Fall 2016

Concurrent Biological, Electromagnetic Pulse, And Cyber Attacks - A Challenge To The Interagency Response

Patricia Rohrbeck

CONCURRENT BIOLOGICAL, ELECTROMAGNETIC PULSE, AND CYBER ATTACKS - A CHALLENGE TO THE INTERAGENCY RESPONSE

A Masters Thesis

Presented to

The Graduate College of

Missouri State University

In Partial Fulfillment

Of the Requirements for the Degree

Master of Science, Defense and Strategic Studies

By

Patricia Rohrbeck

December 2016

CONCURRENT BIOLOGICAL, ELECTROMAGNETIC PULSE, AND CYBER ATTACKS – A CHALLENGE TO THE INTERAGENCY RESPONSE

Defense and Strategic Studies

Missouri State University, December 2016

Master of Science

Patricia Rohrbeck

ABSTRACT

The U.S. including its military depends on an electrical grid and electricity-based critical infrastructure. An electromagnetic pulse (EMP) and cyber attack can disable not just a significant portion of the electrical grid and critical infrastructure, but also the network-centric military response to such an attack. There is a large range of actors that might attempt EMP attacks against the U.S.. Health surveillance systems are network-centric, and if mass destruction is the goal of an adversary, launching a biological attack concurrently with EMP and cyber attacks may achieve this goal. Current agency response plans focus on one WMD attack at a time but combined attacks without emergency management plans may compromise a timely response. An EMP and cyber attack could amplify the effects of a biological attack because the loss of the electrical grid and electricity-based critical infrastructure could disable detection and response efforts as well as disrupt interagency efforts to coordinate a medical response. EMP is often perceived as science fiction because the immediate effect does not result in loss of life, but the cascading failures of critical infrastructure will affect civilian and military capabilities to support survival and recovery. Key steps to mitigate the catastrophic effects of an EMP attack should be taken and include: prevent an attack in the first place, prepare so personnel can respond after an attack, protect the critical infrastructure to limit the impact, and recover after an attack to restore power and critical infrastructure.

KEYWORDS: WMD, biological warfare agent, EMP, cyber attack, emergency response

This abstract is approved as to form and content

_____

John Mark Mattox, PhD
Chairperson, Advisory Committee
Missouri State University

CONCURRENT BIOLOGICAL, ELECTROMAGNETIC PULSE, AND CYBER ATTACKS – A CHALLENGE TO THE INTERAGENCY RESPONSE

By

Patricia Rohrbeck

A Masters Thesis
Submitted to the Graduate College
Of Missouri State University
In Partial Fulfillment of the Requirements
For the Degree Master of Science, Defense and Strategic Studies

December 2016

Approved:

_____
John Mark Mattox, PhD

_____
John Rose, PhD

_____
Andrei Shoumikhin, PhD

_____
Julie Masterson, PhD: Dean, Graduate College

ACKNOWLEDGEMENTS

I would like to whole-heartedly thank the following individuals for their support, guidance, and mentorship during the course of my graduate studies:

Dr. John Mark Mattox
Dr. John Rose
Dr. Andrei Shoumikhin

TABLE OF CONTENTS

Introduction.....1

Characteristics of Biological, EMP and Cyber Attack..…….…….. 5
Biological Warfare Agents…….…….. 6
Biosensors, Disease Surveillance Systems, and Health Communication…. 10
Electromagnetic Pulse (EMP) and Cyber Attack…….…… 15

Biodefense—Sensors and Federal Surveillance and Supply Programs…….24
BioWatch……... 25
BioSense…… 27
Strategic National Stockpile (SNS)……... 30
National Reference Laboratories (NRL)……34

Interagency Coordination of a Public Health Response……...……. 38
Department of Homeland Security (DHS)…… 39
Federal Emergency Management Agency (FEMA)…….. 41
Department of Health and Human Services (HHS)……...42
Office of the Assistant Secretary for Preparedness and Response (ASPR).. 43
Centers for Disease Control and Prevention (CDC)……..45
U.S. Food and Drug Administration (FDA)…….. 46
U.S. Northern Command (NORTHCOM)……47
Federal Bureau of Investigation (FBI)…….. 48

Challenges During a Response to a Biological Attack After EMP……... 51
Interagency Coordination……...51
Public Health Response…….……...……. 54
Communicating with the Public…….59

Current Issues with the Public Health Response…….…….……..65
Threat Assessment.…… 65
Preparing for Concurrent WMD Attacks.……...…..……..... 69
Education and Training……..72
Protection and Recovery of Critical Infrastructure……..…….....75

Conclusion and Recommendations…….…..…….80

References…….....86

INTRODUCTION

The U.S. including its military depends on an electrical grid and electricity-based critical infrastructure such as telecommunications, transportation, banking and finance, petroleum and natural gas, food and water, public health and health care, and security. In addition, the U.S. Armed Forces rely on information technology and computer networks to manage its weapons platforms, sensor systems, and command and control centers. An electromagnetic pulse (EMP) and cyber attack can disable not just a significant portion of the electrical grid and critical infrastructure, but also the network-centric military response to such an attack. A high altitude nuclear detonation, radiofrequency weapon, or solar flare can cause an EMP. The range of actors that might attempt EMP attacks against the U.S. is increasing and may include countries with nuclear weapons such as Russia and China, rogue states with limited conventional and nuclear military capabilities such as North Korea, as well as terrorist groups throughout the world that seek to inflict catastrophic damage on America. The U.S. military has hardened some of its strategic defense systems, such as missile silos, but not all systems are protected and little effort has been made to protect the civilian infrastructure. Even if hardened, systems can be disrupted by a cyber attack in preparation for an EMP. Health surveillance systems in the U.S. are network-centric, and if mass destruction is the goal of an adversary, launching a biological attack concurrently with EMP and cyber attacks may achieve this goal. Current agency preparedness and response plans focus on one WMD attack mode at a time so combined attacks without emergency management plans may present a vulnerability. An EMP and cyber attack could amplify the effects of a biological attack because the loss of

the electrical grid and electricity-based critical infrastructure could disable detection and response efforts as well as disrupt interagency efforts to coordinate a medical response.

Detection of biological agents could be disabled after an EMP and cyber attack because electronic healthcare surveillance systems would be no longer operational and could no longer process and exchange information among agencies. Laboratories would no longer receive and be able to process suspected specimens, which could not identify potentially hazardous biological agents. Telecommunication has a crucial role in health surveillance because it makes receiving and analyzing of health encounter data via standard, cellular phones, and computers networks possible. Lack of communication from one healthcare facility to another significantly hinders timely detection and response efforts. Without a timely response, the spread of disease in a population may not be contained during its early stages and could lead to an outbreaks and epidemics. Without the ability to detect biological agents, public health officials cannot initiate timely treatment and preventive measures, which could result in higher than expected morbidity and mortality.

Response efforts may also be disrupted because resources needed to treat medical emergencies cannot be delivered or need to be diverted to fill other gaps. With the breakdown of the entire transportation system in EMP-affected areas, sending laboratory specimens or distributing medical supplies may not be a priority as compared to food and water deliveries. This may disrupt how public health officials assess the ongoing health threat and how treatment has to be prioritized. Additionally, medical supplies and pharmaceuticals may not be delivered in the same dose and format requiring adjustments

before administering. As a result, disruption of resource supply chains may cause a delay in patient treatment and care.

Response efforts may also be disrupted because interagency efforts could not be coordinated due to the lack of communication. For emergencies across state lines, support from federal agencies such as the Department of Homeland Security (DHS), Health and Human Services (HHS), and the Federal Emergency Management Agency (FEMA) is usually requested. Yet without the ability to communicate and travel, federal support may be delayed, which requires local agencies to lead the initial response. Local public health and health care personnel may lack the necessary training to coordinate a medical response to a biological agent. As a result, response efforts may be executed inefficiently. Vertical coordination may cause issues with local response efforts, which makes communication imperative to prevent duplication of efforts.

One could argue that after an EMP and cyber attack adversaries may not see the need for a biological attack because lack of electricity, water and food supplies alone will result in significant loss of lives. Yet, in order to recover from these attacks and to restore electricity and normal operation of systems, there need to be healthy people who can contribute to the recovery process. Additionally, one could argue that after a major blackout, adversaries may have a difficult time disbursing biological agents so that such an event may not occur. At the same time and in order to cause high casualties, it may be more plausible that an agent could be distributed immediately prior to an EMP and cyber attack without individuals realizing that a biological attack had occurred. This would allow a disease to spread within a population undetected and untreated until a major outbreak has occurred that may not be contained due to limited medical supplies.

Disruption of the electrical grid, electricity-based infrastructure, and network-centric systems as a result of an EMP and cyber attack and concurrent with a biological attack may cause significantly more destruction and loss of lives than any of these WMD by themselves. EMP is often perceived as science fiction, and the immediate effect usually does not result in loss of life, but the unprecedented cascading failures of critical infrastructure will affect civilian and military capabilities to support survival and will compromise recovery. Comprehensive threat assessment and scenario planning for EMP and cyber attacks remain underdeveloped and so does a combined attack with a biological agent. As a result, adversaries could exploit this vulnerability so that interagency and multi-disciplinary efforts are needed to defend against these concurrent WMDs.

CHARACTERISTICS OF BIOLOGICAL, EMP AND CYBER ATTACKS

The biological threat is real and growing. A threat consists of intent and capability and even though many state actors and terrorist organizations have expressed intent in the past, many have expanded their capabilities and developed or acquired biological agents in recent years. At the same time, not every biological agent capable of causing infectious diseases and outbreaks can be transformed into a biological weapon. Biological agents are diverse in regards to biological characteristics, disbursal, the number of people they can affect as well as the rate of survival. To distinguish between infectious agent and potential biological weapon, agencies need to be able to electronically monitor population health. Identification of clusters or outbreaks of diseases in a timely manner is important to coordinate effective interventions. As a result, prevention of contagious diseases with high morbidity and mortality presumes a fully operational electrical grid that supports disease surveillance systems. Individuals that were exposed to biological agents can easily be identified through comprehensive surveillance efforts, and vaccination or medical treatment will contain further spread of disease. An EMP and cyber attack could amplify the effects of exposure to a biological agent by disabling electronic surveillance and communication systems. This would limit the ability of public health officials and health care staff to identify unusual disease occurrences in the population. Unmonitored disease progression and transmission would result in higher than expected morbidity and mortality.

Biological Warfare Agents

Early detection and identification of unusual symptoms or disease spikes is crucial to prevent spread of infections with biological agents. Naturally occurring biological agents such as virus, bacteria, fungi, protozoa or toxins can devastate livestock, crops, and dairy or produce supplies, harming millions of people and producing a debilitating effect on the U.S. economy.[1] These natural biological agents can be weaponized and used during a WMD event. The preparedness against biological warfare agents (BWA) needs complete knowledge about the disease, better research and training facilities, diagnostic facilities, and improved public health systems.[2] Biological attacks require only release of a small quantity of viable material since agents are capable of self-replication to spread disease throughout a population.[3] BWA pose a challenge to public health because they can cause a large number of causalities for many symptoms and will therefore be difficult to detect.[4] Additionally, the effects of these agents are not always instantaneous and require few hours to weeks before symptoms appear in the affected population.[5] As a result, ongoing health surveillance of the population is necessary to detect unusual symptoms during early onset of disease to prevent large-scale mortality and reduce morbidity.

---

[1] Hudson Institute," A National Blueprint For Biodefense: Leadership and Major Reform
[2] Thavaselvam D, Vijayaraghavan R., Biological warfare agents, *Journal of Pharmacy &BioAllied Sciences*, Jul-Sep 2010, 2(3): 179-188.
[3] Hudson Institute," A National Blueprint For Biodefense: Leadership and Major Reform Needed to Optimize Efforts," Bipartisan Report of the Blue Ribbon Study Panel on Biodefense, Oct 2015, p. 20, at http://hudson.org/research/11824-a-national-blueprint-for-biodefense-leadership-and-major-reform-needed-to-optimize-efforts (Nov 1, 2015).
[4] Ibid.
[5] Ibid.

The Centers for Disease Control and Prevention (CDC) created a BWA classification based on public health impact, dissemination potential, public perception, and public health preparedness requirements rather than biological characteristic to assist public health officials with creating targeted response efforts.[6] The categories rang from most dangerous (Category A) to emerging infections (Category C), and healthcare providers should be alert to illness patterns and diagnostic clues of these agents.[7] Some of the category A agents of concern are plague, anthrax, and smallpox because they were associated with intentional use in the past or could cause high mortality if no available treatment options were used. The category A agents pose unique health surveillance challenges due to their distinct biological characteristics and require targeted response efforts cases are identified in the population.

Plague is a curable infectious disease caused by the bacteria *Yersinia pestis*, which, without antibiotic treatment, can cause a 50 percent mortality rate.[8] As a BWA, the plague bacteria can be disbursed and inhaled as an aerosol. If inhaled, the bacteria can cause pneumonic plague, which is highly contagious and can spread from person-to-person by airborne droplets through sneezing or coughing. Clinical signs will show after one to six days after exposure and include common cold symptoms such as fever, swollen lymph nodes, chills, cough (with or without bloody sputum), and pneumonia.[9] Since *Yersinia pestis* is naturally occurring, it could easily be isolated and grown in laboratories

---

[6] Centers for Disease Control and Prevention (CDC), Recognition of Illness Associated with the Intentional Release of a Biologic Agent, *Morbidity and Mortality Weekly Report*, Oct 19, 2001, 50(41): 893-7.
[7] Ibid.
[8] Thavaselvam D, Vijayaraghavan R., Biological warfare agents, *Journal of Pharmacy &BioAllied Sciences*, Jul-Sep 2010, 2(3): 179-188.
[9] Ibid.

and then be weaponized. Even though pneumonic plague is a rare naturally occurring event, the symptoms mimic common cold and flu symptoms, so that cases may not immediately seek medical care. As a result, healthcare providers may not identify the disease in its early stages. In this case, syndromic surveillance may be helpful in identifying unusual clusters of cold symptoms that would warrant further investigation by public health officials. Plague can easily be treated if identified early and poses less of a health threat, but if surveillance system do not pick up potential cases and individuals are left untreated, the mortality rate can be higher than expected.

Smallpox (variola virus) has no proven treatment except for supportive medical care, which makes early detection and isolation of cases important to prevent further spread of disease among the population. Vaccination to prevent disease is the most appropriate course of action, yet the vaccine is no longer administered routinely to the general population in the U.S. since the mid-70s. With waning immunity among those who previously received the vaccine and the large number of unvaccinated individuals in today's population, the case fatality rate could be as high as 30 percent; survivors are often left with permanent scares or blindness.[10] The incubation period averages 12 days during which a case experiences headaches and fever only; the pus-filled vesicles throughout the body, indicative of smallpox infection, only show after the 12-day period.[11] During the incubation period, cases are highly infectious and can spread the smallpox virus through airborne droplets. The deliberate release of smallpox will be difficult to detect until individuals develop lesions and seek medical care. As a result, the

[10] Thavaselvam D, Vijayaraghavan R., Biological warfare agents, *Journal of Pharmacy &BioAllied Sciences*, Jul-Sep 2010, 2(3): 179-188.
[11] Ibid.

main priority to contain further spread of disease will be tracking, isolating, and monitoring of individuals who have been in close contact with a case. This will require close monitoring of the affected population.

Anthrax, a spore-forming bacterium (Bacillus anthracis), infects humans through direct contact (ingestion, inhalation, cutaneous, injection) with the spores and is not transmitted from person-to-person, but the spores can be easily disbursed among a population. Signs and symptoms can develop after one days of exposure up to two months depending on the type of anthrax infection; the most severe form, inhalation anthrax, develops symptoms rapidly and consist of flu-like symptoms. Antibiotic treatment can be effective, but if inhalation anthrax is not treated within 48 hours after exposure the fatality rate can reach up to 90-100 percent.[12]Anthrax vaccine is not administered to the general public, but only to those who are at risk for naturally occurring exposure or military personnel and first responders. Since testing of blood samples to confirm anthrax infection can take up to 48 hours, but immediate treatment may be necessary to save lives. Environmental surveillance through sensors to pick up disbursal of spores may be more crucial than syndromic surveillance.

Identification of biological agents is complicated due to the diverse nature of the agents and the variety of modes of transmission and disbursal methods. The use of anthrax spores in letters in the 2001 bioterrorism event, which caused inhalation anthrax emphasized the need for immediate detection and identification of biothreat agents from environmental samples as well as from affected persons.[13] Identification of BWA relies

[12] Thavaselvam D, Vijayaraghavan R., Biological warfare agents, *Journal of Pharmacy &BioAllied Sciences*, Jul-Sep 2010, 2(3): 179-188.
[13] Ibid.

on rapid and accurate systems capable of detecting multiple threat agents since symptoms of many biological agents are similar. In addition to human clinical samples like blood, sputum, urine, stool, cerebrospinal fluid, a system also needs to be able to analyze powdery materials, food and water samples, and environmental air and soil samples.[14] Good sample preparation is needed depending on the detection system, and sample preparation can take hours to days depending on the standardized protocols and often cannot be performed in field conditions, especially if the agent is highly contagious and lethal.[15] Although the sample preparation and efficacy of extraction procedures determine the concentration of the agent availability for detection, in some instances, the viability of virus or bacteria has to be confirmed by conventional laboratory culture methods.[16] One concern are genetically modified bacterial and viral agents not covered under the list of known and probable agents which may pose an additional threat and make the detection much more difficult.[17] As a result, public health officials depend on readily accessible health surveillance data and detection systems to support their efforts in identifying the BWA.

Biosensors, Disease Surveillance System, and Health Communication

Biological attacks are difficult to predict and prevent because biological agents have unique characteristics that could be exploited for specific purposes by adversaries. As a result, there is a need for rapid and accurate detection systems to ensure public

[14] Ibid.
[15] Ibid.
[16] Thavaselvam D, Vijayaraghavan R., Biological warfare agents, *Journal of Pharmacy &BioAllied Sciences*, Jul-Sep 2010, 2(3): 179-188.
[17] Ibid.

health officials know early on which agent(s) was used during an attack. These systems are highly interconnected and depend on a continuous data exchange to identify unusual events.

