Concurrent Biological, Electromagnetic Pulse and Cyber-attacks: The Ultimate Interagency Response Challenge

by Patricia Rohrbeck

The Perfect Storm

The critical infrastructure components of an advanced society—telecommunications, transportation, banking and finance, petroleum and natural gas, food and water, public health and healthcare, and security—have at least one feature in common: All depend upon electrical and cyber power. Two well-known threats— electromagnetic pulse (EMP) and cyberattack—could, operating in tandem, disable not just a significant portion of the electrical grid and critical infrastructure, but also the network-centric military response to such an attack. If a high-altitude EMP attack were paired with both a large-scale cyberattack and a biological attack, the resulting challenge to the interagency could surpass anything the interagency is currently structured or equipped to respond to.

Current preparedness and response plans focus primarily on one weapons of mass destruction (WMD) attack mode at a time. However, an EMP and cyberattack would amplify the effects of a biological attack and vice-versa. The ramifications of such a combination of attacks are staggering:

- Detection of biological agents could be disabled after an EMP and cyberattack 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 or process suspected specimens to identify potentially hazardous biological agents. Without a timely response, the spread of disease in a population may not be contained during its early stages and could lead to 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.

U.S. Air Force Lieutenant Colonel Patricia Rohrbeck serves at the 779th Medical Group, Joint Base Andrews, Maryland. She holds a Dr.P.H. degree in Public Health Practice and received a M.S. degree in WMD Studies as a National Defense University Countering WMD Graduate Fellow.

- 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, which may disrupt how public health officials assess the ongoing health threat and how treatment is prioritized.

- Medical supplies and pharmaceuticals may not be delivered in the same dose and format requiring adjustments before administering. Thus, disruption of resource supply chains may cause a delay in patient treatment and care.

- The absence of telecommunication would severely disrupt interagency coordination efforts. 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, leaving local agencies to lead the response. Local public health and healthcare personnel may lack the necessary training to coordinate a medical response to a biological agent. Thus, response efforts may be executed inefficiently.

These catastrophic attack combinations are not merely the stuff of science fiction. Adversaries of the U.S. certainly have the capability to execute EMP, cyber, and biological attacks. Some adversaries have the capability to execute them on a very large scale. In this latter case, the decision not to execute these large-scale attacks in tandem would be more reflective of the adversary's policy preference rather than the adversary's ability. Hence, failure to prepare against an attack combination cannot simply be dismissed as unthinkable. On the contrary, now is the time for the interagency to think about just such an eventuality.

One could argue that after EMP and cyberattacks, adversaries may not see the need for a biological attack because the lack of electricity, water, and food supplies alone will result in significant loss of lives. While that certainly is true, it is likewise the case that 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. A biological attack in the wake of an EMP attack or cyberattack or both could render an effective response impossible and lead to societal collapse.

Understanding the Threat

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.[1] Despite the reduction in the size of the Russian strategic nuclear force, Russia has optimized its strategic missile force to generate enhanced EMP effects.[2]

In a 2004 article, Russian Major General Vladimir Belous advocated an "asymmetric response" against deployed U.S. missile defense capabilities by detonating nuclear weapons prepositioned in orbit above the U.S.[3] China's interest in EMP goes back decades, and there is concern in Taiwan that China would use EMP weapons as part of a Chinese invasion of Taiwan.[4] 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, while U.S. forces stationed on the Korean Peninsula would be extremely vulnerable.[5] Moreover the North Korean KN-08 missile, while inaccurate and possibly not able to reach a specific target in

the U.S., could be used to launch a high-altitude nuclear EMP attack.[6]

Even if a state was not disposed to launch a crippling EMP strike against the U.S. with no resulting fatalities, it may be willing to do so in combination with a biological attack.[7] Russia does not allow inspectors into all of its facilities capable of producing biological weapons.[8] The Department of State assesses that China, Iran, North Korea, Russia, and Syria continue to engage in dual-use activities with potential biological weapon applications.[9]

The most likely source of a bioterrorist attack is not governments, but radicalized groups or individuals, both within the U.S. or outside, that intend to utilize biological agents to cause mass casualties,[10] and it is not essential to assume that a combination EMP/cyber/biological attack must be perpetrated by the same actor. A state could execute an EMP or cyberattack or both, and a terrorist organization could seize the ensuing period of chaos to execute a biological attack. Terrorist organizations have expressed intent to use and show some capacity to develop biological weapons.[11]

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.[12] Additionally, some laboratory leaders have paid insufficient attention to the details necessary to ensure laboratory biosafety and have inadvertently contributed to the biological threat.[13]

EMP, Cyber, and the State of Public Health Preparedness

Current issues with the public health response are multifaceted and start with a significant lack of understanding of the threat among public health professionals. Scientists and medical professionals are focused on their areas of expertise and may not appreciate the nature of the WMD threat. Many public health professionals may not even know what an EMP attack is and how it can impact infrastructure relevant to their work. Moreover, most response plans 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 the entire public health community response.

The most likely source of a bioterrorist attack is not governments, but radicalized groups or individuals...

