World Medical and Health Policy

Cyber Security Threats to Public Health

Daniel J. Barnett, Tara Kirk Sell, Robert K. Lord, Curtis J. Jenkins, James W. Terbush, and Thomas A. Burke

Ever-increasing threats to cyber security present serious challenges for population health. However, the direct intersections between cyber security and public health can benefit from examination through the lenses of public health system operational frameworks. In this paper, we thus provide an overview of how cyber security issues may systemically impact public health emergency preparedness and imperil the delivery of essential public health services. We discuss future broad-based policy and research considerations accordingly for this critical public health security dimension.

KEY WORDS: cyber security, public health, preparedness, essential services, threats

Introduction

The vulnerability of the public's health to cyber security threats has received insufficient attention in the research literature to date, and has yet to be well understood (Harries & Yellowlees, 2013). This paper is intended as a step toward analyzing cyber-related public health challenges in a systematic fashion. The research gaps on cyber security and public health are particularly striking in light of an April 2012 report by the Government Accountability Office, which noted not only the ever-increasing prevalence of cyber security threats ("cyber threats"), but the many intentional and unintentional sources from which such threats can originate, the numerous targets that malicious actors might exploit, and the varied tools at the disposal of those who would seek to launch cyber attacks (U.S. Government Accountability Office, 2012a). The adage noted by security expert Bruce Schneier in his 2012 *Science* piece rings truer with each passing day: "Everything gets hacked" (Schneier, 2012)."

With increased funding for health information technology through such legislation as the Health Information Technology for Economic and Clinical Health (HITECH) Act (Centers for Disease Control and Prevention, 2012) comes an increased need to protect health information and public health infrastructure (Anonymous, 2009; Hathaway, 2009). Indeed, the health care sector has been described in the literature as a "tantalizing opportunity" for cyber terrorism (Harries & Yellowlees, 2013). However, as noted in 2011, the focus in

Published by Wiley Periodicals, Inc., 350 Main Street, Malden, MA 02148, USA, and 9600 Garsington Road, Oxford, OX4 2DQ.

peer-reviewed literature has been more on the role of information technology during emergencies, and less on how electronic systems would respond to threats themselves (McGowan, Cusack, & Bloomrosen, 2011). U.S. government reports provide perhaps the richest cyber threat response literature, but even here details regarding the specific effects of cyber threats on public health and strategies for threat mitigation is lacking. Health care seems to "[lag] behind the other critical industries, mostly because of its diverse, fragmented nature and a relative lack of regulation when compared with, say, the energy industry" (Colias, 2004). In this paper, we briefly describe the effect of cyber threats on several aspects of public health and suggest future research to better characterize this problem and determine policy solutions.

Cyber Security and the Public Health Emergency Preparedness System

In 2008, the Institute of Medicine presented a seven-stakeholders framework for the Public Health Emergency Preparedness System, comprised of (i) Health Care Delivery System; (ii) Homeland Security and Public Safety; (iii) Employers and Businesses; (iv) The Media; (v) Academia; (vi) Communities; and (vii) Governmental Public Health Infrastructure, the last of which serves as an organizational hub for the other participants (Altevogt, Pope, Hill, & Shine, 2008). This framework (Figure 1) offers a useful analytic lens for understanding the interconnected elements collectively essential for public health emergency readiness—and by extension, provides a window into how these vital elements may be critically endangered by cyber threats. While the framework does not explicitly mention information technology, such technology is nonetheless heavily utilized

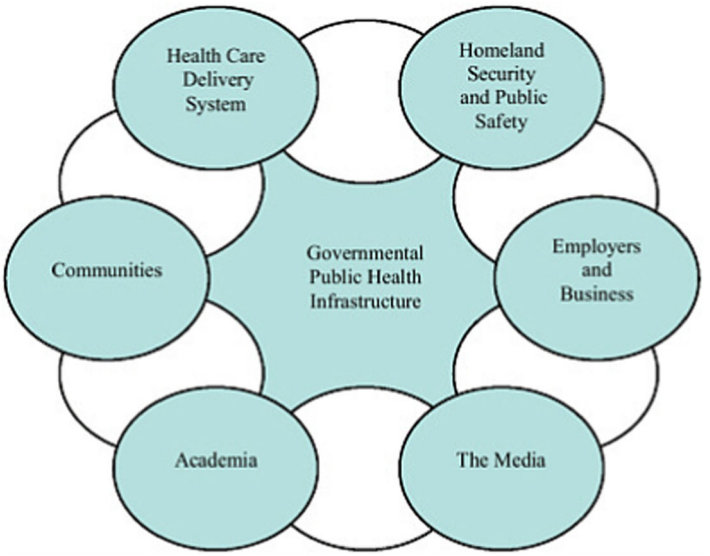

Figure 1. The Public Health Emergency Preparedness System.
Source: Institute of Medicine (2008) as adapted from Institute of Medicine, *The Future of the Public's Health in the 21st Century* (2002).

by (and represents a potential significant security vulnerability for) each of its seven stakeholders, and thus infuses all elements of this system.