Local clinics and hospital laboratories are the first facilities likely to encounter biological agents as infected or exposed individuals seek medical assistance, which requires them to initiate screening of they encounter a potential case.[18] Widely available microbial identification systems used on a routine basis by clinical laboratories are not designed or optimized for detection of BWAs.[19] The CDC developed BWA screening guidelines, but the assumption is that hospital staff on duty during an event had sufficient training to know when to implement these guidelines. As a result, tools are being developed to detect BWAs. For the detection of biological agents, sensors have been developed for biochemical, immunologic and nucleic acid based detection systems.[20] These sensors combine a biological recognition system and a physical transducer but are not as specific as antibody- or nucleic acid-based methods.[2122] Other sensors, such as electronic nose devices, can detect volatile organic compounds and toxins produced during the growth of bacteria or fungi.[2324] Electronic nose devices can be rapid and sensitive but not very specific because the compounds produced by microorganisms can

---

[18] Lim DV, Simpson JM, Kearns EA, Kramer MF, Current and Developing Technologies for Monitoring Agents of Bioterrorism and Biowarfare. *Clinical Microbiology Reviews,* Oct 2005, 18(4), 583-607.
[19] Ibid.
[20] Thavaselvam D, Vijayaraghavan R., Biological warfare agents, *Journal of Pharmacy &BioAllied Sciences*, Jul-Sep 2010, 2(3): 179-188.
[21] Lim.
[22] Thavaselvam.
[23] Ibid.
[24] Lim DV, Simpson JM, Kearns EA, Kramer MF, Current and Developing Technologies for Monitoring Agents of Bioterrorism and Biowarfare. *Clinical Microbiology Reviews,* Oct 2005, 18(4), 583-607.

fluctuate depending on environmental conditions and different organisms can produce similar volatile products.[25] As a result, detection tools such as biosensors used exclusively for surveillance purposes may not produce the needed rapid and accurate results; instead, they should be used in combination with other surveillance systems. With that being said, surveillance systems are highly interdependent and require continuous data exchange to put results into context.

Biosensors may be able to identify the BWA, but further laboratory testing may be needed to sequence the agent in an effort to determine if the agent was engineered and its origin. Databases have been developed to organize information around gene or protein function for pathogen characterization.[26] The GenBank sequence database includes complete genomic sequences as well as individual sequences, which can also be used to determine the agent's origin as well as DNA synthesis orders that use sequences of pathogens of concern.[27] In recent years, genomic barcoding has been used to standardize genome segment use as the discriminatory parameter for detecting the presence of an organism or to distinguish it from other species.[28] As a result, genetic databases with sequence information could address concerns about the possibility of engineering *de novo* biological pathogens that could be used during a biological attack. Yet, genetic

---

[25] Lim DV, Simpson JM, Kearns EA, Kramer MF, Current and Developing Technologies for Monitoring Agents of Bioterrorism and Biowarfare. *Clinical Microbiology Reviews,* Oct 2005, 18(4), 583-607.
[26] Lindler LE, Lebeda FJ, Korch GW, *Biological Weapons Defense: Infectious Diseases and Counterbioterrorism*, (Humana Press: Totowa, New Jersey, 2005), p.390.
[27] Valdivia-Granda WA, Biodefense Oriented Genomic-Based Pathogen Classification System: Challenges and Opportunities. *Journal of Bioterrorism & Biodefense*, Mar 2012, 3(1), 1000113.
[28] Valdivia-Granda WA, Biodefense Oriented Genomic-Based Pathogen Classification System: Challenges and Opportunities. *Journal of Bioterrorism & Biodefense*, Mar 2012, 3(1), 1000113.

sequencing of a BWA takes time and may only be valuable after a biological attack to gather further information, which suggests that medical encounter data and syndromic surveillance systems may have greater utility to detect early onset of disease within a population.

Various databases have been developed to monitor signs, symptoms, and biological information related to a biological attack. The Defense Health Agency of the DoD maintains and operates the Defense Medical Surveillance System (DMSS), which is a longitudinal and relational database. It contains medical encounter, laboratory, and immunization data as well as demographic and military information on all service members during their active service time. DMSS receives data feeds from numerous DoD agencies, which depending on the data are loaded daily, weekly, or monthly. The data is mainly used to assess health trends and establish baselines for diseases. Most analyses are published in the Medical Surveillance Monthly Report, which are readily available on the agencies website. For near real-time surveillance both DoD and civilian public health departments utilize ESSENCE (Electronic Surveillance System for the Early Notification of Community-based Epidemics), a syndromic surveillance system that provides alerts on unusual increases of infectious disease related symptoms. Updated medical data, such as encounter, pharmacy prescriptions, radiology, and laboratory test orders, are loaded multiple times during the day into ESSENCE and surveillance staff have the opportunity to access patient-identifiable data for further investigation or validation. Disease surveillance databases rely on in-person patient encounters to capture data on the medical event, but often, patients do not have access to medical facilities requiring other methods of patient-provider interaction.

In areas to far away from medical facilities or in communities with limited medical services, telemedicine, a combination of telecommunication and information technology, has been used to bridge the continuum of care. Telemedicine used in DoD and in civilian medical communities is integrated with medical information databases and linked to the National Library of Medicine.[29] Telemedicine consultations rely on computerized consult sheets that were developed using database management software and represent multimedia medical records.[30] The telemedicine approach is based on a computerized two-way audio communication and image transfer linked with satellite video teleconferencing.[31] In addition, consults can be conducted via email, smart phone, wireless tools, and other forms of telecommunications technology. The use of telemedicine during a biological attack could improve situational awareness and ensure comprehensive surveillance of the population by including communities and areas that would not access hospital care.[32] Besides telemedicine, telehealth applications such as hotlines and interactive web-based programs can provide information and guidance to communities and manage patient behaviors after a biological attack.[33] Telehealth message could be used to alleviate public fear and panic to avoid the "worried well" from

---

[29] Lindler LE, Lebeda FJ, Korch GW, *Biological Weapons Defense: Infectious Diseases and Counterbioterrorism*, (Humana Press: Totowa, New Jersey, 2005), p.395.
[29] Valdivia-Granda WA, Biodefense Oriented Genomic-Based Pathogen Classification System: Challenges and Opportunities. *Journal of Bioterrorism & Biodefense*, Mar 2012, 3(1), 1000113.
[30] Lindler, p.395.
[31] Ibid.
[32] Public Health Emergency (PHE)—Department of Health and Human Services, Telehealth Report to Congress, Jan 2009, p.19, at http://www.phe.gov/Preparedness/legal/pahpa/Documents/telehealthrtc-091207.pdf (1 Nov 2015).
[33] Ibid.

overcrowding emergency rooms. Additionally, telehealth communication programs could provide information on points of dispensing for vaccinations or antibiotic prophylaxis administration during emergency management events. Telemedicine and telehealth networks allow for outreach to all communities within a population but require an operational telecommunication infrastructure and electronic access to medical records and medical services.

The combined use of biosensors, disease surveillance systems, and telemedicine for health communication provides timely and relevant information to detect biological attacks and assess their impact on the population. The alignment of health information is critical to make informed decisions on intervention and prevention strategies to reduce morbidity and mortality. At the same time, these systems depend heavily on a fully operational electrical grid. New funding is provided to further electronically integrate existing systems and develop new systems rather than invest in securing to electric grid. Advances in information technology have paved the way for public health surveillance to function more efficiently and effectively, but this progress can be eradicated in no time if circuits have been damaged and electronic health surveillance tools can no longer be accessed. As a result, efforts should be made to harden existing surveillance systems

Electromagnetic Pulse (EMP) and Cyber Attack

Monitoring a population to identify potential exposure to a biological agent presumes an electrical grid that is functioning since detection, surveillance, identification, and communication efforts are based on electronic system capabilities. An EMP is a high-intensity burst of electromagnetic energy that can destroy, damage, or cause the

malfunction of electronic systems by overloading their circuits.[34] Harmless to people but catastrophic to critical infrastructure such as electric power, telecommunications, transportation, banking and finance, food and water for which there are limited countermeasures in place.[35] A single nuclear weapon detonated at high-altitude will generate an electromagnetic pulse that can damage the power grid across the entire contiguous U.S.[36] Non-nuclear weapons, also referred to as radiofrequency weapons, can also generate an EMP but have a limited range that could damage the critical infrastructure locally.[37] The power grid could also be downed through hackers during a cyber attack. EMP or cyber attacks are threats that can hold society at risk of catastrophic consequences especially if launched concurrently with a biological attack.

An EMP could arise from natural, man-made, or weapons detonation, yet the effects on the electrical grid and information systems are similar even though different in intensity. A naturally occurring EMP could happen through lightening or a solar flare reaching earth. A man-made EMP or High-Power Microwave (HPM) electromagnetic energy can be produced through special electrical equipment that transforms battery power, or a powerful chemical reaction, or explosion into intense microwaves.[38] These microwaves can be as damaging to electronics as a high altitude EMP but on a smaller

[34] Securethegrid, EMP: Technology's Worst Nightmare, 2015, at http://securethegrid.com/emp-technologys-worst-nightmare/ (Oct 30, 2015).
[35] Ibid.
[36] Ibid.
[37] Ibid.
[38] Wilson C., "High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessment", Congressional Research Service Report to Congress. Jul 2008, p. 6, https://www.fas.org/sgp/crs/natsec/RL32544.pdf , 3 Nov 2015.

scale over a smaller area.[39] An EMP caused by a nuclear detonation above the U.S. has the potential to cause large-scale destruction and disruption of electrical devices and systems. The two types of EMP threats that are most concerning are the 1) intentional electromagnetic interference (IEMI) and the 2) high altitude electromagnetic pulse (HEMP). The IEMI is created by deliberate electromagnetic weapon attack, and the HEMP is created by a high-altitude nuclear weapon detonation. A single nuclear weapon exploded at high altitude (40 to 400 kilometers) above the U.S. will interact with the Earth's atmosphere, ionosphere, and magnetic field to produce an EMP radiating down to the earth.[40] The electromagnetic fields produced by weapons designed and deployed with the intent to produce EMP have a high likelihood of damaging electrical power systems, electronics, and information systems.[41] With its destructive power toward the electrical grid and critical infrastructure, a HEMP may be used by adversaries and should be considered a WMD even though it initially will not cause physical damage or loss of life.

The nuclear EMP, even though instantaneous, is a complex multi-pulse that occurs in three phases which is unique to the nuclear detonation. The first component (E1) is a free-field energy pulse, also called the "electromagnetic shock" that disrupts or damages electronics-based control systems, sensors, communications systems, protective systems, computers, and similar devices.[42] Disruption occurs over a very large area and could include multiple cities or an entire region such as the East Coast. The second

---

[39] Wilson C., "High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessment", Congressional Research Service Report to Congress. Jul 2008, p. 6, https://www.fas.org/sgp/crs/natsec/RL32544.pdf , 3 Nov 2015.
[40] Foster JS et al. "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Volume1: Executive Report 2004", 2004, p. 1, at http://www.empcommission.org/docs/empc_exec_rpt.pdf (2 Nov 2015).
[41] Ibid.
[42]Foster, p. 5.

component (E2) is similar to lightening and would affect the same geographic area as the first component.[43] Most critical infrastructure has protective measure for defense against lightning strikes, but since the E2 component follows within a small fraction of the E1, it has the ability to destroy many protective and control features and damage systems.[44] The third component (E3) is a slower-rising, longer-duration pulse that disrupts electricity transmission lines and therefore causes damage to the electrical supply and distribution system.[45] The three components build on each other and in unison can destroy about 70 percent of the total electrical power load within a region of attack.

In order to understand the impact of an EMP attack, it is important to understand the electromagnetic immunity. Most electronic equipment can survive a pulse of 10 Volts per meter (V/m). Computers and other systems based on microprocessors are vulnerable to radiated narrowband fields above 30 V/m, and newer high-speed PCs may be resistant up to about 300 V/m.[46] Most robust aircraft cockpit equipment is only designed to survive up to 7,200 V/m. A HEMP could result in a high intensity pulse of over 10,000 V/m, which is more than 1,000 times than what IT systems can handle. In addition, a HEMP will not just damage the electrical grid, but can also have a direct impact on stored data by irrevocably destroying and erasing data. Another key vulnerability are Supervisory Control And Data Acquisition systems (SCADAs) which are small

---

[43] Foster JS et al. "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Volume1: Executive Report 2004", 2004, p. 6, at http://www.empcommission.org/docs/empc_exec_rpt.pdf (2 Nov 2015).
[44] Ibid.
[45] Foster, p. 1.
[46] Radasky W.A., "Electromagnetic Warfare is Here: A briefcase-size radio weapon could wreak havoc in our networked world", Institute of Electrical and Electronics Engineers (IEEE), 25 Apr 2015, http://spectrum.ieee.org/aerospace/military/electromagnetic-warfare-is-here , 20 Nov 2015.

computers imbedded into the electrical grid and critical infrastructure. SCADAs regulate the flow of electricity into a transformer, control the flow of gas through a pipeline, or run traffic control lights and manage the infrastructure of entire cities, and are highly vulnerable to an EMP.[47] As a result, a HEMP significantly disrupts the critical infrastructure, electrical grid, and electronic equipment, and is more than just a power outage because some of the damage is permanent.

Electronic failures occur all the time under normal operation, but any type of EMP induces unique failures and upsets which may take weeks, months, or years to repair. Some components of critical infrastructures, such as large turbines, generators, and high-voltage transformers in electrical power systems, would require long periods of time to repair or replace.[48] Similar damage occurred during the Northeast power blackout of 1965, during which the Ravenswood power plant in New York City suffered damage and was out of service for nearly a year.[49] In 1977, two lightning strikes caused overloading in the electric power substations of the Con Edison power company in New York City, and even though the blackout only lasted one day, nearly 3,000 people were arrested for widespread looting and damage repair costs were approximately $346

[47] Pry PV, "Electromagnetic Pulse: Threat to Critical Infrastructure", Testimony before the Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies House Committee on Homeland Security, 8 May 2014, p. 8, http://docs.house.gov/meetings/HM/HM08/20140508/102200/HHRG-113-HM08-Wstate-PryP-20140508.pdf, 6 Dec 2015.
[48] Foster JS et al. "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Volume1: Executive Report 2004", 2004, p. 12, at http://www.empcommission.org/docs/empc_exec_rpt.pdf (2 Nov 2015).
[49] Ibid.

million.[50] Similar effects occurred during a less sever event caused by a HPM. In 2001, a U.S. Comanche helicopter equipped with HPM weapons, generated a low-level energy pulse while performing a radar test that disrupted GPS systems of a nearby airport for two weeks.[51] In comparison to routine technical issues with electronic devices and systems, EMP produces simultaneous outages and damages of electronic and of other electrical equipment. These concurrent outages make it difficult to determine where to take actions first to restore the systems further slowing down the recovery process. The National electrical grid not infrequently operates at or very near local limits on its physical capacity to move power from generation to load so that even minor upsets can cause a functional collapse.[52] Prior power outages, even though not as destructive as a large-scale EMP, have shown that repairing the electrical grid can be time consuming and can be a significant financial burden.

After having observed the impact of prior outages similar to an EMP, adversaries may be interested in pursuing EMP attacks. To launch a HEMP at the U.S., an adversary would need missiles capable of an intercontinental launch or a platform that can be moved within range of the U.S. to launch a missile. In order to discuss an imminent attack, cyber attacks could be used to weaken power and early warning systems. Cyber attacks are executed via the internet and use malicious code to alter existing computer

---

[50] The Heritage Foundation, "Think Ahead: Preparing for the Threat of Our Wired World", p. 4, http://www.heritage.org/issues/missile-defense/electromagnetic-pulse-attack (2 Nov 2015).
[51] Wilson C., "High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessment", Congressional Research Service Report to Congress. Jul 2008, p. 9, https://www.fas.org/sgp/crs/natsec/RL32544.pdf , (3 Nov 2015).
[52] Foster JS et al. "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Volume1: Executive Report 2004", 2004, p. 18, at http://www.empcommission.org/docs/empc_exec_rpt.pdf (2 Nov 2015).

code, logic, or data. A cyber attack may be different from an EMP because it often leaves "fingerprints" behind, which can then be used to track its originator. An EMP, on the other hand, is often so quick that electronic systems will be unable to identify the cause of the electronic shutdown. One of the main goals of a cyber attack is to steal information, but it can also be used to disrupt online processes. In 2003, more than 200 power plants were shut down after a software bug in the computer system of one power plant caused an initial blackout.[53] Today's power grid relies increasingly on modern computational platforms (SCADAs), field devices, and communication networks so that IT functions intended to surveil, disrupt, deny, degrade, compromise, or control the performance the system could be introduced.[54] Since an EMP could cause more large-scale damage and may be more suitable for a WMD attack, a cyber attack may be executed in combination with an EMP to eliminate detection. Cyber weapons need to be tailored to the devices they are targeting and only attack systems that are software dependent.[55] Neither EMP nor cyber attacks are deterministic, nor are they completely random, which makes it difficult to predict their effect.[56] Not every targeted system will be in the same state of vulnerability, so there is a random component to the failures

---

[53] The Heritage Foundation, "Think Ahead: Preparing for the Threat of Our Wired World", p. 5, http://www.heritage.org/issues/missile-defense/electromagnetic-pulse-attack (2 Nov 2015).
[54] Hawk C, Kasushiva A. "Cybersecurity and the Smart Grid", *The Electricity Journal*, Oct 2014, 27(8), 84-95, doi:10.1016/j.tej.2014.08.008.
[55] Frankel M, Scouras J, DeSimone A, "Assessing the Risk of Catastrophic Cyber Attack: Lessons from the Electromagnetic Pulse Commission", Research Note, Johns Hopkins Applied Physics Laboratory, 2015, p. 8, http://www.jhuapl.edu/newscenter/publications/pdf/AssessingtheRiskofCatastrophicCyberAttack.pdf, (6 Dec 2015).
[56] Frankel, p. 9.

induced by a cyber attack.[57] Both EMP and cyber attack present threats to systems and using them combined could cause prolonged regional and national recovery.