One of the most challenging issues for public health in the present context is the ever-increasing reliance of public health on electronic and cyber technology. 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.[14] 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.[15] 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.[16] During 2013, the Centers for Disease Control and Prevention (CDC) conducted two emergency notification drills with organizations that had received CDC funds for preparedness and response

capabilities.[17] The goal was to test whether CDC's Emergency Operation Center (EOC) laboratory staff and epidemiologists could contact each other regarding potential threats and disease outbreaks in a timely manner.[18] 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.[19]

Underneath these marvelous capabilities, however, lies a significant vulnerability. The problem is not the community's reliance on these communication and surveillance systems *per se*. The problem is that many of these systems are highly vulnerable to cyberattack; practically none of them are hardened against EMP-attack, and little has been done to train the public health community to function if these systems were suddenly to become non-operational. Local, state, and federal emergency management plans generally do not include back-up plans in case these electronic systems fail during an EMP and cyberattack. 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.

...there is a false sense of security among public health agencies and responders that they are sufficiently prepared...

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 for more than 60 percent 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.[20] 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.[21] The CIPA Act passed the House in 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 Strategic National Stockpile assets are deployed, to ensure that vaccines and medications are received in a timely manner if local supplies have run out.[22] Yet, none of the exercises include scenarios in which the transportation and communication systems have failed. In 2014, the Assistant Secretary for Preparedness and the CDC together awarded more than $840 million in emergency preparedness and response fund to improve existing response measures.[23] Whereas the close alignment of the funding support improved efficiency in grant administration, no funding was allotted to evaluate 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.

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.[24] Affected individuals may not necessarily seek care in the emergency room, but rather consult with their primary care provider or their staff or support staff, so providing training to even the nonmedical personnel in a physician's office could aid in early detection.[25] 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.[26]

Beyond training, practitioners still must seek opportunities to become familiar with local emergency medical series as well as local chain of command and their contact information.[27] In light of competing priorities for training and education, the amount of time a practitioner might actually devote to the difficult task of functioning successfully without electricity is questionable at best.

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.[28] Additionally, most plans do not extensively describe how to work side-by-side with responders from other agencies.[29] 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.[30] If training is mandated, agencies participating in an emergency response are often not coordinated in their efforts.[31]

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.[32] 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; all will need to act under emergency conditions.

However, even if the entire public health community and all other public servants were adequately trained, a major public education effort would be required to condition American society—unaccustomed as it is to major, long-term inconveniences, to deal with privations that would render their circumstances more closely akin to those of the seventeenth century than of the twenty-first century.

Many public and private organizations lack the comprehensive, emergency-response plan that defines the roles and responsibilities of trained personnel...

Protecting and Recovering Critical Infrastructure

Incidents of biological threats, such as the so-called "Amerithrax" attack of 2001, have been well documented. Since that time, disease surveillance tools and rapid testing capabilities have been deployed and have, it may be argued, protected against attacks that

otherwise could have been more effective than they were or caused more panic than they did. What is underappreciated, however, is the total reliance of these technologies on electric and cyber power, as well as the fact that they are not hardened against EMP.

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

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.[33] 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.[34] The North American Aerospace Defense Command (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.[35] In addition, the Pentagon awarded a $700 million contract to upgrade its electronics through 2020.[36] With that being said, most computers and electronic equipment in DoD is still vulnerable, such that an EMP attack could still severely degrade the ability of the armed forces to operate effectively.

If an EMP attack would occur, near-term recovery would prove impossible because of, (1) the nation's almost total dependence on the electrical grid[37] and (2) the interdependence of the critical infrastructures powered by the grid.[38] Restarting the grid, also known as a "black start," requires communication and energy transport, which both require electricity—causing an intractable "chicken or the egg" problem. Transformers and generators are not readily available for purchase and repairs may take months.[39] Thus, modernizing and hardening the electrical grid is as much a public health imperative as it is a defense or economic imperative.

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 disturbances.[40] 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.[41] 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.[42] A modern grid would address cyber security and EMP, as well as increased consumer demand, so governors have an important role in moving this agenda forward and making it a funding priority. 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 but relatively cost-

effective if integrated into the design phase of a new grid, but in either case, they are essential to the nation's security in a dangerous and uncertain world.

Conclusion

Perfect storm scenarios like the catastrophic convergence described herein are indeed the stuff of thriller novels and movies and, as a result, may seem simply too awful to be possible. However, it is precisely this "unthinkable" quality that demands the attention of thoughtful persons, intent upon securing the nation from those scenarios, which, even if unlikely, could prove the nation's undoing.

Operational planners have long noticed the vulnerabilities posed by bureaucratic gaps and seams. However, this convergence is not a problem of "gaps" and "seams." Rather, it is a problem of total systemic failure. EMP is real. Cyberattacks are real. Biological attacks are real. Adversaries of the U.S. who possess one or more of these capabilities are real. When the problem is considered in that light, it assumes a much more plausible form than it might when viewed on the Hollywood screen. Now is the time for the interagency to devote reasonable attention to the problem. ***IAJ***

NOTES

1 Jenna Baker McNeill and Richard Weitz, "Electromagnetic Pulse (EMP) Attack: A Preventable Homeland Security Catastrophe," The Heritage Center, October 20, 2008, <http://www.heritage.org/research/reports/2008/10/electromagnetic-pulse-emp-attack-a-preventable-homeland-security-catastrophe>, accessed on December 6, 2015.

