost to maintain these systems and making this method of surveillance more cost effective than current methods.

The U.S. requires innovation to maintain a strong defensive posture against individuals that would think to use biological weapons on U.S. soil. Nanotechnology can assist in maintaining a strong defensive posture by evading or outsmarting our enemies. Enemies of the U.S. would have to be able to determine, a) what the biosensors could identify, b) how quickly the interagency could mount a response, and c) whether there is the possibility for attribution. The efficacy of bio-surveillance in the U.S. requires policies that use organizations and technology to reduce the risk of a biological warfare agent. Bio-surveillance policies that focus on interagency cooperation and employ next-generation bio-sensors and nanotechnology could mitigate the potential threat of biological weapons.

Bio-surveillance policies that focus on interagency cooperation and employ next-generation bio-sensors and nanotechnology could mitigate the potential threat of biological weapons.

The numerous programs and tools the U.S. and other nations have invested in cost billions of dollars, yet most come short of a real-time solution. A well-constructed biological agent could kill thousands of people and cripple healthcare critical infrastructure before the agent is identified. Identifying deadly diseases that cause micro-level changes in a patient's biochemistry can alert doctors, scientists, law enforcement, and government officials of a potential outbreak before the first patient becomes symptomatic.

Investing in a comprehensive real-time solution that will provide rapid information to public health officials will save lives, reduce the cost of treatment, and provide a more comprehensive program that is easier to maintain over time. As infected individuals have time to drive or fly out of the affected area, the need to engage all agencies of the government becomes critical. Tracking and treating infected individuals becomes not only a matter of

national security, but also a domestic crisis with the potential loss of millions of lives.

Several countries developing nano-weapons, such as insect-like lethal robots, could disseminate toxins or a harmful virus. The U.S., Russia, and China have invested billions on nano-weapons research. Research to identify biological agents can deter the attacks by biological weapons if an aggressor knows the attack will be unsuccessful. While science fiction today, the advancement of nanotechnology in the coming years continues to increase this threat in the twenty-first century in the way that nuclear weapons did in the twentieth century.[30]

Most technologies developed for good can also be used for nefarious purposes, and nanotechnology is no exception.

New Technologies: Molecular Biodefense

The Defense Advanced Research Projects Agency (DARPA) is also leveraging new technologies to improve bio-surveillance and defend the homeland against a biological outbreak with programs called Prometheus and the Pandemic Prevention Platform (P3) program.[31] Though not yet ready for implementation, the Prometheus program aims to determine whether an individual is contagious before he or she exhibits symptoms of illness.[32] Specifically, DARPA is working to develop a molecular test that uses an individual's own immune responses and biological markers that arise after infection to determine if an individual will contract and become contagious within 24 hours after exposure to an infectious agent.[33]

The Pandemic Prevention Platform (P3) program is seeking to enable the development of automatic immunity. The concept uses nucleic acids to produce treatments "against any known or previously unknown infectious threat within 60 days of identification,"[34] building on the Autonomous Diagnostics to Enable Prevention and Therapeutics program, which provides the body with instructions on how to immediately begin producing protective antibodies against a given threat.[35] This program primarily supports military readiness in the case of use of biological weapons on the battlefield, but it can also prevent the spread of any disease in the homeland.[36] Both of these DARPA programs are designed to identify the contagion in an individual before the infection can spread within a population.

Conclusion

Most technologies developed for good can also be used for nefarious purposes, and nanotechnology is no exception. The positive applications of nano-technology in conjunction with bio-sensors could help avoid mass destruction by those who might use the new technologies to target individuals or specific groups. While harnessing the protective power of these technologies, the interagency must also take action to develop tools to prevent the public health catastrophes that could arise. Although reluctance to use nano-biosensors may stem from the novelty of the technology and a hesitation to make a change in the how the U.S. government currently monitors biological agents in the environment, the interagency must consider that there are currently no systems that can conduct biological surveillance and simultaneously perform analysis, and that the lag time between obtaining a sample and analyzing the sample leaves a vulnerable population unprotected and at risk of exposure to a biological weapon.

Biological sensors that work autonomously with nanotechnology to identify agents and warn public health officials secures the U.S. homeland against designed biological agents and naturally-occurring outbreaks. Biological nano-sensors conducting biological surveillance will provide invaluable lead time to mount an effective, well-orchestrated, interagency response against

a biological agent such as anthrax or Ebola. Many agencies monitor different kinds and networks. For biological sensors, many signals can be monitored to notify the appropriate agencies at the first sign of an outbreak.