An EMP and cyber attack may not have a direct harmful effects on human life, yet indirectly disrupt the infrastructure necessary for human survival such as food and water supplies, equipment for hospitals and first responders, as well as fuel distribution and transportation. The simultaneous loss of communications and power as a result of an EMP attack will make it difficult to ascertain the nature and location of the damage and to send personnel to the sites to initiate repairs. [58] With electrical systems non-operational for weeks or months or longer, a concurrent biological attack would be difficult to detect. Electronic equipment such as biological sensors and testing devices will be non-functional after an EMP. In addition, the healthcare sector relies on advanced information technology systems to track medical encounters, patient health histories, pharmaceutical prescriptions and prophylaxes, as well as laboratory testing results. These health surveillance systems depend on telecommunication networks to maintain data transfers and exchange of information between organizations. These systems are also used to communicate with patients to send out alerts and notifications during emergencies to advice communities on preventive health measures and when to seek medical care. Since the symptoms of most diseases caused by a biological agents mimic the symptoms of the

---

[57] Frankel M, Scouras J, DeSimone A, "Assessing the Risk of Catastrophic Cyber Attack: Lessons from the Electromagnetic Pulse Commission", Research Note, Johns Hopkins Applied Physics Laboratory, 2015, p. 9, http://www.jhuapl.edu/newscenter/publications/pdf/AssessingtheRiskofCatastrophicCyberAttack.pdf, (6 Dec 2015).

[58] Wilson C., "High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessment", Congressional Research Service Report to Congress, Jul 2008, p. 9, https://www.fas.org/sgp/crs/natsec/RL32544.pdf , (3 Nov 2015).

common cold, people may be less likely to seek medical care, especially if they have to face other priorities such as procuring food and water. This may allow for uncontrolled spread of disease within populations, and if affected individuals who seek treatment at a later stage of the disease may overwhelm emergency rooms with limited ability to properly test, diagnose, and treat them. It is therefore not the immediate effect of the loss of power that makes an EMP so destructive, but the cascading losses of critical infrastructure over time.

In summary, biological, EMP and cyber attacks pose unique response challenges and by themselves are destructive in nature. EMP and cyber attack as compared to a biological attack may not directly affect human life, but the consequences of lack of electricity and data systems that manage our daily lives will indirectly affect our well-being. Most biological category A agents are extremely contagious and deadly if not identified and treated immediately. At the same time, they are relatively easy to identify and manage in a population if health surveillance systems are fully functioning. Yet, without existing electronic public health tools, it will be difficult to identify these agents and track the mode of transmission and individuals affected. As a result, these agents can become true hazards and can lead to increased morbidity and mortality. EMP and cyber attacks can disable disease surveillance systems and have the potential to exacerbate the effects of a biological attack by itself.

BIODEFENSE—SENSORS, FEDERAL SURVEILLANCE AND SUPPLY PROGRAMS

Prevention of a WMD event and responding to one if people have been exposed is a multimodal and multiagency approach, which requires resource and information sharing. There is no central agency that leads control and coordination of the defense against biological threats. Many agencies at the local, state, and federal level with unique capabilities are involved in a response to a biological attack. The lack of centralized biodefense leadership may be of concern because it allows agencies to operate independently or duplicate each other's efforts. The lack of a comprehensive, cohesive, and regularly updated strategy has resulted in disorganization and confusion on how to execute a response.[59] Biodefense planning has become driven by agencies with requirements that may or may not meaningfully contribute to national biodefense.[60] Yet, the limitations and shortfalls of the various disease surveillance systems sponsored by federal agencies is only one problem. Each system will be affected by an EMP and cyber attack through disrupting the normal functioning of system components such as electronic tools and equipment, data transfer, transportation and delivery mechanisms. The following sections assume that a biological agent has been released among a population followed by an EMP and cyber attack and will assess a selected number of surveillance systems most commonly used to detect biological agents.

---

[59] Hudson Institute, "A National Blueprint For Biodefense: Leadership and Major Reform Needed to Optimize Efforts," Bipartisan Report of the Blue Ribbon Study Panel on Biodefense, Oct 2015, p. 29, at http://hudson.org/research/11824-a-national-blueprint-for-biodefense-leadership-and-major-reform-needed-to-optimize-efforts (Nov 1, 2015).
[60] Hudson Institute, p. 29.

BioWatch

BioWatch, a Department of Homeland Security (DHS) program developed in collaboration with the Environmental Protection Agency (EPA), is a nationwide bio-surveillance system designed to detect the intentional release of selected aerosolized biological agents. It is an environmental monitoring system that collects and analyzes samples in designated laboratories every 24 hours.[61]Deployed in more than 30 metropolitan areas throughout the country, the system is a collaborative effort of health personnel at all levels of government. The BioWatch program has air samplers intended to swiftly detect the presence of certain aerosolized biological agents to assist local and state health officials in their surveillance efforts.[62] BioWatch has the potential to provide a timelier alert than the public health and health care system if a large-scale aerosol attack occurs where BioWatch is deployed, if an air sampler lies in the path of the release, and if the pathogen used is one of those included in the BioWatch laboratory assays.[63] With that being said, small quantities of a biological agent may not be detected by BioWatch and is a limitation of the surveillance capability.

BioWatch may be a useful system to detect specific biological agents, but infectious disease surveillance through the public health and health care systems is broader and more flexible than BioWatch. Disease surveillance systems currently in existence have the potential to detect infectious diseases resulting from various

[61] Institute of Medicine (IOM) and National Research Council (NRC), *BioWatch and public health surveillance: Evaluating systems for the early detection of biological threats. Abbreviated version,* Washington, DC: The National Academies Press, 2011, p.3.
[62] IOM, p. 1.
[63] IOM, p. 2.

exposures.[64] One of the issues with the BioWatch program is that it is not fully integrated into the local systems in which it operates. The "BioWatch System" refers to the collection of operational components that produce information from air sampling and feed it into a public health decision-making process to determine appropriate response to BioWatch Actionable Result (BAR).[65] Public health officials particularly need greater assistance in developing the necessary capabilities to interpret and respond to BARs.[66] BioWatch may be able to detect DNA segments of a BWA, but those may not be BARs because detection does not necessarily imply a biological attack occurred or that individuals have been exposed.[67] Besides early detection, BioWatch is currently working on improving communication with local, state, and federal public health officials. Currently, the program does not share information with other systems on animal health, vector control, water and air quality, meteorology, and syndromic health surveillance.[68] Even though the information may be helpful for early warning and situation awareness, as a stand-alone system BioWatch data may not be accurately interpreted.

BioWatch has its limitations but otherwise may be a useful surveillance tool as part of a larger surveillance system. One of the concerns is that during an EMP or cyber attack or both, BioWatch may not be able to function because the equipment depends on electricity. Additionally, staff may not be able to reach the equipment in a timely manner due to disruption of transportation, which will result in the filters not being shipped to the

---

[64] Institute of Medicine (IOM) and National Research Council (NRC), *BioWatch and public health surveillance: Evaluating systems for the early detection of biological threats. Abbreviated version,* Washington, DC: The National Academies Press, 2011, p. 2.
[65] IOM, p. 37.
[66] IOM, p. 6.
[67] Ibid.
[68] IOM, p. 13.

nearest laboratory for analysis. The air samplers BioWatch deploys have a 24-hour collection cycle, and their dry filters are manually collected and transported to laboratories for processing and analysis.[69] The program requires a person to go out every day to collect the filters and deliver them to the laboratory according to strict standard operating procedures.[70] With this approach, the time between exposure, detection, confirmation and declaration of a BAR is somewhere between 12 to 36 hours.[71] If BioWatch could move to autonomous detection systems, this time could be reduced to 3 to 6 hours.[72] As a result, routine maintenance and monitoring of the sensors is crucial for the program to function, which may be fully disrupted through an EMP or cyber attack therefore making this surveillance tool inoperable.

BioSense

Mandated in the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, the BioSense platform was launched in 2003 as a National Syndromic Surveillance Program (NSSP) by the Centers for Disease Control and Prevention (CDC). The program is considered a "system-of-systems" that integrates patients' symptoms, quantities and types of drug prescriptions, number of emergency

---

[69] Institute of Medicine (IOM) and National Research Council (NRC), *BioWatch and public health surveillance: Evaluating systems for the early detection of biological threats. Abbreviated version,* Washington, DC: The National Academies Press, 2011, p. 33.
[70] Institute of Medicine (IOM) and National Research Council (NRC), *Technologies to Enable Autonomous Detection for BioWatch: Ensuring Timely and Accurate Information for Public Health Officials. Workshop Summary,* Washington, DC: National Academies Press, 2013, at http://www.ncbi.nlm.nih.gov/books/NBK201349/, (2 Nov 2015).
[71] IOM, 2013.
[72] Ibid.

room visits, and various other patient data.[73] It is a nationwide system that builds on state and local health department surveillance systems.[74] State and local systems often operate independently from each other and do not share information, yet the purpose of BioSense is to combine these existing data systems. The data is still stored at state and local health departments, who collect them for their disease surveillance purposes, but CDC is granted access to the data, which creates for a more robust framework, so if one data feed is interrupted, BioSense will still function with the available data.[75] BioSense started incorporating Department of Defense (DoD) health data, to include outpatient encounter data, as well as data from Department of Veterans Affairs (VA) hospitals to be able to conduct comprehensive surveillance on the majority of the U.S. population. The goal of BioSense is to provide public health officials on all levels a common electronic health information system with standardized tools and procedures for rapidly collecting, sharing, and evaluating of information.

Over the years, the BioSense platform has undergone numerous updates and revisions, but the system was never fully operational. The system is now being switching to ESSENCE (Electronic Surveillance system for the Early Notification of Community-based Epidemics), which has been used successfully by local and state health departments for the past 10 years for local syndromic surveillance purposes as well as by DoD for surveillance on its military population in the U.S. and overseas. Additionally, data for the new BioSense platform will be stored on a secure internet government cloud

[73] Levi, J, *Ready or Not?: Protecting the Public's Health from Diseases, Disasters, and Bioterrorism,* Darby, PA: DIANE Publishing, 2011, p. 34
[74] Ibid.
[75] Ibid.

rather than on servers in fixed facilities.[76] This means that copies of the data are distributed among multiple servers in widely separated locations, so that no single disaster can destroy or render the data inaccessible.[77] Amazon Web Services, currently one of the leading provider of cloud computing, guarantees that data will survive any catastrophe; yet, in 2009, lightning caused its cloud computing services to go offline for four hours.[78] In 2012, a storm disrupted an Amazon data center in Virginia, disrupting access to Netflix, Instagram, Pinterest, and other sites for hours, even though no data was destroyed.[79] Even though single catastrophic events may not disrupt cloud services for a lengthy period since other cloud servers can support the system, large-scale events, such as EMP may impact all cloud servers in a region and could disrupt and destroy data.[80] As a result, surveillance system platforms, no matter how they store data, are vulnerable to EMP and access may be disrupted.

The goal of the new BioSense platform is to enhance regional and national all-hazards public health situation awareness, yet cooperative agreements have not been signed by all public health departments to share data and information electronically. So far, only 35 public health jurisdictions have entered cooperative agreements, which include states, cities, and counties.[81] For example, there is no agreement for health care

---

[76] CDC, National Syndromic Surveillance Program (NSSP), BioSense Platform, State and Local Support: Cooperative Agreement, 15 Mar 2015, http://www.cdc.gov/nssp/biosense/cooperativeagreement.html, (25 Nov 2015).
[77] Adams, C, "How safe is 'the cloud'?", The Straight Dope, 15 May 2015, http://www.straightdope.com/columns/read/3228/how-safe-is-the-cloud , (6 Jan 2016).
[78] Ibid
[79] Ibid.
[80] Ibid.
[81] CDC.

data sharing with Texas, but Tarrant County, one of the Texas counties which includes the Fort Worth area, has agreed to share their data.[82] Instead of state-wide surveillance, some surveillance data is restricted to counties and cities only. As a result, one of the limitations with the new BioSense version continues to be completeness of surveillance data.

Even with this limitation, the BioSense platform can provide nation-wide syndromic surveillance capability but relies on electronic transfer of health care encounter and related data from its participants. If an EMP and cyber attack would occur, this electronic transfer of data would be disrupted. An attack restricted to a geographic area not to include Atlanta where the CDC resides would allow the system to continue functioning, but would miss the data from the affected area. More concerning is that such an attack would erase exiting data in the surveillance systems. ESSENCE uses algorithms comparing historical data to current data feeds to calculate alerts indicating potential spikes in syndromic and disease categories. If this functionality is lost in affected areas, re-establishing the electronic data transmission after an attack may not be useful for continued disease monitoring.

Strategic National Stockpile (SNS)

Project BioShield was signed into law in 2004, in response to the need for funds to stockpile medical countermeasures against any CBRN threats, even though the initial

[82] CDC, National Syndromic Surveillance Program (NSSP), BioSense Platform, State and Local Support: Cooperative Agreement, 15 Mar 2015, http://www.cdc.gov/nssp/biosense/cooperativeagreement.html, (25 Nov 2015).

focus was on biological threats.[83] Although the funds are in the DHS appropriation, the Department of Health and Human Services (HHS) was designated as the acquisition agency.[84]BioShield provides funds and spurs private sector research and procurement of appropriate medical countermeasures such as new PEP to the Strategic National Stockpile (SNS), while the development of new treatment has been modest in scope.[85] The bill also gave the U.S. Food and Drug Administration the authority to provide Emergency Use Authorization before licensure for medical countermeasures in the later stages of product development in the event of an emergency need.[86] Whereas BioShield provides funding for research and procurement of products for the Strategic National Stockpile (SNS) in response to a biological attack, the Public Health Service Act authorized HHS in coordination with DHS and CDC to maintain the SNS.

Strategic stockpiles of vaccines as well as respective medication to treat a highly contagious diseases can be provided within less than 24 hours to an affected area.[87] The SNS program was designed to supplement and resupply state and local inventories of medicines and supplies during emergencies once local supplies had been exhausted.[88] As a result, state governors or their designees may request deployment of SNS assets, yet the

---

[83] Russell PK, "Project BioShield: What Is It, Why It Is Needed, and Its Accomplishments So Far," *Clinical Infectious Diseases,* 2007, 45(S1), S68-S72, p. S68.
[84] Russell, p. S69.
[85] Grundmann O, "The current state of bioterrorist attack surveillance and preparedness in the U.S.", *Risk Management and Healthcare Policy*, Oct 2014, 7, 177-187, http://dx.doi.org/10.2147/RMHP.S56047, (14 Dec 2015).
[86] Russell, p. S69.
[87] Grundmann, p. 181.
[88] Association of State and Territorial Health Officials (ASTHO), Emergency Use Authorization Toolkit: Strategic National Stockpile, http://www.astho.org/Programs/Preparedness/Public-Health-Emergency-Law/Emergency-Use-Authorization-Toolkit/Strategic-National-Stockpile-Fact-Sheet/, (30 Nov 2015).

federal government is responsible for making the decision to deploy all or portions of the SNS.[89] Each state within the U.S. has established protocols and facilities where sufficient amounts of vaccines and antibiotics are being stored, and in addition, facilities across the nation collectively house vaccine and antibiotic supplies.[90] Major metropolitan areas have established measures to ensure supply of vaccines and medicines if needed within 48 hours through dispensaries in the communities.[91] Locations of the warehouses are not made public and distribution assumes that the supplies can be readily accessed and transported.

Early outbreak detection can only achieve a lower mortality rate if a rapid and high dispensing capacity of vaccines and medications can be achieved among the affected population.[92] The declaration of a federal or state public health emergency is not required to deploy the stockpile and its contents can also be deployed in advance of a public health emergency.[93] With that being said, local and state authorities need to have the capability to communicate their needs to federal authorities, yet means of communications will be most likely disrupted during an EMP and cyber attack. Additionally, SNS assets are delivered to one predesignated location in the state, and state personnel have to travel to the designation to receive and transport the medications to the locations where the

---

[89] Association of State and Territorial Health Officials (ASTHO), Emergency Use Authorization Toolkit: Strategic National Stockpile, http://www.astho.org/Programs/Preparedness/Public-Health-Emergency-Law/Emergency-Use-Authorization-Toolkit/Strategic-National-Stockpile-Fact-Sheet/, (30 Nov 2015).
[90] Grundmann O, "The current state of bioterrorist attack surveillance and preparedness in the U.S.", *Risk Management and Healthcare Policy*, Oct 2014, 7, 181, http://dx.doi.org/10.2147/RMHP.S56047, (14 Dec 2015).
[91] Ibid.
[92] Grundmann, p. 181.
[93] ASTHO.

supplies are needed.[94] Since an EMP will disrupt the transportation infrastructure, state personnel will not be able to travel to and from the predesignated SNS location. As a result, the federal government needs to be able to provide more support and be prepared to deliver the medical assets to the needed locations. Since local and state public health authorities have to use their medical stockpiles first, there may not be an initial need for SNS supplies during the early stages after an EMP attack. This may allow local authorities to reestablish communication, but may also lead to unrest in the population, which could make it difficult for federal authorities to deliver needed medical supplies or to make their deliver a priority. One possible alternative would be the use of commercial products within the local area. During the 2009 H1N1 pandemic influenza outbreak, federal and state health officials identified limited visibility into commercial supply chains but also lack of knowledge by local public health authorities on what is available through the SNS.[95] As a result, the Commercial Supply Chain Dashboard was developed to maintain situation awareness on the available medical stock and coordinate supplies between local commercial partners and the federal and state governments.[96] This relationship with private-sector companies to improve the medical response was beneficial during the H1N1 pandemic, yet in the aftermath of an EMP attack, this

---

[94] Association of State and Territorial Health Officials (ASTHO), Emergency Use Authorization Toolkit: Strategic National Stockpile, http://www.astho.org/Programs/Preparedness/Public-Health-Emergency-Law/Emergency-Use-Authorization-Toolkit/Strategic-National-Stockpile-Fact-Sheet/, (30 Nov 2015).