2 Mark Schneider, "The Emerging EMP Threat to the United States," U.S. Nuclear Strategy Forum paper, National Institute Press, Fairfax, VA, November 2007, p. 3, <http://www.nipp.org/wp-content/uploads/2014/12/EMP-Paper-Final-November07.pdf>, accessed on December 6, 2015.

3 Ibid., p. 4.

4 Ibid., pp. 5–6.

5 Ibid., p. 10.

6 Ibid.

7 Clay Wilson, "High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessment," Congressional Research Service Report to Congress, July 2008, p. 20, <https://www.fas.org/sgp/crs/natsec/RL32544.pdf>, accessed on November 3, 2015.

8 Ibid.

9 U.S. Department of State, "Adherence to and Compliance with Arms Control, Nonproliferation, Disarmament Agreements and Commitments," Bureau of Arms Control, Verification, and Compliance Report, <http://www.state.gov/t/avc/rls/rpt/2015/243224.htm>, accessed on June 5, 2015.

10 Oliver Grundmann, "The Current State of Bioterrorist Attack Surveillance and Preparedness in the U.S.," *Risk Management and Healthcare Policy*, October 2014, Vol. 7, pp. 177–187, <http://dx.doi.org/10.2147/RMHP.S56047>, accessed on December 15, 2015.

11 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, October 2015, p. 4, <http://hudson.org/research/11824-a-national-blueprint-for-biodefense-leadership-and-major-reform-needed-to-optimize-efforts>, accessed on November 1, 2015.

12 Grundmann, p. 182.

13 Hudson Institute, p. 5.

14 Shawn D. Smith, "Inter-Agency Collaboration and Consequence Management: An All-Hazard Approach to Emergency Incident Response," EHS Today, May 16, 2006, <http://ehstoday.com/fire_emergencyresponse/ehs_imp_17938>, accessed on December 6, 2015.

15 Ibid.

16 Ibid.

17 Centers for Disease Control and Prevention, "National Snapshot of Public Health Preparedness," 2015, p. 11, <http://www.phe.gov/Preparedness/mcm/phemce /Pages/default.aspx>, accessed on February 7, 2016.

18 Ibid.

19 Ibid.

20 "H.R.2417, Secure High-voltage Infrastructure for Electricity from Lethal Damage Act," 113th Congress, June 18, 2013, <https://www.congress.gov/bill/113th-congress/house-bill/2417>, accessed on December 6, 2015.

21 "H.R.3410, Critical Infrastructure Protection Act," 113th Congress, October 30, 2013, <https://www.congress.gov/bill/113th-congress/house-bill/3410>, accessed on December 6, 2015.

22 Centers for Disease Control and Prevention.

23 Ibid., p. 27.

24 Gail Dudley and Robin B, McFee, "Preparedness for Biological Terrorism in the United States: Project BioShield and Beyond," *The Journal of the American Osteopathic Association,* 2005, Vol. 105, No. 9, p. 421.

25 Ibid.

26 Ibid.

27 Ibid., p. 422.

28 Smith.

29 Ibid.

30 Ibid.

31 Ibid.

32 James C. Kile et al., "Impact of 2003 Power Outages on Public Health and Emergency Response," *Prehospital and Disaster Medicine*, Vol. 20, No. 2, 2005, p. 96.

33 Baker Spring et al., "Before the Lights Go Out: A Survey of EMP Preparedness Reveals Significant Shortfalls," August 15, 2011, <http://www.heritage.org/research/reports /2011/08/before-the-lights-go-out-a-survey-of-emp-preparedness-reveals-significant-shortfalls>, accessed on December 6, 2015.

34 Ibid.

35 Henry F. Cooper and Peter Vincent Pry, "The Threat to Melt the Electric Grid," *The Wall Street*

Journal, April 30, 2015, <http://www.wsj.com/articles/the-threat-to-melt-the-electric-grid-1430436815>, accessed on December 6, 2015.

36 Ibid.

37 McNeill and Weitz.

38 Electric Power Research Institute, "Enhancing Distribution Resiliency: Opportunities for Applying Innovative Technologies," January 2013, p. 3, <http://www.epri.com/abstracts/Pages /ProductAbstract.aspx ?ProductId=000000000001026889&Mode=download>, accessed on December 6, 2015.

39 J. S. Foster et al., "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures," April 2008, p. 50, <http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf>, accessed on December 6, 2015.

40 Jenna Bergal, "States Work to Protect Electric Grid," February 27, 2015, <http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2015/2/27/states-work-to-protect-electric-grid>, accessed on January 15, 2016.

41 National Governors Association, "Governors' Guide to Modernizing the Electric Power Grid," March 2014, p.1, <http://www.nga.org/files/live/sites/NGA/files/pdf /2014/1403GovernorsGuideModernizingElectricPowerGrid.pdf>, accessed on January 15, 2016.

42 Ibid., p. 2.