The U.S. conducts many interagency preparedness exercises to respond to outbreaks once detected. Nevertheless, detection of biological agents does not yet occur in real-time, leaving many populated areas outside of the 30 cities monitored by BioWatch at risk. While other mechanisms such as self-reporting of symptoms to pharmacies and hospital emergency rooms assist with monitoring illnesses in the country, nano-biosensors with an integrated interagency portal designed to identify and provide healthcare practitioners in almost real-time to respond to any outbreak will be crucial to future U.S. national security. ***IAJ***

The views expressed in this article are those of the authors and are not an official policy or position of the National Defense University, the Department of Defense or the U.S. government.

NOTES

1 The BioWatch Program, December 7, 2017, https://www.dhs.gov/biowatch-program, accessed on December 10, 2017.

2 Ibid.

3 Ibid.

4 Congressional Research Service Report, "The BioWatch Program: Detection of Bioterrorism," No. RL 3215, November 19, 2003, accessed on October 22, 2017.

5 Ibid.

6 Brandon Mercer, "That Mysterious Homeland Security Box Plugged into an SF Utility Pole Is a. . .", January 28, 2016, http://www.sfgate.com/superbowl/article/That-mysterious-Homeland-Security-box-plugged-6790510.php, accessed on April 9, 2019.

7 The BioWatch Program, 2017.

8 Ibid.

9 Ibid.

10 Congressional Research Service Report.

11 Ibid.

12 Patrick Tucker, "The Government's Bioterror-Response Website May Be Leaking Sensitive Data," December 13, 2018, https://www.defenseone.com/technology/2018/12/governments-bioterror-response-website-may-be-leaking-sensitive-data/153518/, accessed on December 16, 2018.

13 Ibid.

14 Ibid.

15 Ibid.

16 Kelly J. Henning, "Overview of Syndromic Surveillance What is Syndromic Surveillance?" https://www.cdc.gov/mmwr/preview/mmwrhtml/su5301a3.htm, accessed on April 9, 2019.

17 The University of Wisconsin, "Nanotechnology in the Military," http://ice.chem.wisc.edu/Small%20Science/From_Small_Science_Comes_Big_Decisions/Choices_files/Military.pdf, accessed on December 10, 2017.

18 Ibid.

19 Nanowerk, March 15, 2013, https://www.nanowerk.com/nanotechnology-news/newsid=39401.php, accessed on January 29, 2019.

20 Udo Hoss and Erwin Satrya Budiman, "Factory-Calibrated Continuous Glucose Sensors: The Science Behind the Technology," May 2017, https://www.ncbi.nlm.nih.gov /pmc/articles/PMC5444502, accessed on January 29, 2019.

21 Ibid.

22 Ibid.

23 News Medical Life Science, "What is a Biosensor?" https://www.news-medical.net/health/What-are-Biosensors.aspx, accessed on February 15, 2018.

24 Ibid.

25 Ibid.

26 Kim Riley, "End of BioWatch Looms Near, Blue Ribbon Study Panel Members Learn," Homeland Preparedness News, November 20, 2018, https://homelandprepnews.com/stories /31415-end-of-biowatch-looms-near-blue-ribbon-study-panel-members-learn, accessed on April 9, 2019.

27 Ibid.

28 United Nations Office for Disarmament Affairs, "Biological Weapons," https://www.un.org/disarmament/wmd/bio, accessed on December10, 2017.

29 Ibid.

30 Jeff Daniels, "Mini-Nukes and Mosquito-Like Robot Weapons Being Primed for Future Warfare," CNBC: Defense, March 17, 2017, http://www.cnbc.com/2017/03/17/mini-nukes-and-inspect-bot-weapons-being-primed-for-future-warfare.html, accessed on December 10, 2017.

31 Matthew Hepburn, "Prometheus," Defense Advanced Research Projects Agency, https://www.darpa.mil/program/prometheus, accessed on December 11, 2018.

32 Ibid.

33 Ibid.

34 Matthew Hepburn, Pandemic Prevention Plan (P3), Defense Advanced Research Projects Agency, https://www.darpa.mil/program/pandemic-prevention-platform, accessed on December 11, 2018.

35 Ibid.

36 Ibid.