[95] Institute of Medicine (IOM), "Medical Countermeasures Dispensing: Emergency Use Authorization and the Postal Model", Workshop Summary, Washington DC. National Academy Press, 2010, p.13, http://www.ncbi.nlm.nih.gov/books/NBK53126/pdf/Bookshelf_NBK53126.pdf, (2 Dec 2015).

[96] Ibid.

capability would be lost since companies and local public health authorities affected by the attack could not forward valuable information electronically.

Laboratory Response Network (LRN)

The Laboratory Response Network consists of approximately 25,000 commercial and private sentinel laboratories for initial detection of biological and other agents, which will then be confirmed by over 150 reference laboratories across the nation.[97] The LRN was established by HHS and CDC in collaboration with the Federal Bureau of Investigations (FBI), state and local agencies, as well as the Association of Public Health Laboratories.[98] LRN is funded and managed by the Department of Health and Human Services (HHS) through CDC, but state and local public health agencies are responsible for on-the ground management of network assets and response to positive findings.[99] The LRN is tasked to maintain an integrated network of state and local public health, federal, military, and international laboratories that can respond to bioterrorism and other WMD events.[100] Since local hospitals and laboratories are often not equipped to work with potential biological agents, reference laboratories are needed to accurately identify a biological agent during the early stage of transmission to determine the type of care for the cases and the preventive measures for the non-affected population.

---

[97] Grundmann O, "The current state of bioterrorist attack surveillance and preparedness in the U.S.", *Risk Management and Healthcare Policy*, Oct 2014, 7, 177-187, http://dx.doi.org/10.2147/RMHP.S56047, p. 182, (15 Dec 2015).
[98] CDC, Emergency Preparedness and Response: The Laboratory Response Network Partners in Preparedness", 30 Sep 2014, http://emergency.cdc.gov/lrn/, 3 Dec 2015.
[99] Shea DA, Lister SA, "The BioWatch Program: Detection of Bioterrorism", Congressional Research Service *Report to Congress*, 19 Nov 2003, http://www.fas.org/sgp/crs/terror/RL32152.html (3 Nov 2015).
[100] CDC.

The majority of the 25,000 private and commercial laboratories in the U.S. are located in hospitals, clinical institutions, and commercial diagnostic facilities and often lines of communications are not well established.[101] The laboratories often cannot perform specialized testing but can only conduct initial screening. As a result, the sample will be forwarded to a reference laboratory that has the ability to investigate referral specimens suspect of a biological agent. The referral laboratories are made up of more than 150 state and local public health, military, international, veterinary, agriculture, food, and water testing laboratories.[102] If it was determined that the sample may contain a highly contagious agent, the sample will be forwarded to a national laboratories operated by the CDC, the U.S. Army Medical Research Institute for Infectious Diseases (USAMRIID), or the Naval Medical Research Center (NMRC).[103] The national laboratories will conduct strain characterization of the contagious agents.[104] As a result of moving samples through the system, it is often unclear who needs to review the results and most of the laboratories are not integrated into the EHR can cannot provide their results electronically to the patient record. One of the problems with the LRN is that even though clear lines of responsibilities have been established, communications between laboratories and with public health officials are not always clear.

One of the challenges after an EMP will be the transportation of samples from the local collection sites to the appropriate laboratory since the transportation infrastructure will have collapsed. The majority of states and territories currently have laboratories that

---

[101] CDC, Emergency Preparedness and Response: The Laboratory Response Network Partners in Preparedness", 30 Sep 2014, http://emergency.cdc.gov/lrn/, 3 Dec 2015.
[102] Ibid.
[103] Ibid.
[104] Ibid.

are designated as Biosafety Level 3 facilities, meaning they are facilities that meet strict safety and security guidelines to handle potentially highly infectious agents, yet even local transportation will be difficult to undertake.[105] Even if transportation were to become available, it may not be used for transporting lab specimens but rather food and water supplies. Additionally, laboratories within the affected area may not operational due to lack of electricity and data analysis tools. The Air Force Research Laboratory demonstrated that hydrogen fuel cell technology could be used during a power outage to sustain laboratory functions, but these fuel stations could only provide power for 10 days and did not provide a long-term solution. Another issue is the communication of laboratory results. The majority of the LRN laboratories are not integrated into the electronic healthcare record (EHR), so results will not be electronically reported to the local providers who ordered the test but has to be reported via phone or email. If a biological agent was disbursed prior to an EMP attack so that a national LRN laboratory was able to identify the agents, it will be challenging after the EMP to communicate the results to the public health officials.

In summary, existing electronic public health surveillance systems are operated by various agencies and have limitations in regards to the way they operate and the data they collect. The majority of the systems do not share their data, but if used together, they can complement each other and may provide useful early detection capabilities to limit

[105] CDC, Emergency Preparedness and Response: The Laboratory Response Network Partners in Preparedness", 30 Sep 2014, http://emergency.cdc.gov/lrn/, 3 Dec 2015.

morbidity and mortality within an affected population. After an EMP and cyber attack, these systems will become inoperable and existing data may have been erased so that once electricity has been restored, they may still not be fully operational. An EMP and cyber attack will also have an impact on the systems that manage and monitor medical supplies and equipment, so that it will be challenging to ensure the appropriate medical supplies are at hand and disbursed. Given that these systems by themselves face significant issues that compromise their effectiveness during a response to a biological agent, an EMP and cyber attack in combination with a biological agent will confound these issues and will make it more difficult conduct health surveillance and coordinate an effective medical response.

INTERAGENCY COORDINATION OF A PUBLIC HEALTH RESPONSE

The tools needed to respond to a public health emergency involving a biological threat need to involve the relevant communities. A potential biological weapons' incident needs to involve the public health and medical communities, law enforcement and counterterrorism agencies, national security, emergency management agencies, biotech, pharmaceutical, and related companies, as well as the scientific community. In order for those communities and agencies to work together and coordinate their efforts, the ability to communicate during a response to biological agent exposure followed by an EMP and cyber attack becomes the main issue. During routine operations, established and standard response procedures to a biological agent are well described, yet with concurrent EMP and cyber attacks, internal and external factors may create stressors that disable normal functioning of agencies. The purpose of communication and coordination is to protect and prevent one agency or organization from becoming overwhelmed with the public health response and management. Many organizations have crisis contingency and disaster recovery plans, but especially civilian organization do not test these plan on a regular basis, and most plans do not address concurrent WMD events. The Department of Homeland Security (DHS) and its Federal Emergency Management Agency (FEMA) have the lead on all responses to disasters, including for coordinating the federal response to a bio event. The Office of the Assistant Secretary for Preparedness and Response (ASPR) is the lead Department of Health and Human Services (HHS) agency coordinating a medical response to disasters and public health events. DoD Northern Command (NORTHCOM) and a state's National Guard are able to support emergency

responses with more than 18,000 military responders. The Centers for Disease Control and Prevention (CDC) assists state and local governments to develop emergency response plans and can support this plans if needed. The Federal Bureau of Investigation (FBI) has the authority to investigate individuals that attempt to obtain or use WMD materials. As a result, communication to enable coordination of response efforts is crucial, and numerous federal agencies will have active roles.

Department of Homeland Security (DHA)

The DHA has the mission to ensure a safe and secure homeland, and one of its tasks is to ensure resilience to disasters by regulating interaction of federal, state, local, tribal, private sector, and nongovernmental organizations.[106] One way to build resilience is to coordinate the comprehensive federal response to a terrorist attack or large-scale event while working with other agencies and the private sector.[107] In order to support this task, the DHS provides plans and training to its partners. Additionally, the DHS Office of Emergency Communications (OEC) developed the National Emergency Communications Plan (NECP) to improve emergency communications and interoperability between the various response teams and agencies.[108] The vision of the NECP is to communicate and share information across all levels of government when there is a threat or hazard; yet, the plan does not outline what to do in case communication channels have been disrupted by an EMP and cyber attack. According to The Homeland Security Act of 2002, the task

[106] Department of Homeland Security (DHS), "About DHS: Our Mission", 16 Jul 2015, http://www.dhs.gov/our-mission , (30 Jan 2016).
[107] DHS, "Mission: Building a Resilient Nation", 17 Jul 2015, http://www.dhs.gov/building-resilient-nation , (30 Jan 2016).
[108] Ibid.

is not to provide or determine methods of communications, but to provide recommendations regarding how the U.S. should support and promote the ability of emergency response providers and relevant government officials to continue to communicate during an incident.[109] With that being said, the DHS emphasizes interoperability and the supporting technologies, but does not take it a step further and recommend how to protect such communication networks during an EMP, cyber attack, or other events. Instead, it is the responsibility of each organization to ensure comprehensive cyber training and education on the proper use and security of devices and applications.[110] Additionally, each organization needs to conduct assessments of cyber risks and strategies to mitigate vulnerabilities before the deployment of internet protocol-based networks.[111] The OEC provides assistance with tools and services, as well as technical assistance; yet updating broadband and cyber security may be too costly for some states and local organizations. As a result, emergency communications funding by DHA needs to be expanded to ensure consistent updating and securing of systems among agencies. Nevertheless, the NECP does not address protection of communications equipment and devices against EMP specifically, which should be integrated along with cyber security requirements.

[109] DHS, "National Emergency Communications Plan", 2014, p. 2, http://www.dhs.gov/sites/default/files/publications/2014%20National%20Emergency%20Communications%20Plan_October%2029%202014.pdf , (2 Feb 2016).
[110] DHS, "National Emergency Communications Plan", 2014, p. 10.
[111] Ibid.

Federal Emergency Management Agency (FEMA)

Using the authorities outlined under the Homeland Security Presidential Direactive-5 and the Stafford Act, FEMA leads the federal interagency team in support of state governors.[112] FEMA's role is to lay out guiding principles of the DHS's National Response Framework (NRF) for all response partners when preparing for a national disaster or an emergency.[113] State and local officials have a need for the federal government to provide useful tools and assets during an emergency, especially for outlying communities, but have often not develop concrete plans for a response, despite considerable guidance from the federal government.[114] The national framework focuses on prevention, protection, mitigation, response, and disaster recovery. The goal is to build a culture of preparedness and to ensure that response plans have been established and are being maintained, as well as that emergency responders are trained and maintain their competency and expertise. FEMA, therefore, has established a National Exercise Program (NEP), which allows federal and whole community partners to organize an exercise in their community, state, agency, or organization.[115] In part, NEP's purpose is to evaluate the preparedness and readiness of the U.S. and across the interagency, and to test their ability to perform missions and functions while responding to an emergency or

[112] DHS, "Disasters: Disasters Results", 16 Jul 2015, http://www.dhs.gov/topic/disasters-results , (30 Jan 2016).
[113] Institute of Medicine (IOM). "Nationwide Response Issues After an Improvised Nuclear Device Attack: Medical and Public Health Considerations for Neighboring Jurisdictions: Workshop Summary", Washington DC, *National Academy Press*, 2014, p. 23, http://www.nap.edu/read/18347/chapter/4 , (7 Feb 2016).
[114] Ibid.
[115] Federal Emergency Management Agency (FEMA), "National Exercise Program", 23 Jun 2015, http://www.fema.gov/national-exercise-program , (2 Feb 2016).

terrorist event.[116] FEMA assists with facilitating seminars, workshops, tabletop exercise, modeling and simulations, dills, functional exercises, or full-scale exercise to foster relationships within and across agencies.[117] For the private sector, FEMA promotes preparedness through its Ready Business campaign, a nationwide initiative that provides materials to businesses to encourage continuity planning and crisis management.[118] Yet with all the assistance and education FEMA provides, none includes scenarios of an EMP and cyber attack during which communication and transportation networks have been disrupted.

Department of Health and Human Services (HHS)

Under the Pandemic and All-Hazards Preparedness Reauthorization Act, HHS is the lead agency for the National Response Framework (NRF) Emergency Support Function. The mission of HHS is to plan for all health hazards and to augment state and local capabilities when requested, as well as to coordinate all civilian and federal medical and public health responders.[119] The emergency management group (EMG) is the command and control hub for HHS and deals with situational awareness and responds to requests by interfacing with regional HHS emergency coordinators who controls

[116] Federal Emergency Management Agency (FEMA), "National Exercise Program", 23 Jun 2015, http://www.fema.gov/national-exercise-program , (2 Feb 2016).
[117] Ibid.
[118] FEMA, "Disasters: Disaster Results", 16 Jul 2015, http://www.dhs.gov/topic/disasters-results , (6 Feb 2016).
[119] Institute of Medicine (IOM). "Nationwide Response Issues After an Improvised Nuclear Device Attack: Medical and Public Health Considerations for Neighboring Jurisdictions: Workshop Summary", Washington DC, *National Academy Press*, 2014, p. 23, http://www.nap.edu/read/18347/chapter/4 , (7 Feb 2015).

activities on the ground.[120] For situational awareness, HHS coordinators rely on MedMap, which is an interactive geographic information system (GIS)-based electronic mapping application that relies on data from numerous sources during a public health emergency.[121] MedMap has the ability to display medical care sites, assembly centers, evacuation routes and evacuation centers, as well as damage-level zones.[122] Unfortunately, this tool will not be available once an EMP and cyber attack have disrupted data transfer and rendered electronic devices non-operational. HHS does not address if MedMap has been hardened against an EMP and cyber attack, or what system could be used instead to gain situational awareness to coordinate a medical and public health response. Additionally, it is unclear on how information will flow from the regional HHS emergency coordinators to the EMG if communications have been disrupted.

Office of the Assistant Secretary for Preparedness and Response (ASPR)

ASPR is the principal advisor to the HHS Secretary on all matters related to public health emergencies preventing and responding to adverse health effects of public health emergencies and disasters. ASPR delivers self-sustained medical teams for triage, transportation, decontamination, mental health care, medical care, and mortuary duty.[123] ASPR also oversees the National Disaster Medical System (NDMS) who has the mission

[120] Institute of Medicine (IOM). "Nationwide Response Issues After an Improvised Nuclear Device Attack: Medical and Public Health Considerations for Neighboring Jurisdictions: Workshop Summary", Washington DC, *National Academy Press*, 2014, p. 43, http://www.nap.edu/read/18347/chapter/4 , (7 Feb 2015).
[121] Ibid.
[122] Ibid.
[123] IOM, p. 20.

to provide personnel, supplies, and equipment to a disaster area, assist in patient movement, as well as provide medical care at hospitals in unaffected areas.[124] The NDMS is an ASPR-led collaborative partnership among HHS, the Department of Veterans Affairs (VA), the Department of Defense (DoD), and DHS to supplement state and local resources.[125] Another function of ASPR is to assist the CDC to procure medical countermeasures for the SNS so they can be delivered to the affected areas, or in case the countermeasure does not yet exist, can fund research and development.[126] ASPR has also developed numerous playbook scenarios to help implement the role of the HHS as the lead agency for public health and medical services under FEMA's NRF.[127] This allows participants to exercise decision making under a distinct set of disaster scenarios and identifies potential gaps in capabilities and assets.[128] ASPR uses various electronic systems to manage patients, such as the Joint Patient Assessment and Tracking System (JPATS), which is an important system considering that patient care may has to be coordinated through various agencies, and patients may have to move through various treatment facilities.[129] However, JPATS and NDMS have numerous shortfalls and deficiencies, and especially military transports are neither properly equipped nor positioned for a timely response and interagency communication.[130] More importantly, after an EMP and cyber attack cause a power outage, it will be difficult to move any

---

[124] Institute of Medicine (IOM). "Nationwide Response Issues After an Improvised Nuclear Device Attack: Medical and Public Health Considerations for Neighboring Jurisdictions: Workshop Summary", Washington DC, *National Academy Press*, 2014, p. 20, http://www.nap.edu/read/18347/chapter/4 , (7 Feb 2015).
[125] IOM, p. 66.
[126] IOM, p. 21.
[127] IOM, p, 43.
[128] IOM, p. 20.
[129] Ibid.
[130] Ibid.

equipment or personnel to and from an incident site. Yet rather than addressing these issues to improve response capabilities, ASPR is developing more system-based approaches.

Centers for Disease Control and Prevention (CDC)

The CDC is one of the major operating component of the HHS and is tasked to monitor the health of the nation for chronic or acute, curable or preventable diseases, as well as human error or deliberate biological attacks, to increase health security. In order to save lives and protect from health threats, the CDC provides health information, conduct research to develop countermeasures, and responds to public health emergencies. The CDC Preparedness and Response Capability supports critical infrastructure and cross-cutting research to facilitate rapid response to public health emergencies and maintains the Emergency Management Program (EMP) and the LRN.[131] The CDC's EOC with support of the EMP serves as the command center for monitoring and coordinating responses to domestic and international public health emergencies.[132] Clinicians, public health agencies and responders, as well as the general public can report potential health threats to the CDC's EMP, and CDC staff will connect callers to the appropriate CDC subject matter expert to address the health concern or threat.[133]

[131] Centers for Disease Control and Prevention (CDC), "National Snapshot of Public Health Preparedness", 2015, p. 7, http://www.phe.gov/Preparedness/mcm/phemce/Pages/default.aspx , (7 Feb 2016).
[132] CDC, p. 10.
[133] Ibid.

U.S. Food and Drug Administration (FDA)

Within the FDA, the Center for Biologics Evaluation and Research (CBER) regulates biological products for human use under applicable federal laws to ensure safe and effective use. In emergency situations, the FDA can use mechanisms such as its Emergency Use Authorization (EUA) authority to approve medical countermeasures currently not approved for public use.[134] One of these products the FDA regulates is the collection of blood and blood components used for transfusions in case of a pubic health emergency.[135] Another function of CBER is the expeditious development and licensing of products to diagnose, treat or prevent disease following exposure to a biological agent.[136] Since some biological agents may require long incubation periods for analysis and identification and as a result delay a needed response to contain a disease outbreak, CBER can approve emergency release of detection tools. CBER works with other federal agencies and private industry through the Public Health Emergency Medical Countermeasure Enterprise (PHEMCE) on projects aimed to developing new countermeasures for WMD events.[137]

It will be problematic for the FDA to assist local public health and medical communities if an EMP and cyber attacks disrupted communication and transportation systems. In order to deliver medical countermeasures such as vaccines or blood products, it will be important to communicate what is needed, the amount needed, and when these

---

[134] U.S. Food and Drug Administration (FDA), "Countering Bioterrorism and Emerging Infectious Diseases", 2015, http://www.fda.gov/BiologicsBloodVaccines/SafetyAvailability/ProductSecurity/ucm110311.htm , (24 Mar 2016).
[135] Ibid.
[136] Ibid.
[137] Ibid.

products need to arrive at the site in order to be effectively administered. Lack of communication and transportation will significantly delay the support the FDA can offer or can coordinate with local agencies.

U.S. Northern Command (NORTHCOM)

NORTHCOM is the operational command responsible for homeland defense and providing defense support to civilian authorities (DSCA).[138] If first responders are overwhelmed and additional support is needed, the governor of the affected state may choose to deploy the state's National Guard.[139] If an Emergency Management Assistance Compact (EMAC) exists, governors may rely on assistance from other states.[140] National Guard forces can be drawn from three distinct units depending on the incident and need: 1) civil support teams; 2) CBRN response; 3) and homeland response forces.[141] If additional forces are needed, the Secretary of Defense can authorize utilization of DoD resources upon request of the state governor following a Presidential disaster declaration.[142] Additional active duty and reserve forces may be integrated into the response process; yet, whether military forces would be send to support medical and public health requirements needs to be coordinated with ASPR through the MDNS.[143]

---

[138] Institute of Medicine (IOM). "Nationwide Response Issues After an Improvised Nuclear Device Attack: Medical and Public Health Considerations for Neighboring Jurisdictions: Workshop Summary", Washington DC, *National Academy Press*, 2014, p. 23-24, http://www.nap.edu/read/18347/chapter/4, (7 Feb 2016).
[139] Ibid.
[140] Johnson K, "Disaster Response: Key Legal Issues for US Northern Command", Global Legal Challenges: Command of the Commons, Strategic Communications, and Natural Disasters, p. 280.
[141] IOM, p. 23-24.
[142] Johnson, p. 278.
[143] IOM, p. 24.

There are two USNORTHCOM response units that can integrate with the National Guard forces and support DSCA missions and have the ability to provide additional emergency response capabilities.[144]

Federal Bureau of Investigation (FBI)

The FBI's number one priority is to protect the U.S. from terrorist attacks, to include WMD events such as a biological attack or EMP. As a result, the FBI is the lead law enforcement agency responsible for investigation such events.[145]In response to the recommendations of the 9/11 Commission, the FBI created a new specialized and integrated national security branch (NSB) with an operational element, the WMD Directorate or WMDD, to respond to WMD threats and investigate WMD events.[146] This directorate consists of a unique combination of law enforcement authorities, intelligence analysis capabilities, and technical subject matter expertise.[147] In order to investigate a WMD threat, the WMDD has the responsibility to collect evidence in contaminated areas, disarm hazardous devices, and provide direct command and control support for critical incidents.[148] In 2006, the FBI and Pennsylvania Department of Health epidemiologist worked on an inhalational anthrax case. Through sharing of knowledge and collaboration,

---

[144] Institute of Medicine (IOM). "Nationwide Response Issues After an Improvised Nuclear Device Attack: Medical and Public Health Considerations for Neighboring Jurisdictions: Workshop Summary", Washington DC, *National Academy Press*, 2014, p. 23-24, http://www.nap.edu/read/18347/chapter/4, (7 Feb 2016).
[145] Federal Bureau of Investigation (FBI), "Testimony: Ten Years after 9/11 and the Anthrax Attacks: Protecting Against Biological Threats", 2011, https://www.fbi.gov/news/testimony/ten-years-after-9-11-and-the-anthrax-attacks-protecting-against-biological-threats , (12 Mar 2016).
[146] Ibid.
[147] Ibid.
[148] Ibid.

as well as joint environmental sampling and testing the investigation concluded that the anthrax exposure was related to occupational exposure of contaminated animal skins found in African drums.[149] Joint efforts between public health and law enforcement are therefore imperative to efficiently address biological events.

Yet in order to investigate a biological attack a high level of communication and cooperation between public health and law enforcement needs to occur. The FBI and CDC developed the Joint Criminal and Epidemiological Investigation training program to improve the technical and scientific understanding between public health and law enforcement.[150] The course focuses on improving local response plans and information sharing protocols, and trains participants on the joint investigation principles.[151] Yet, even with increased mutual awareness and understanding on biological events, in the absence of established communication procedures as a result of an EMP and cyber attack, could limit the effectiveness of the FBI and public health investigations.[152] Additionally, FBI laboratories have to investigate and analyze evidence contaminated with a biological agent to determine the potential use of a biological weapon and work with CDC and the LRN.[153] This assumes that after an EMP and cyber attack, FBI field agents will be able to reach the outbreak site, and that agents can collect and transport hazardous evidence to the medical community and laboratories for analysis. With the collapse of the

---

[149] Institute of Medicine (IOM). "Nationwide Response Issues After an Improvised Nuclear Device Attack: Medical and Public Health Considerations for Neighboring Jurisdictions: Workshop Summary", Washington DC, *National Academy Press*, 2014, p. 23-24, http://www.nap.edu/read/18347/chapter/4, (7 Feb 2016).
[150] Anthrax Attacks: Protecting Against Biological Threats", 2011, https://www.fbi.gov/news/testimony/ten-years-after-9-11-and-the-anthrax-attacks-protecting-against-biological-threats , (12 Mar 2016).
[151] Ibid.
[152] Ibid.
[153] Ibid.

infrastructure after an EMP, besides communication, basic FBI investigation tools may not be accessible or functioning. As a result, FBI support on scene may not be available.

In summary, every public health response to a biological attack, especially after an EMP and cyber attack, require communication and coordination of resources by the interagency. Since local organizations have to maintain routine operations of medical services, a response to an infectious disease outbreak may create internal and external factors that stress the systems and disable normal functioning of agencies. Federal agencies have various response plans and resources available to support their local counterparts, but these systems and processes may become disabled in the aftermath of an EMP and cyber attack. DHS, FEMA, HHS, ASPR, and DoD NORTHCOM have crisis contingency and disaster recovery plans, but most civilian organization either do not coordinate their plans with these agencies or do not exercise them. The current systems therefore already have existing challenges with communication and coordination, which become more difficult if an EMP and cyber attack disrupt the electrical grid.

CHALLENGES DURING A RESPONSE TO A BIOLOGICAL ATTACK AFTER EMP

A response to a potential disease outbreak in a population exposed to a biological agent is a multiagency effort facing significant challenges after an EMP. After EMP and cyber attacks, parts or all of the communication infrastructure will be disabled, inhibiting effective communication from the beginning of the outbreak when collection of information is most important to identify the source and agent. Lacking important information and data from emergency responders on the ground and laboratories will be problematic because informed decision making on public health response coordination depends on the most current and complete information.

Interagency coordination

When communication channels have been disrupted, lack of information may not just impact command and control of the situation, but can also negatively impact how resources and emergency personnel are utilized, therefore complicating existing challenges. Command and control systems are uniquely compromised after an EMP relative to other terrorist events because of the massive disruption of communications, transportation, the scarcity of resources, and the inability to deploy first responders into

areas where there is a medical emergency.[154] Additionally, reconstituting command and control after it was disrupted will be difficult since additional issues may have developed by then such as public unrest. Sharing of valid and timely information is critical when coordinating a response and usually functions efficiently during routine operations, but functions poorly during dynamic and unknown environments .[155] Hierarchical networks of communication perform badly in emergencies because if any node fails, parts of the network become isolated. [156] In addition, when communications are inadequate, personnel and resources are inefficiently used and activities may be unnecessarily duplicated.[157] In times of crisis, such as during September 11, internal and external communications took priority and would have been more effective if more networking between agencies prior to the event would have occurred.[158] When communicating with other organizations, data points themselves may only provide partial information about the current situation. Massive collection of data can be of little value until the data are shared in a usable way.[159] Also, widely shared raw data will be of little use until collated and combined meaningfully.[160] With that being said, communication is more than just an exchange of information but requires interpretation to add context to the information and data provided.

---

[154] Institute of Medicine (IOM). "Nationwide Response Issues After an Improvised Nuclear Device Attack: Medical and Public Health Considerations for Neighboring Jurisdictions: Workshop Summary", Washington DC, *National Academy Press*, 2014, p. 35, http://www.nap.edu/read/18347/chapter/4 , (4 Feb 2016).
[155] Kapucu, N, "Interagency Communication Networks During Emergencies: Boundary Spanners in Multiagency Coordination", *The American Review of Public Administration*, Jun 2006, 36, p. 207.
[156] Ibid.
[157] Kapucu, p. 211.
[158] Kapucu, p. 219.
[159] Kapucu, p. 208.
[160] Ibid.

Each jurisdiction needs to set up an incident command post (ICP) that has legal authority to manage the incident, and an emergency operations center (EOC), which is the hub of communication and coordination serving the ICP.[161] The area-wide ICP should include representatives from all affected agencies, such as law enforcement, public health, fire, emergency medical services, public works, and transportation.[162] The state EOC can coordinate activities with local EOCs and area ICPs and serve as a coordinator between federal resources and local needs.[163] Lack of coordination among agencies may also be the result of local public health agencies not always being identified locally or nationally as first responders. As a result, public health officials from local agencies and on the ground during emergency operations and community drills are often left out of pre-disaster planning activities and consequently lack expertise and lack resources to appropriately assess a community's vulnerability and capacity.[164] There is the assumption that if an emergency arises, federal support can be requested and will be provided. Even if that were the case, during an EMP and cyber attack, state and federal assistance will stall because of the collapse of transportation and communication systems.

Local public health agencies often have limited staffing, but need to maintain some level of response preparedness. Developing detailed plans for every possible emergency, including an EMP event, by a local agency may not be feasible due to the

---

[161] IOM, "Nationwide Response Issues After an Improvised Nuclear Device Attack: Medical and Public Health Considerations for Neighboring Jurisdictions: Workshop Summary", Washington DC, *National Academy Press*, 2014, p. 37, http://www.nap.edu/read/18347/chapter/4 , (4 Feb 2016).
[162] IOM, p. 37.
[163] IOM, p. 38.
[164] Smith SD, "Inter-Agency Collaboration and Consequence Management: An All-Hazard Approach to Emergency Incident Response", EHS Today, 16 May 2006, http://ehstoday.com/fire_emergencyresponse/ehs_imp_17938, (6 Dec 2015).

sparse resources. Yet, certain public health issues are common to most incidents. This resulted in an "all-hazards" approach to incident management and may be more efficient and effective across agencies, even though, EMP is not included in this approach because there remains a lack of understanding that an EMP is a threat to public health and safety especially if concurrent with a biological attack.

Public Health Response

Communication across agencies is crucial for situational awareness and to coordinate the distribution of resources where needed most. Hospitals need to communicate with the local Emergency Medical Service (EMS) system relaying information on availability of beds and resources, as well as share with other hospitals in the area if they have been overwhelmed with patients.[165] Hospitals need to communicate with public health agencies and support their ongoing surveillance efforts, since electronic surveillance system are not operational. This will be challenging since local public health departments are typically short-staffed and not geared toward having one person assigned to monitor hospital facilities. There may not be a public health staff available so that hospital staff needs to keep track of suspected and confirmed cases to report to public health staff when requested. This assumes that hospital staff is trained in disease surveillance to take over this function and that they are not needed otherwise in the hospital. Surveillance may not be a priority depending on how overcrowded the emergency room is so that situational awareness may be limited to the hospital only.

[165] Keyes DC, Burstein JL, Schwartz RB, Swienton RE, *Medical Response to Terrorism*: *Preparedness and Clinical Practice,* Philadelphia, PA, Lippincott Williams & Wilkins, 2005, p. 316.

During the 2009 H1N1 pandemic, state public health systems were highly effective in managing and coordinating a complex logistical operation of receiving, staging, storing, distributing, and dispensing medical countermeasures.[166] This success was due to a fully functional communication and transportation systems, which would not be available after EMP and cyber attacks. Additionally, computer systems and the necessary technology need to be operational at the local level to manage and store the supplies received by the SNS, which will not be the case after an EMP. Some vaccines and medications need to be refrigerated and backup systems at local supply centers have only limited capabilities to maintain refrigeration. Emergency generators are usually only set up to support a few days of power, so there currently is no long-term solution in place to maintain refrigeration. This may make further distribution and tracking of supplies to local distribution centers challenging lack of visibility on how much more medical assets will be needed from the SNS to sustain a public health response. Another issues that arose during the 2009 response when there was a need for N95 particulate-filtering face-piece respirators, yet different N95 models were released from the SNS.[167] The lack of standardization of materials caused problems among recipients of those materials because individuals are fit tested to ensure maximum effectiveness of the N95 respirator, so if different models are supplied, the personal protection of healthcare workers is at risk.[168] This benefits of having a national stockpile with medical supplies and equipment is only

---

[166] Institute of Medicine (IOM), "Medical Countermeasures Dispensing: Emergency Use Authorization and the Postal Model", Workshop Summary, Washington DC. National Academy Press, 2010, p.15, http://www.ncbi.nlm.nih.gov/books/NBK53126/pdf/Bookshelf_NBK53126.pdf, (2 Dec 2015).
[167] (IOM), p.14.
[168] Ibid.

effective if the appropriate supplies are distributed. As a result, communication between local and federal authorities managing the SNS is crucial to request the appropriate supplies, which during an EMP and cyber attack will be compromised.

If preventive measures such as vaccines or treatment options are available to contain the spread of a biological agent among the population, mass vaccination campaigns need to consider vaccine safety to avoid secondary health issues that may drain medical supplies. Monitoring vaccine safety is important because large numbers of vaccines might be given in a short period of time, which may trigger more adverse events.[169] Under normal circumstances, adverse events such as possible side effects are reported to the Vaccine Adverse Event Reporting System (VAERS), which after an EMP and cyber attack will not be possible. VAERS serves as an early warning system to detect possible safety issues with U.S. vaccines by collecting and compiling adverse event reports.[170] This will be important when administering new vaccines or medications approved for emergency use by the FDA because safety data at the time of administration will be limited. In this situation it will be important to closely monitor the population to detect unexpected or concerning patterns of side effects, yet this will be challenging due to the large number of individuals that received a vaccine or medication combined with the fact that none of the surveillance tools will be operational. With that being said, healthcare staff may see secondary infections unrelated to the biological agent exposure within the community requiring additional resources for treatment.

---

[169] CDC, Vaccine Safety: Emergency Preparedness for Vaccine Safety, 27 Oct 2015, http://www.cdc.gov/vaccinesafety/ensuringsafety/monitoring/emergencypreparedness/, (6 Dec 2015).
[170] Ibid.

Based on experiences gained from the Oklahoma City bombing, the Tokyo subway sarin and the September 11 attacks, casualties may not arrive at a hospital via EMS since law enforcement, fire, and EMS personnel may not be available because they are responding to the EMP incident and the resulting public unrest. EMS staff will usually triage patients prior to arriving at the hospital and assess if special precautions need to be taken such as isolation or decontamination. As a result, hospitals may have to decontaminate patients prior to entering the hospital. Decontamination procedures are more commonly used for patients exposed to chemical and radiation materials, yet certain biological agents may warrant decontamination prior to treatment. Several biological agents can remain viable in the environment for an extended period of time, lasting from hours to days such as ricin and botulinum toxin, and anthrax spores can persist in the environment or in clothing for month or years.[171] Depending on the decontamination measure, affected people may have to be evacuated from exposed areas or quarantined to avoid further distribution of the agent. As a result, it will be important to communicate laboratory results of the agent quickly, so hospitals can prepare accordingly as well as notify other medical facilities and first responders in the affected area. Yet without the ability to communicate after an EMP this will slow down necessary quarantine procedures and unnecessarily overcrowd emergency rooms.

Once a biological agent has been identified, it is important to determine the actual exposure area in terms of location (indoors, outdoors), access (restricted or open to the public), and nature of the agent (airborne particles, solid, fume, etc.). The most common

[171] Grundmann O, "The current state of bioterrorist attack surveillance and preparedness in the U.S.", *Risk Management and Healthcare Policy*, Oct 2014, 7, 177-187, http://dx.doi.org/10.2147/RMHP.S56047, (15 Dec 2015).

method of decontamination is sealing off the affected area and treating it with a gaseous sporicide, such as chlorine dioxide, vaporized hydrogen peroxide, ethylene oxide, or paraformaldehyde.[172] Hazmat Units from the local fire department should be able to clean affected areas, but they may not be able to drive their Hazmat trucks to the location after an EMP and need to find other ways to transport their equipment to the affected areas.

Currently, emergency services have plans and processes in place to respond to biological attacks, which include detection, mitigation, and decontamination procedures. An EMP and cyber attack would impact not just communication equipment but also computers and network equipment as well as transportation. As a result, a biological attack will most likely be detected long after individuals show symptoms because it will be difficult to travel to a hospital or emergency clinic for care. By that time, any infectious agent may have spread from person to person within a population without access to treatment and supportive medical care. More importantly, it will be near impossible to track cases to determine how many individuals were affected. With the additional disruption of the transportation system, it will be difficult to coordinate a public health response among agencies and request assistance. Any plans currently in place to respond to a biological attack will most likely fail during the aftermath of an EMP, and agencies should consider incorporating scenarios that address loss of electricity and transportation for lengthy periods of time.

---

[172] Grundmann O, "The current state of bioterrorist attack surveillance and in the U.S.", *Risk Management and Healthcare Policy*, Oct 2014, 7, 177-187, http://dx.doi.org/10.2147/RMHP.S56047, (15 Dec 2015).

Communicating with the Public

The Commission to Assess the Threat to the United States from EMP Attack discusses in their report that improving protection and recovery after an EMP attack is crucial, yet providing reliable channels of information to citizens about the situation is crucial as well.[173] The purpose of public health and emergency communication is to offer information to the public that is needed to maintain health and safety and to counter potentially harmful behaviors, such as public unrest. During an emergency or crisis event, individuals experience a wide range of emotional and psychological responses that influence their perception of risk, which can lead to anger, fear, depression, and anxiety.[174] The more outrage individuals feel, the more likely they are to perceive higher levels of risk.[175] Emergency risk communication during the early stages of an outbreak or an incident may be challenging because various agency have jurisdiction over what information can be shared and with whom. The FBI is the lead agency for crisis management and has the final say over the release of information regarding the incident. FEMA, on the other hand, is the lead agency on consequence management and operational coordination of mass immunization and contingency medical support and needs to release information on prevention and disease management. Each agency has developed communication plans, yet after a concurrent EMP attack, neither one will be on site during the beginning when events unfold, so local agencies have to assume

---

[173] Foster JS, Gjedle E, Graham WR, Hermann RJ, Kluepfel H, Lawson RL, Soper GK, Wood LL, Woodard JB, "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Volume1: Executive Report 2004, 2004, p.46, http://www.empcommission.org/docs/empc_exec_rpt.pdf, 6 Feb 2016.
[174] Northwest Center for Public Health Practice (NWCPHP), "Emergency Risk Communication", p. 3, http://www.nwcphp.org/docs/cerc/toolkit/ercprint.pdf , (8 Feb 2016).
[175] Ibid.

responsibility for communicating with and informing the public. There are two communication streams to the public that need consideration: 1. explain what happened and associated risks, and 2. instructions on how to stay safe and healthy.

Communication information immediately after a biological agent has been identified is important to contain a disease and reduce the risk of it becoming an epidemic. Often, one of the concerns is the need to protect civil liberties versus the need to stop the transmission of disease. In this case, it may actually be advantageous for local public health officials who are familiar with their communities to communicate the necessary preventive measures rather than an outside agency that has no trust relationship with the local population. Local public health officials may also have a better understanding of the special needs of elderly, institutionalized persons, and people with visual and hearing impairment in their community as well as the need to translate messages into various languages commonly spoken in their population. During the September 11 attacks, the Department of Health of New York City and the Office of the Chief Medical Examiner engaged in an aggressive public information campaign via the internet to update the public on health and safety issues and available medical services.[176] This was a well-received local campaign that addressed the needs of the community but relied heavily on electronics and internet capabilities.

Communicating safety and health messages during the early stages of the event is important to reduce illness and injury cases which could have otherwise been prevented. Individuals need to maintain personal health and avoid overcrowding emergency rooms,

[176] Kapucu, N, "Interagency Communication Networks During Emergencies: Boundary Spanners in Multiagency Coordination", *The American Review of Public Administration*, Jun 2006, 36, p. 220.

which will use up resources that should be dedicated to treating highly infectious patients or other emergencies. During the 2003 major power outage in the Midwest and northeast U.S. which affected 50 million people, emergency rooms were overcrowded with carbon monoxide poisoning cases.[177] These cases resulted from inappropriate placement of generators or heaters due to the cold weather; other cases of morbidity and mortality included cold injuries, heat-related illnesses, and fire, which could have all been prevented if the public had been educated on usage and preparedness.[178] Additionally, inadequate backup generators at some wastewater treatment plants resulted in the release of sewage into surface water, so messages were distributed to alert people to avoid contact with public water areas such as beaches or rivers in an effort to reduce enteric (diarrheal) illnesses.[179] Another risk for enteric illnesses was created by the loss of refrigeration and the resulting food spoilage in homes and restaurants, and food inspectors found that some foods had reached unsafe temperatures during the power outages.[180] Enteric diseases are usually not a major concern and can easily be treated with antibiotics while staying hydrated, yet with the loss of power and transportation after an EMP attack, access to antibiotics and safe drinking water may be limited therefore making enteric illnesses life-threatening.

During a public health emergency, the CDC's EOC will stand up the Joint Information Center (JIC) with staff from the CDC who is trained in risk communication

[177] Kile JC, Skowronski S, Miller MD et al., "Impact of 2003 power outages on public health and emergency response", *Prehosp Disaster Med*,2005, 20(2), p. 94.
[178] Kile, p. 95.
[179] Kile, p. 94.
[180] Ibid.

as well as has the public health expertise to answer questions.[181] Often the JIC is supported by the Joint Information System (JIS) to integrate and coordinate available critical emergency information. The CDC also provides risk communication training online and has released the Crisis Emergency Risk Communication (CERC) document for guidance. One of the key steps toward successful communication is rapid message distribution to build credibility and reassure the public that a system is in place and that appropriate action has been taken.[182] During Hurricane Katrina, power outages were more extensive and prevented the use of electronic channels like websites, radio, and television to distribute health information.[183] Delivery of printed copies of information was not possible because CDC trucks could not reach the area because of impassable roads.[184] Instead, CDC relied on local, face-to-face channels as well as partnerships with faith-based organizations, local retailers, and shelters, to deliver health and safety messages.[185] This mode of communication is time consuming and does not aid in rapid message distribution to build credibility, and more importantly, requires large number of personnel which after an EMP and biological attack may not be available because their focus is on treating patients or distributing clean water.

Most emergency management events included pre-scripted messages to the public, which were released via phone, cell phone, internet, and TV. A healthcare system may also use telehealth capabilities to connect with their population and release general health

---

[181] Office of Public Health Preparedness and Response (PHPR), CDC Emergency Operations Center, 10 Apr 2015, http://www.cdc.gov/phpr/eoc.htm , (8 Feb 2016).
[182] CDC, "Crisis Emergency Risk Communication", 2012 edition, p. 76, http://emergency.cdc.gov/cerc/resources/pdf/cerc_2012edition.pdf, (8 Feb 2016).
[183] Ibid.
[184] Ibid.
[185] Ibid.

information or patient-specific information via phone or internet. Neither system will work after an EMP. Phones, cell phones, computers, television, and radio are all vulnerable to EMP and cannot operate without electricity. [186] In addition, satellites that operate at Low-Earth-Orbit (LEO) for communications, weather, scientific, and military purposes will also be vulnerable to an EMP attack.[187] As a result, commonly used communication methods and social media to inform the public will not be available after an EMP. The public health community often provides fliers with important information, but since electric printers will most likely not work either, no printed messages can be distributed. A public health response to a biological attack is not a single agency effort but requires coordination among agencies from the local, state, and federal levels. Components of this response effort include the telecommunication, computer and electronic equipment, as well as transportation infrastructures. An EMP and cyber attack will significantly disrupt these infrastructures so that coordination efforts will be significantly disabled. Lack of surveillance data and case information will make it difficult for local emergency responders to determine the health impact on the population. Not being able to make informed decisions on the public health response due to the lack of data and communication may cause a biological agent to spread more rapidly among a population resulting in higher morbidity and mortality. To reduce adverse health impacts, emergency responds agencies need to integrate EMP and cyber attack scenarios into their

[186] Pry PV, "Electromagnetic Pulse: Threat to Critical Infrastructure", Testimony before the Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies House Committee on Homeland Security, 8 May 2014, p. 10, http://docs.house.gov/meetings/HM/HM08/20140508/102200/HHRG-113-HM08-Wstate-PryP-20140508.pdf, (6 Dec 2015).
[187] Ibid.

response plans, so they are prepared in the event of massive loss of electricity, communication, and transportation.

CURRENT ISSUES WITH THE PUBLIC HEALTH RESPONSE

Current issues with the public health response are multifaceted and starts with a significant lack of understanding of the threat among public health professionals. Scientists and medical professionals are focused on their area of expertise and fail to understand that the threat of WMD may not that straightforward. Most public health professionals do not know what an EMP attack is and how it can impact the infrastructure to include emergency response procedures. Most response plan are written for one WMD and do not consider concurrent events to inflict mass casualties. Current education and training programs on EMP for emergency responders is limited and not readily available to everybody involved in a public health response. Additionally, protection and recovery of infrastructure needed to detect health outbreaks and assess biological agents have only been implemented sparsely. These current issues are reflective of a lack of understanding of the threat of an EMP and more education and training is needed within the public health community.

Threat Assessment

The range of actors that might attempt EMP attacks against the U.S. is quite large and ranges from states with nuclear weapons, such as Russia and China, to rogue states with limited conventional and nuclear military capabilities, such as North Korea and

terrorist groups that seek to inflict catastrophic damage on America.[188] Despite the reduction in the size of the Russian strategic nuclear force, Russia has optimized its strategic missile force to generate enhanced EMP effects.[189] A 2004 article, Russian Major General Vladimir Belous advocated an "asymmetric response" against deployed U.S. missile defense capabilities by detonating nuclear weapons pre-positioned in orbit above the U.S.[190] China's interest in EMP goes back decades, and there is concerns in Taiwan that China will use EMP weapons as part of a Chinese invasion of Taiwan.[191] An EMP attack would probably be very attractive to North Korea because its primitive economy would be less vulnerable to EMP than those of advanced industrial nations, and the use of EMP against U.S. forces stationed on the Korean Peninsula would be a suitable option.[192] According to North American Aerospace Defense Command (NORAD) Commander Adm. William Gortney, North Korea has mobile intercontinental ballistic missiles, the KN-08, armed with nuclear warheads that can strike the U.S.[193] While the KN-08 is inaccurate and may not reach a specific target in the U.S., it could be used to launch a high-altitude nuclear EMP attack.[194] Furthermore, in July 2013, a North Korean freighter transited the Gulf of Mexico with two unarmed, but nuclear capable, SA-2

---

[188] McNeill JB, Weitz R, Electromagnetic Pulse (EMP) Attack: A Preventable Homeland Security Catastrophe, 20 Oct 2008, http://www.heritage.org/research/reports/2008/10/electromagnetic-pulse-emp-attack-a-preventable-homeland-security-catastrophe, (6 Dec 2015).
[189] Schneider M, "The Emerging EMP Threat to the United States", (Fairfax, VA: National Institute Press), Nov 2007, p. 3, http://www.nipp.org/wp-content/uploads/2014/12/EMP-Paper-Final-November07.pdf, (6 Dec 2015).
[190] Schneider, p. 4.
[191] Schneider, p. 5-6.
[192] Schneider, p. 10.
[193] Cooper HF, Pry PV, "The Threat to Melt the Electric Grid", *The Wall Street Journal*, 30 Apr 2015, http://www.wsj.com/articles/the-threat-to-melt-the-electric-grid-1430436815, (6 Dec 2015).
[194] Ibid.

missiles mounted on their launchers, while Iranian freighters regularly visit their allies in Cuba and Venezuela.[195] As a result, the U.S. may be at risk for a ship-launched EMP attack.

Unlike other means of a WMD, such as chemical and biological weapons, which may require laboratory facilities and scientific expertise for safe handling, EMP weapons have much simpler requirements for handling, storage, and execution. International arms control treaties have made chemical and biological weapons the nearly exclusive prerogative of rogue states[196], even though the replication of biological agents by scientists and in makeshift laboratories is still a possibility. Yet, materials for an EMP weapon can be readily purchased at local hardware stores and can be easily applied. A larger EMP weapon could be hidden in a small van with side panels made of fiberglass, which is transparent to electromagnetic radiation.[197] If the van is parked about 5 to10 meters away from the target, the electromagnetic fields propagating to the wall of the building can be very high, especially if the walls are masonry without metal shielding.[198] Most building do not have metal shielding because it would disrupt personal cellphone

---

[195] West AB, "Texas is Working to Protect the Electrical Grid Against Natural or Man-Made Electromagnetic Pulse", Statement of Record, U.S. House Committee on Science, Space and Technology, Subcommittee on Oversight, Subcommittee on Energy, 10 Sep 2015, p. 3, http://www.ncpa.org/pdfs/15-0910%20NCPA%20Testimony-%20West-%20Texas%20is%20Working%20to%20Secure%20the%20Grid-%20House%20Science%20Subcommittees%20on%20Energy%20and%20Oversight.pdf, (6 Dec 2015).

[196] Schneider M, "The Emerging EMP Threat to the United States", (Fairfax, VA: National Institute Press), Nov 2007, p. 8, http://www.nipp.org/wp-content/uploads/2014/12/EMP-Paper-Final-November07.pdf, (6 Dec 2015).

[197] Radasky W.A., "Electromagnetic Warfare is Here: A briefcase-size radio weapon could wreak havoc in our networked world", Institute of Electrical and Electronics Engineers (IEEE), 25 Apr 2015, http://spectrum.ieee.org/aerospace/military/electromagnetic-warfare-is-here , (20 Nov 2015).

[198] Ibid.

communication once inside a building. Utilizing a nuclear device to trigger an EMP may require more technical knowledge, but given that only one device will be needed to achieve a WMD attack, a determined adversary may be willing to make the effort.

In order to cause mass destruction, the leader of a rogue state may not be motivated to use a small nuclear arsenal to launch a crippling HEMP strike against the U.S. with no resulting fatalities, but may be more plausible if used in combination with a biological attack. [199] A smaller-scale HEMP weapon requires a relatively simple design, and can be built using electrical materials and chemical explosives that are readily available for purchase.[200] It is possible to construct a suitcase-size HEMP for less than $2,000 within the capabilities of almost any nation and many terrorist groups.[201]

The former Soviet Union began its biological weapons program in the 1920s, and even though it signed onto the Biological and Toxin Weapons Convention (BWC) to discontinue the program, sources relayed that the program continued into the 1990s.[202] Today, Russian has still not allowed inspectors into all of its facilities capable of producing biological weapons.[203] The Department of State assesses that China, Iran, North Korea, Russia, and Syria continue to engage in dual-use or biological weapons-

---

[199] Wilson C., "High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessment", Congressional Research Service Report to Congress. Jul 2008, p. 20, https://www.fas.org/sgp/crs/natsec/RL32544.pdf, (3 Nov 2015).
[200] Wilson, p. 21.
[201] Ibid.
[202] Hudson Institute, "A National Blueprint For Biodefense: Leadership and Major Reform Needed to Optimize Efforts," Bipartisan Report of the Blue Ribbon Study Panel on Biodefense, Oct 2015, p. 3, at http://hudson.org/research/11824-a-national-blueprint-for-biodefense-leadership-and-major-reform-needed-to-optimize-efforts (Nov 1, 2015).
[203] Ibid.

specific activities and are failing to comply with the BWC.[204] The most likely source of a bioterrorism are not governments, but radicalized groups or individuals, both within the U.S. or outside, that intend to utilize biological agents to cause mass casualties.[205] Terrorist organizations have expressed intent to use and show some capacity to develop biological weapons.[206] Scientific expertise on acquiring biological resources and development of a biological weapon can be easily obtained through the internet. Additionally, small amounts of bacterial agents are sufficient to be cultured and grown into larger quantities in laboratories. Some agents, such as ricin, is readily available as a waste product of castor oil production, which is commonly used in the cosmetics industry.[207] Additionally, some laboratory leaders have paid insufficient attention to the details necessary to ensure laboratory biosafety and have inadvertently contributed to the biological threat.[208]

Preparing for Concurrent WMD Attacks

One of the issues with protection from biological, EMP, and cyber attacks is that reliance on technology is encouraged. The heavy reliance on health surveillance tools has been outlined previously, but it is also the response management and coordination community that utilizes electronic systems to faster and more accurate exchange data in

---

[204] Hudson Institute, "A National Blueprint For Biodefense: Leadership and Major Reform Needed to Optimize Efforts," Bipartisan Report of the Blue Ribbon Study Panel on Biodefense, Oct 2015, p. 4, at http://hudson.org/research/11824-a-national-blueprint-for-biodefense-leadership-and-major-reform-needed-to-optimize-efforts (Nov 1, 2015).
[205] Grundmann O, "The current state of bioterrorist attack surveillance and preparedness in the U.S.", *Risk Management and Healthcare Policy*, Oct 2014, 7, 177-187, http://dx.doi.org/10.2147/RMHP.S56047, (15 Dec 2015).
[206] Hudson Institute, p. 4.
[207] Grundmann, p. 182.
[208] Hudson Institute, p. 5.

an effort to improve preparedness and coordination during an incident response. Current technologies, such as incident communication networks, disease surveillance databases, and resource distribution tools have made a dramatic and positive difference in the overall preparation for and response to 9/11-like events and subsequent incidents.[209]

Software automation tools are available to support the planning, coordination and response of local governments and private sector organizations to potential emergencies and biological threats.[210] Management technologies may include functionality for event prediction, contingency planning, consequence coordination and response, post-event audit and documentation, recovery and remediation initiatives, as well as simulation and drill development.[211] During 2013, the CDC conducted two emergency notification drills with organizations that had received CDC funds for preparedness and response capabilities.[212] The goal was to test whether CDC's EOC, laboratory staff, and epidemiologists could contact each other regarding potential threats and disease outbreaks in a timely manner.[213] The target response time was 45 minutes for each drill with 84 percent of participants meeting the target in the first drill and 94 percent meeting the target in the subsequent drill.[214] The problem is not necessarily reliance on these established communication and surveillance systems, but that no efforts have been established and outlined on what to do if those systems become non-operational. Local,

---

[209] Smith SD, "Inter-Agency Collaboration and Consequence Management: An All-Hazard Approach to Emergency Incident Response", EHS Today, 16 May 2006, http://ehstoday.com/fire_emergencyresponse/ehs_imp_17938, (6 Dec 2015).
[210] Ibid.
[211] Ibid.
[212] Centers for Disease Control and Prevention (CDC), "National Snapshot of Public Health Preparedness", 2015, p. 11, http://www.phe.gov/Preparedness/mcm/phemce/Pages/default.aspx , (7 Feb 2016).
[213] Ibid.
[214] Ibid.

state, and federal emergency management plans do not include back-up plans in case these electronic systems fail during an EMP and cyber attack. Neither response plans to biological agents nor overall incident nor emergency plans—regardless of organization—contain appendices that outline how to coordinate a response when the power grid is not operational. As a result, there is a false sense of security among public health agencies and responders that they are sufficiently prepared to respond to any threat.

In 2013, the Secure High-voltage Infrastructure for Electricity from Lethal Damage Act (SHIELD Act; H.R. 2417) was introduced to Congress. The SHIELD Act assumes that the U.S. is currently ill-prepared to recovery after an EMP event and that the loss of electrical power systems will have catastrophic consequences to include potential casualties in excess of 60% of the population. As a result, the SHIELD Act would authorize the Federal Energy Regulatory Commission (FERC) to propose standards and processes for industry and government alike to address vulnerabilities of the electric grid.[215] Congress has not passed the SHIELD Act because it would require industry to harden and protect its electric infrastructure at a high cost. In addition, the Critical Infrastructure Protection Act (CIPA) was also introduced in 2013, which authorizes DHS to include EMP events in national planning scenarios and conduct outreach to educate owners and operators of critical infrastructure and emergency planners and responders on the threats by EMP events.[216] The CIPA Act passed the House in

[215] H.R.2417--Secure High-voltage Infrastructure for Electricity from Lethal Damage Act, 113th Congress, 18 June 2013, https://www.congress.gov/bill/113th-congress/house-bill/2417, (6 Dec 2015).
[216] H.R.3410—Critical Infrastructure Protection Act, 113th Congress, 30 Oct 2013, https://www.congress.gov/bill/113th-congress/house-bill/3410, (6 Dec 2015).

December 2014. Whereas some bills and plans have been established, little effort has been made so far to physically protect the electrical grid.

Education and Training

Education and training are crucial in ensuring that healthcare professionals can adequately recognize and respond to a biological attack as well as help maintain professional skills and expertise. The CDC's Office of Public Health Preparedness and Response (PHPR) conducts training and exercises to prepare state and local health departments to respond effectively during an emergency when SNS assets are deployed to ensure that vaccines and medications are received in a timely manner if local supplies have run out.[217] Yet, none of the exercises include scenarios in which the transportation and communication systems have failed. In 2014, ASPR and CDC together awarded more than $840 million in emergency preparedness and response fund to improve existing response measures.[218] Whereas the close alignment of the funding support improved efficiency in grant administration, no funding was allotted toward evaluating the supported programs. It is therefore uncertain if funding has improved levels of preparedness within organizations and whether gaps in health security preparedness such as EMP have been identified and addressed.

[217] Centers for Disease Control and Prevention (CDC), "National Snapshot of Public Health Preparedness", 2015, p. 7, http://www.phe.gov/Preparedness/mcm/phemce/Pages/default.aspx, (7 Feb 2016).
[218] CDC, p. 27.

Another problem is that emergency preparedness training is often limited to federal, state, and local agencies and first responders and not routinely to primary care providers.[219] Affected individuals may not necessarily seek care in the emergency room but consult with their primary care provider, their staff or support staff, so providing training to even the nonmedical personnel in a physician's office could aid in early detection.[220] Medical schools offer various courses on national disaster and emergencies, hazardous materials, and federal emergency response, but there is no recognized standard for training providers and these courses are not widely utilized.[221] Once providers practice in the community, they should seek opportunities to become familiar with local emergency medical series as well as local chain of command and their contact information.[222] The coordination problem between inter-governmental agencies is exacerbated by the lack of a comprehensive biodefense strategy and a unified approach to budgeting.[223]

Many public and private organizations lack the comprehensive emergency response plan that defines the roles and responsibilities of trained personnel responding to an unexpected incident.[224] Additionally, most plans do not extensively describe how to

---

[219] Dudley G, McFee RB, "Preparedness for Biological Terrorism in the United States: Project BioShield and Beyond", *The Journal of the American Osteopathic Association,* 2005, 105(9), p. 421.
[220] Ibid.
[221] Ibid.
[222] Dudley, p. 422.
[223] Hudson Institute, "A National Blueprint For Biodefense: Leadership and Major Reform Needed to Optimize Efforts," Bipartisan Report of the Blue Ribbon Study Panel on Biodefense, Oct 2015, p. 20, at http://hudson.org/research/11824-a-national-blueprint-for-biodefense-leadership-and-major-reform-needed-to-optimize-efforts (Nov 1, 2015).
[224] Smith SD, "Inter-Agency Collaboration and Consequence Management: An All-Hazard Approach to Emergency Incident Response", EHS Today, 16 May 2006, http://ehstoday.com/fire_emergencyresponse/ehs_imp_17938, (6 Dec 2015).

work side-by-side with responders from other agencies.[225] Many organizations do not know where to turn for assistance regarding emergency preparedness, nor do they have the time to stop the daily task of operating a business or service.[226] If training is mandated, agencies participating in an emergency response are often not coordinated in their efforts.[227] During the 2003 power outage in the Midwest and Northeast U.S., public health and emergency responders noted that there was a lack of preparations and resources for coping with public anxiety and behavioral issues, lack of training in dealing with power outage emergencies, and lack of planning for multiple-system failures across states when relying on aid from nearby communities.[228] In addition, the assumption is that healthcare staff trained in emergency response and disease surveillance will be in the right place at the right time to respond to a biological event after an EMP. Yet, with the collapse of the transportation infrastructure, trained staff may not be able to reach their hospital or public health facility in a timely manner or at all. Under normal circumstances, it may make sense to only train a selected few individuals as emergency essential personnel who can then direct the remaining staff, but after an EMP this concept will not work. With that being said, all hospital and public health staff should prepare for emergencies and catastrophic events in some capacity to take over duties if colleagues cannot reach the medical facility.

---

[225] Smith SD, "Inter-Agency Collaboration and Consequence Management: An All-Hazard Approach to Emergency Incident Response", EHS Today, 16 May 2006, http://ehstoday.com/fire_emergencyresponse/ehs_imp_17938, (6 Dec 2015).
[226] Ibid.
[227] Ibid.
[228] Kile JC, Skowronski S, Miller MD et al., "Impact of 2003 power outages on public health and emergency response", *Prehosp Disaster Med*,2005, 20(2), p. 96.

There also is a lack of understanding what an EMP attack is and how it can impact existing infrastructure to include the emergency response systems. Without this knowledge and threat awareness, public health professionals will be less likely to make EMP training a priority or necessity.

Protect and Recover of Critical Infrastructure

Biological threats are real, whether naturally occurring or man-made through bioterrorism event, and various protective measures are in place or could be implemented on short notice. Incidents of biological threats, such as the anthrax exposure at the DC post office in 2001, have been well documented and communicated to the public making them less of a concern to the public. Yet, the success of mitigating potential outbreaks is in part due to the heavy reliance on disease surveillance tools and rapid testing capabilities by the public health community. At the same time, EMP threats are not taken seriously and only limited protective measures have been implemented, especially in the civilian sector. With that being said, the electrical grid and critical infrastructure are left vulnerable to an EMP and loss of power for weeks or months if not longer may be the consequence if an attack should occur. This in turn, will affect the public health capabilities and can disrupts detection and preventive measures causing highly contagious agents otherwise readily contained to become biological threats. Yet, it seems that neither the public nor Congress make this connection and are reluctant to emphasize protective measures to mitigate power loss as a result of an EMP.

State and local governments have made sparse efforts to incorporate EMP preparedness and response measures into their response plans. Alaska and some New

York municipal organizations include EMP preparedness measures in their response plans.[229] Whereas most of these plans address survivability measures, they do not include actual hardening of electricity-based infrastructure. The variability in how local and state governments address their needs for protective measures against an EMP attack is often due to lack of knowledge on the impact of an EMP on the electrical grid. The DoD, on the other hand, has continuously prepared for an EMP over the past decade and continues to invest in hardening its military infrastructure. In 2012, the DoD spent $22.1 million to harden Minuteman missiles against EMP attacks.[230] The NORAD Commander recently announced that NORAD headquarters which provides early warning and command and control for the defense of the continental U.S. against nuclear attack has been moved from Peterson Air Force Base in Colorado back into Cheyenne Mountain because going underground ensured protection against EMP.[231] In addition, the Pentagon awarded a $700 million contract to upgrade its electronics through 2020.[232] With that being said, most computers and electronic equipment in DoD is still vulnerable, so an EMP could still severely degrade the ability of Armed Forces to operate effectively.

---

[229] Carfano JJ, Spring B, Weitz R, "Before the Lights Go Out: A Survey of EMP Preparedness Reveals Significant Shortfalls", 15 Aug 2011, http://www.heritage.org/research/reports/2011/08/before-the-lights-go-out-a-survey-of-emp-preparedness-reveals-significant-shortfalls, (6 Dec 2015).
[230] Ibid.
[231] Cooper HF, Pry PV, "The Threat to Melt the Electric Grid", *The Wall Street Journal*, 30 Apr 2015, http://www.wsj.com/articles/the-threat-to-melt-the-electric-grid-1430436815, (6 Dec 2015).
[232] Ibid.

If an EMP attack would occurr, near-term recovery would prove impossible because of America's dependence on the electrical grid.[233] The complexity is exacerbated by the interdependence of the grid and other critical infrastructures such as telecom, natural gas and oil, water supply systems, banking and finance, and transportation.[234] Restarting the grid, also known as "black start", requires communication and energy transport, which both depend on electricity and can therefore not be performed. Black start capacity could be extended with at-site fuel switching capability.[235] Transformers and generators are not readily available for purchase and repairs may take months.[236] Instead, modernizing and hardening of the electrical grid would limit some of the destructive effects on the power grid. Engineering approaches such as shielded enclosures, grounding techniques, current limiting line filters, terminal protection devices, and cable management are costly if added to an existing grid, yet most cost effective if integrated into the design phase of new grid developments.

Current grid protection measures require state legislator involvement since they have regulatory authority over the systems, so states can require power companies to install blocking devices and other technologies to protect against EMP or geomagnetic

---

[233] McNeill JB, Weitz R, Electromagnetic Pulse (EMP) Attack: A Preventable Homeland Security Catastrophe, 20 Oct 2008, http://www.heritage.org/research/reports/2008/10/electromagnetic-pulse-emp-attack-a-preventable-homeland-security-catastrophe, (6 Dec 2015).

[234] Electric Power Research Institute (EPRI), "Enhancing Distribution Resiliency: Opportunities for Applying Innovative Technologies", Jan 2013, p. 3, http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001026889&Mode=download, (6 Dec 2015).

[235] Foster JS, Gjelde E, Graham WR, Hermann RJ, Kluepfel HM, Lawson RL, Soper GK, Wood LL, Woodard JB, "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures" Apr 2008, p. 57, http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pd, (6 Dec 2015).

[236] Foster, p. 50.

disturbances.[237]According to the National Governors Association, 70 percent of transmission lines and transformers are at least 25 years old, 60 percent of circuit breakers are at least 30 years old, and much of the infrastructure was designed in the 1950s making the entire grid vulnerable to EMP.[238] One of the major issues that limits grid modernization is that the current spending of $34 billion per year to maintain and partially upgrade the grid will have to be increased by $8 to $16 billion per year through 2030 to ensure a fully modernized grid.[239] A modern grid would address cyber security as well as EMP as well as increased consumer demand, so governors have an important role in moving this agenda forward and making it a funding priority.

The public health response to a biological attack during the aftermath of an EMP and cyber attack is facing considerable challenges. One of the most important issues is that EMP threat awareness is almost non-existing in the medical and public health community. There is a failure to understand that the disruption of the communication and transportation infrastructure will significantly impact surveillance and emergency response efforts. As a result, EMP scenarios are not integrated into response plans leaving the public health community underprepared if such an event should occur. The limited training that is available through federal agencies is not offered to all emergency responders and is not a mandatory as part of the annual training curriculum. Additionally, protection and recovery of infrastructure is limited

---

[237] Bergal J, "States Work to Protect Electric Grid", 27 Feb 2015, http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2015/2/27/states-work-to-protect-electric-grid , (15 Jan 2016).
[238] National Governors Association (NGA), "Governors' Guide to Modernizing the Electric Power Grid", Mar 2014, p.1, http://www.nga.org/files/live/sites/NGA/files/pdf/2014/1403GovernorsGuideModernizingElectricPowerGrid.pdf , (15 Jan 2016).
[239] NGA, p. 2.

through sparse research funding and limited funding to upgrade the states' electrical grid. Congress and state governors have not made EMP protection a priority issue and have not mandated comprehensive improvements to the current infrastructure. The majority of these issues is related to a lack of understanding the threat of an EMP, especially within the public health community, and requires an open dialog on this topic.

CONCLUSION AND RECOMMENDATIONS

The U.S. heavily depends on the electrical grid and critical infrastructure for survival and daily operations. At the same time, the majority of the electricity-based infrastructure is vulnerable to an EMP attack that could disrupt the shut down the entire grid. This threat is real because the number of U.S. adversaries with intent and capability of a nuclear EMP attack is greater than during the Cold War, yet the public does not seem to recognize that threat. EMP is often perceived as science fiction, rather than WMD, and the lack of understanding what an EMP is and its impact on the U.S. infrastructure and human survival in the long-term will prevent the implementation of much needed preventive measures. EMP events have already occurred in the U.S., even though at a smaller scale, and it took weeks or months to fully restore the electrical grid. Yet these events are not being recognized as EMP but rather "power outages" which are not comparable events. EMP and cyber attacks do not cause initial mass destruction to the environment and population like a nuclear WMD would to, yet it is the cascade and potential multiplication of effects that can be catastrophic.[240] Combined with a biological attack, EMP and cyber attacks could amplify the effects of a biological attack because the loss of the electrical grid and electricity-based critical infrastructure could disable detection and response efforts as well as disrupt interagency efforts to coordinate a medical response.

---

[240] Frankel M, Scouras J, DeSimone A, "Assessing the Risk of Catastrophic Cyber Attack: Lessons from the Electromagnetic Pulse Commission", Research Note, Johns Hopkins Applied Physics Laboratory, 2015, p. 9, http://www.jhuapl.edu/newscenter/publications/pdf/AssessingtheRiskofCatastrophicCyberAttack.pdf, (6 Dec 2015).

One could argue that after EMP and cyber attacks adversaries may not see the need for a biological attack because lack of electricity, water and food supplies alone will result in significant loss of lives. Also, the emphasize on supporting the medical and public health community may be short lived since food and water supplies, as well as restoring electricity and critical infrastructure may have a higher priority and take away resources and personnel from the medical response. It is also unknown how an EMP attack will impact the grid since some systems may have been protected or hardened without being impacted by the EMP and cyber attacks. Currently, there is no requirement for agencies to keep track of any systems improvements that would protect against EMP, so it is unclear, who and what systems will be disrupted. During previous major power outages across state lines, telecommunication systems continued to function at some capacity so the impact may not be as catastrophic as anticipated or worse. The public perceives a power outage or EMP commonly as a nuisance and inconvenience rather than a threat to their survival, so besides lack of federal support, the public may not see the needs to support public health efforts until the first patients arrive at the hospital and an epidemic becomes unmanageable. Yet, in order to recover from these attacks and to restore order and electricity, healthy people need to be available who can contribute to the recovery process. Also, the domestic consequences of a biological attack concurrent with EMP and cyber attacks may be so devastating that the U.S. military may not be able to organize a coherent retaliatory strike against the aggressor; especially because it may

be too difficult to rapidly determine the perpetrator of these attacks.[241] The ability to identify and contain the spread of a biological agent in a population to reduce morbidity and mortality will aid in the overall recovery process, and it should be a major focus of emergency response plans to incorporate preparations for concurrent WMD attacks. More importantly, the delivery of aid in a chaotic post-EMP environment will be impossible without robust pre-disaster planning that integrates federal, state, local, private, and non-governmental organizations.[242] As a result, agencies involved in medical emergency response need to consider adding EMP and cyber attack scenarios to their response plans.

There are numerous issues that need to be considered when preparing for concurrent biological, EMP, and cyber attacks of which some were also addressed by the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack in their report. Some of the major issues to consider are the following:

1) Threat awareness: The Commission recommended that individuals in positions of authority and responsibility be trained to recognize an EMP attack and understand the wide range of effects it can produce as well as analyze the status of the infrastructure systems.[243] The report does not specifically include medical and public health

---

[241] McNeill JB, Weitz R, Electromagnetic Pulse (EMP) Attack: A Preventable Homeland Security Catastrophe, 20 Oct 2008, http://www.heritage.org/research/reports/2008/10/electromagnetic-pulse-emp-attack-a-preventable-homeland-security-catastrophe, (6 Dec 2015).

[242] Carafano JJ, Weitz R, "EMP Attacks—What the U.S. Must Do Now", 17 Now 2010, http://www.heritage.org/research/reports/2010/11/emp-attacks-what-the-us-must-do-now , 8 Feb 2016.

[243] Foster JS, Gjedle E, Graham WR, Hermann RJ, Kluepfel H, Lawson RL, Soper GK, Wood LL, Woodard JB, "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Volume1: Executive Report 2004, 2004, p.13, http://www.empcommission.org/docs/empc_exec_rpt.pdf, 6 Feb 2016.

professionals, but recommends awareness for all leaders and those with authority. As a result, this topic is not seen as an urgent or not a large enough threat requiring the attention of the medical community and may be a missed opportunity by the Committee to draw medical leadership into the EMP discussion. Congress has reassumed its leadership role on EMP and held hearings in 2008, but its ability to compel executive branch action in this area is limited.[244]More research will be needed to assess the type of damage to the U.S. infrastructure based on the EMP weapon utilized. Also more information will be needed on the knowledge and expertise potential adversaries have acquired on EMP, cyber, and biological weapons to determine the current threat. Yet, the information currently available should suffice to educate those not familiar with the impact of EMP and cyber attacks and should be integrated into current response and training plans.

2) Medical preparedness by the interagency: The Commission also recommends that training, procedures, simulations, and exercise must be developed and carried out to address the effects of an EMP, since the immediate aftermath is not the time to begin planning for an effective response.[245] Agencies tasked to provide emergency response and medical care are heavily dependent on electronics, telecommunications, and information technology to conduct surveillance and coordinate their response. These technological innovations have brought great benefits, but also make the U.S. vulnerable

[244] McNeill JB, Weitz R, "Electromagnetic Pulse (EMP) Attack: A Preventable Homeland Security Catastrophe", 20 Oct 2008, http://www.heritage.org/research/reports/2008/10/electromagnetic-pulse-emp-attack-a-preventable-homeland-security-catastrophe, (6 Dec 2015).

[245] Foster JS, Gjedle E, Graham WR, Hermann RJ, Kluepfel H, Lawson RL, Soper GK, Wood LL, Woodard JB, "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Volume1: Executive Report 2004, 2004, p.13-14, http://www.empcommission.org/docs/empc_exec_rpt.pdf, (6 Feb 2016).

to an EMP and cyber attack. Telecommunication is important for personnel within each agency and local responders to coordinate support and recovery efforts. To offset the temporary loss of electric power, telecommunications sites started to utilize a mix of batteries, mobile generators, and fixed-location generators, but these typically only provide backup power from 4 to 72 hours.[246] These temporary fixes may be sufficient for a power outage but not an EMP attack, which can cause a power outage to last for months. Additionally, a concurrent biological attack may be identified after an incubation period of a few days to weeks, so backup generators need to provide longer periods of power to enable surveillance and case identification. With that being said, comprehensive preparedness by the interagency to respond to a concurrent EMP, cyber and biological attack remains underdeveloped.

3) Protection and recover of critical infrastructure: The Commission points out that very little research and development has been spent to address EMP- related system response protection and recovery issues.[247]It is impractical to protect the entire electrical power system from damage by an EMP attack because there are too many components of too many different types, but it is practical to determine which systems need to remain operational and reduce the impact on the systems and reduce their recovery time.[248]Yet, government support for research to develop EMP response measures and devices to harden the electronic infrastructure has been limited because EMP is still not a priority issue. Since an EMP attack is most likely to occur via a ballistic missile armed with a

---

[246] Foster JS, Gjedle E, Graham WR, Hermann RJ, Kluepfel H, Lawson RL, Soper GK, Wood LL, Woodard JB, "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Volume1: Executive Report 2004, 2004, p.28, http://www.empcommission.org/docs/empc_exec_rpt.pdf, (6 Feb 2016).
[247] Foster, p. 16.
[248] Foster, p. 20.

nuclear warhead, the suggestion has been made to build a missile defense system that would intercept and destroy the missile before it could cause an EMP.[249] This would require Congress to send a clear message that the U.S. is serious about protecting itself against EMP, while justifying large amounts of resources and funding being dedicated towards this effort.

Biological, EMP, and cyber attacks, whether applied individually or combined, will not cause the initial mass destruction other WMD would cause, even though that does not make them less of a threat. Cascading failure of critical infrastructure will affect civilian and military capabilities to support our survival and compromise recovery. As a result, efforts to mitigate the effect of these concurrent attacks need to be well planned or coordinated. Interagency and multi-disciplinary efforts are needed to respond to developing threats and issues. Comprehensive threat assessment and scenario planning for EMP and cyber attacks remain underdeveloped and so does a combined attack with a biological agent. As a result, local, state, and federal agencies need to incorporate EMP, cyber, and concurrent WMD events in their response planning and exercises. Key steps to mitigate the catastrophic effects of an EMP attack are to prevent an attack in the first place, prepare so personnel can respond after an attack, protect the critical infrastructure to limit the impact, and recover after an attack to restore power and critical infrastructure.

[249] McNeill JB, Weitz R, "Electromagnetic Pulse (EMP) Attack: A Preventable Homeland Security Catastrophe", 20 Oct 2008, http://www.heritage.org/research/reports/2008/10/electromagnetic-pulse-emp-attack-a-preventable-homeland-security-catastrophe, (6 Dec 2015).

REFERENCES

Adams, C (2015). How safe is "the cloud"? *The Straight Dope*. Retrieved on 6 Jan 2016 at http://www.straightdope.com/columns/read/3228/how-safe-is-the-cloud.

Association of State and Territorial Health Officials (ASTHO). (2015). Emergency Use Authorization Toolkit: Strategic National Stockpile. Retrieved on 30 Nov 2015 http://www.astho.org/Programs/Preparedness/Public-Health-Emergency-Law/Emergency-Use-Authorization-Toolkit/Strategic-National-Stockpile-Fact-Sheet/.

Bergal J. (2015). States Work to Protect Electric Grid. Retrieved on 15 Jan 2016 at http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2015/2/27/states-work-to-protect-electric-grid .

Carfano JJ, Spring B, Weitz R. (2011).Before the Lights Go Out: A Survey of EMP Preparedness Reveals Significant Shortfalls. Retrieved on 6 Dec 2015 at http://www.heritage.org/research/reports/2011/08/before-the-lights-go-out-a-survey-of-emp-preparedness-reveals-significant-shortfalls.

Carafano JJ, Weitz R. (2010). EMP Attacks—What the U.S. Must Do Now. Retrieved on 8 Feb 2016 at http://www.heritage.org/research/reports/2010/11/emp-attacks-what-the-us-must-do-now .

Centers for Disease Control and Prevention (CDC). (2001). Recognition of Illness Associated with the Intentional Release of a Biologic Agent. *Morbidity and Mortality Weekly Report*, 50(41), 893-7.

CDC. (2014). Emergency Preparedness and Response: The Laboratory Response Network Partners in Preparedness. Retrieved on 3 Dec 2015 http://emergency.cdc.gov/lrn/.

CDC. (2015). Vaccine Safety: Emergency Preparedness for Vaccine Safety. Retrieved on 6 Dec 2015 at http://www.cdc.gov/vaccinesafety/ensuringsafety/monitoring/emergencypreparedness/.

CDC. (2015). National Snapshot of Public Health Preparedness. Retrieved on 7 Feb 2015 at http://www.phe.gov/Preparedness/mcm/phemce/Pages/default.aspx .

CDC. (2012). Crisis Emergency Risk Communication. Retrieved on 8 Feb 2016 at http://emergency.cdc.gov/cerc/resources/pdf/cerc_2012edition.pdf.

CDC (2015). National Syndromic Surveillance Program (NSSP), BioSense Platform, State and Local Support: Cooperative Agreement. Retrieved on 25 Nov 2015 at http://www.cdc.gov/nssp/biosense/cooperativeagreement.html.

Cooper HF, Pry PV. (2015). The Threat to Melt the Electric Grid. *The Wall Street Journal*. Retrieved on 6 Dec 2015 at http://www.wsj.com/articles/the-threat-to-melt-the-electric-grid-1430436815.

Department of Homeland Security (DHS). (2015). *About DHS: Our Mission*. Retrieved on 30 Jan 2016 at http://www.dhs.gov/our-mission.

DHS (2015). *Mission: Building a Resilient Nation*. Retrieved on 30 Jan 2016 at http://www.dhs.gov/building-resilient-nation.

DHS (2014). *National Emergency Communications Plan*. Retrieved on 2 Feb 2016 at http://www.dhs.gov/sites/default/files/publications/2014%20National%20Emergency%20Communications%20Plan_October%2029%202014.pdf.

Dudley G, McFee RB. (2005). Preparedness for Biological Terrorism in the United States: Project BioShield and Beyond. *The Journal of the American Osteopathic Association,* 105(9), 417-424.

Electric Power Research Institute (EPRI). (2013). Enhancing Distribution Resiliency: Opportunities for Applying Innovative Technologies. Retrieved on 6 Dec 2015 at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001026889&Mode=download.

Federal Bureau of Investigation (FBI). (2011). Testimony: Ten Years after 9/11 and the Anthrax Attacks: Protecting Against Biological Threats. Retrieved on 12 Mar 2016 at https://www.fbi.gov/news/testimony/ten-years-after-9-11-and-the-anthrax-attacks-protecting-against-biological-threats.

Federal Emergency Management Agency (FEMA). (2015). *National Exercise Program.* Retrieved on 2 Feb 2016 at http://www.fema.gov/national-exercise-program.

Federal Emergency Management Agency (FEMA). (2002). *Managing the Emergency Consequences of Terrorist Incidents: Interim Planning Guide for State and Local Governments*. Retrieved on Oct 12, 2015 https://www.fema.gov/pdf/plan/managingemerconseq.pdf.

Foster JS, Gjedle E, Graham WR, Hermann RJ, Kluepfel H, Lawson RL, Soper GK, Wood LL, Woodard JB. (2004). *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Volume1: Executive Report 2004*. Retrieved on 2 Nov 2015 http://www.empcommission.org/docs/empc_exec_rpt.pdf.

Foster JS, Gjelde E, Graham WR, Hermann RJ, Kluepfel HM, Lawson RL, Soper GK, Wood LL, Woodard JB. (2008). Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures. Retrieved on 6 Dec 2015 at http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pd.

Frankel M, Scouras J, DeSimone A. (2015). "Assessing the Risk of Catastrophic Cyber Attack: Lessons from the Electromagnetic Pulse Commission." Research Note. Johns Hopkins Applied Physics Laboratory. Retrieved on 6 Dec 2015 at http://www.jhuapl.edu/newscenter/publications/pdf/AssessingtheRiskofCatastrophicCyberAttack.pdf.

Graham *et al*. (2008). "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures." Retrieved on 20 Nov 2015 at http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf.

Grundmann O. (Oct 2014). "The current state of bioterrorist attack surveillance and preparedness in the U.S.". *Risk Management and Healthcare Policy*, 7, 177-187, http://dx.doi.org/10.2147/RMHP.S56047.

Hawk C, Kasushiva A. (Oct 2014). Cybersecurity and the Smart Grid. *The Electricity Journal*, 27(8), 84-95, doi:10.1016/j.tej.2014.08.008.

H.R.2417 (2013). Secure High-voltage Infrastructure for Electricity from Lethal Damage Act.113th Congress. Retrieved on 6 Dec 2015 at https://www.congress.gov/bill/113th-congress/house-bill/2417.

H.R.3410 (2013). Critical Infrastructure Protection Act.113th Congress. Retrieved on 6 Dec 2015 at https://www.congress.gov/bill/113th-congress/house-bill/3410.

Hudson Institute. (Oct 2015). A National Blueprint For Biodefense: Leadership and Major Reform Needed to Optimize Efforts. Bipartisan Report of the Blue Ribbon Study Panel on Biodefense. Retrieved on Nov 1, 2015 http://hudson.org/research/11824-a-national-blueprint-for-biodefense-leadership-and-major-reform-needed-to-optimize-efforts.

Institute of Medicine (IOM). (2014). *Nationwide Response Issues After an Improvised Nuclear Device Attack: Medical and Public Health Considerations for Neighboring Jurisdictions: Workshop Summary*. Washington, DC: National Academies Press. Retrieved on Jan 20, 2016 at http://www.nap.edu/read/18347/chapter/4.

Institute of Medicine (IOM) and National Research Council (NRC). (2013). *Technologies to Enable Autonomous Detection for BioWatch: Ensuring Timely and Accurate Information for Public Health Officials. Workshop Summary.* Washington, DC: National Academies Press. Retrieved on Nov 2, 2015 at http://www.ncbi.nlm.nih.gov/books/NBK201349/.

Institute of Medicine (IOM) and National Research Council (NRC). (2011). *BioWatch and public health surveillance: Evaluating systems for the early detection of biological threats. Abbreviated version.* Washington, DC: The National Academies Press.

Institute of Medicine (IOM). (2010). *Medical Countermeasures Dispensing: Emergency Use Authorization and the Postal Model*. Workshop Summary. Washington DC. National Academy Press. Retrieved on 2 Dec 2015 http://www.ncbi.nlm.nih.gov/books/NBK53126/pdf/Bookshelf_NBK53126.pdf.

John S. Foster et al. (2004). Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Volume 1: Executive Report. Retrieved on Oct 12, 2015 http://empcommission.org/docs/empc_exec_rpt.pdf.

Johnson K. Disaster Response: Key Legal Issues for US Northern Command. *Global Legal Challenges: Command of the Commons, Strategic Communications, and Natural Disasters*. Vol. 83, p. 278-291.

Kapucu, N. (2006). Interagency Communication Networks During Emergencies: Boundary Spanners in Multiagency Coordination. *The American Review of Public Administration*, 36, 207-225.

Keyes DC, Burstein JL, Schwartz RB, Swienton RE. (2005). *Medical Response to Terrorism*: *Preparedness and Clinical Practice.* Philadelphia, PA: Lippincott Williams & Wilkins.

Kile JC, Skowronski S, Miller MD et al. (2005). Impact of 2003 power outages on public health and emergency response. *Prehosp Disaster Med*, 20(2), 93-97.

Levi, J. (2011). *Ready or Not?: Protecting the Public's Health from Diseases, Disasters, and Bioterrorism.* Darby, PA: DIANE Publishing.

Lim DV, Simpson JM, Kearns EA, Kramer MF. (2005). Current and Developing Technologies for Monitoring Agents of Bioterrorism and Biowarfare. *Clinical Microbiology Reviews,* 18(4), 583-607.

Lindler LE, Lebeda FJ, Korch GW. (2005). Biological Weapons Defense: Infectious Diseases and Counterbioterrorism. Humana Press: Totowa, New Jersey.

McNeill JB, Weitz R. (2008). Electromagnetic Pulse (EMP) Attack: A Preventable Homeland Security Catastrophe. Retrieved on 6 Dec 2015 at http://www.heritage.org/research/reports/2008/10/electromagnetic-pulse-emp-attack-a-preventable-homeland-security-catastrophe.

National Governors Association (NGA), (2014). Governors' Guide to Modernizing the Electric Power Grid. Retrieved on 15 Jan 2016 at http://www.nga.org/files/live/sites/NGA/files/pdf/2014/1403GovernorsGuideModernizingElectricPowerGrid.pdf.

Northwest Center for Public Health Practice (NWCPHP). *Emergency Risk Communication*. Retrieved on 8 Feb 2016 at http://www.nwcphp.org/docs/cerc/toolkit/ercprint.pdf.

Office of Public Health Preparedness and Response (PHPR). (2015). CDC Emergency Operations Center. Retrieved on 8 Feb 2016 at http://www.cdc.gov/phpr/eoc.htm.

Pry PV. (2014). Electromagnetic Pulse: Threat to Critical Infrastructure. Testimony before the Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies House Committee on Homeland Security. Retrieved on 6 Dec 2015 at http://docs.house.gov/meetings/HM/HM08/20140508/102200/HHRG-113-HM08-Wstate-PryP-20140508.pdf.

Public Health Emergency (PHE)—Department of Health and Human Services (HHS). (2009). Telehealth Report to Congress. Retrieved on 1 Nov 2015 http://www.phe.gov/Preparedness/legal/pahpa/Documents/telehealthrtc-091207.pdf.

Radasky W.A. (2015). Electromagnetic Warfare is Here: A briefcase-size radio weapon could wreak havoc in our networked world. Institute of Electrical and Electronics Engineers (IEEE). Retrieved on 20 Nov 2015 at http://spectrum.ieee.org/aerospace/military/electromagnetic-warfare-is-here.

Russell PK. (2007). "Project BioShield: What Is It, Why It Is Needed, and Its Accomplishments So Far". *Clinical Infectious Diseases,* 45(S1), S68-S72.

Schneider M, (2007). The Emerging EMP Threat to the United States. Fairfax, VA: National Institute Press. Retrieved on 6 Dec 2015 at http://www.nipp.org/wp-content/uploads/2014/12/EMP-Paper-Final-November07.pdf.

Securethegrid, (2015). EMP: Technology's Worst Nightmare. Retrieved on 30 Oct 2015 at http://securethegrid.com/emp-technologys-worst-nightmare/ .

Shea DA, Lister SA. (2003). "The BioWatch Program: Detection of Bioterrorism." Congressional Research Service *Report to Congress*. Retrieved on 3 Nov 2015 at http://www.fas.org/sgp/crs/terror/RL32152.html .

Smith SD. (2006). "Inter-Agency Collaboration and Consequence Management: An All-Hazard Approach to Emergency Incident Response." *EHS Today*. Retrieved on 6 Dec 2015 at http://ehstoday.com/fire_emergencyresponse/ehs_imp_17938.

Thavaselvam D, Vijayaraghavan R. (2010). Biological warfare agents. *Journal of Pharmacy and Bioallied Sciences*, 2(3), 179-188. http://doi.org/10.4103/0975-7406.68499.

The Heritage Foundation (2015). "Think Ahead: Preparing for the Threat of Our Wired World." Retrieved on 2 Nov 2015 at http://www.heritage.org/issues/missile-defense/electromagnetic-pulse-attack.

U.S. Food and Drug Administration (FDA). (2015). Countering Bioterrorism and Emerging Infectious Diseases. Retrieved on 24 Mar 2016 at http://www.fda.gov/BiologicsBloodVaccines/SafetyAvailability/ProductSecurity/ucm110311.htm.

Valdivia-Granda WA. (2012). Biodefense Oriented Genomic-Based Pathogen Classification System: Challenges and Opportunities. *Journal of Bioterrorism & Biodefense*, 3(1), 1000113.

West AB. (2015). Texas is Working to Protect the Electrical Grid Against Natural or Man-Made Electromagnetic Pulse. Statement of Record. U.S. House Committee on Science. Space and Technology. Subcommittee on Oversight. Subcommittee on Energy. Retrieved on 6 Dec 2015 at http://www.ncpa.org/pdfs/15-0910%20NCPA%20Testimony-%20West-%20Texas%20is%20Working%20to%20Secure%20the%20Grid-%20House%20Science%20Subcommittees%20on%20Energy%20and%20Oversight.pdf.

Wilson C. (Jul, 2008). "High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessment". Congressional Research Service *Report to Congress*. Retrieved on 3 Nov 2015 at https://www.fas.org/sgp/crs/natsec/RL32544.pdf .