Of relevance here, cyber threats to these seven stakeholder elements can be classified in terms of their capacity to effect (i) losses of integrity, (ii) losses of availability, (iii) losses of confidentiality, and (iv) physical destruction in systems that contribute to public health (U.S. Army Training and Doctrine Command, 2005). We note parenthetically which of these categories apply to the threats described below.

Health Care Delivery System

The Health Care Delivery System represents the front-line health care providers in the United States, such as hospitals and emergency medical services providers. The effects of power outages on hospitals caused by the collapse of public power grids (U.S. Government Accountability Office, 2012b) or the destruction of generators due to modifying code in Programmable Logic Controllers would have devastating consequences for patient care (physical destruction) (Choo, 2011). There are also more subtle threats such as the theft or loss of patient information (confidentiality) (Martin, 2001), disruption of care due to software outages (availability) (Lichtenfels, 2012), or loss of confidence in health care providers due to perceptions of inadequate security (integrity) (McGowan et al., 2011), the latter of which could decrease utilization of needed services. A newly emergent threat is the potential for security and privacy risks that emerge in personal medical devices, given their increasingly networked and wireless nature (confidentiality/physical destruction) (Avancha, Baxi, & Kotz, 2012; Kramer et al., 2012).

Homeland Security and Public Safety

Homeland Security and Public Safety actors could be affected by a wide array of cyber threats, such as disruption of emergency telephone lines and EMS systems, which could slow or disable emergency medical response (availability/integrity) (Kun, 2002). The role of Homeland Security and Public Safety is also important in managing threats that combine cyber elements with more traditional weaponry. In 2002, the director of the National Infrastructure Protection Center stated that his greatest fear was "a physical attack in conjunction with a successful cyber-attack," a situation that could amplify the public health impact of WMDs or conventional weapons (Gellman, 2002). However, while the DHS has elevated the importance of cyber security, it still faces challenges coordinating and effecting change in this area (Lord & Sharp, 2011).

Employers and Businesses

Traditional cyber threats to businesses present a range of damages that include reputational damage, financial gain and fraud, commercial advantage

and/or economic and political damage (confidentiality/integrity) (Scully, 2011). Any and all of these activities could disrupt the providing of public health resources through an inability to produce needed medical equipment or drugs through manufacturing stoppages (availability) (De Oliveira, Theilken, & McCarthy, 2011), loss of protected health information and subsequent decreases in public trust of health apparatuses (loss of integrity) (McGowan et al., 2011), or failures of vendors to provide key hospital services that might range from software to temporary staffing (availability). In addition, since the Aurora Test in 2007, and the Stuxnet virus of 2010, it has been clear that the potential for users to remotely access and damage physical systems is all too real (U.S. Government Accountability Office, 2012b), and dangerous when applied to the many functions performed by businesses, particularly regulated utilities (physical destruction). The above-noted threats, if they occurred in businesses critical to public health infrastructure, could shut down or slow supply chains, impair patient care, and impede emergency response, potentially leading to significant loss of life.

The Media

The media serves to transmit "legitimated" information as provided by government and expert sources (Wray, Kreuter, Jacobsen, Clements, & Evans, 2004), and to the extent that cyber threats have the potential to corrupt or distort this information, they can detract from the ability of these critical structures to aid in public health (integrity). Even more simply, cyber threats that directly or indirectly disable media transmission or reception impair the ability of actors in this model to reach communities with up-to-date information (availability). There also exists the potential for social media to contribute to public health response (U.S. Department of Homeland Security, 2012), and to the extent that this capability is utilized, it may present a corresponding vulnerability (integrity/availability).

Communities

Communities are highly vulnerable to the public health effects of the failure of cyber-based systems, as they often lack the backup generators and systems that government or industry actors might have. Food and medication may lose their refrigeration, and medical apparatuses outside of hospitals may be vulnerable to power loss (physical destruction/availability) (Clem, Galwankar, & Buck, 2003). Social discontent and unrest are potential consequences of community disruption, with obvious public health consequences if such unrest is large-scale and prolonged in nature (Choo, 2011).

Academia

While academia may not play a core role *during* a cyber threat beyond providing expert advice (Wray et al., 2004), it plays a critical role in *preparation* for

such threats (Institute of Medicine, 2002). One exception to these primarily preparative and advisory roles, however, is the threat of sensitive academic research with uses that could either be weaponizable or induce some manner of public health crisis (confidentiality) (Schneier, 2012). In this case, cyber threats could pose very real dangers, by arming malicious actors with decidedly non-virtual armaments. Moreover, academic campuses are vulnerable to power outages due to cyber threats, given that their laboratories house infectious agents, cadavers, and a host of research animals (physical destruction).

Governmental Public Health Infrastructure

Our final actor, Government Public Health Infrastructure, has many roles that could be disrupted by cyber threats. Such initiatives as the CDC's Select Agent Program (Lister, 2005) could be subject to cyber threats that penetrate and improperly release information that could cause or exacerbate public health crises, given that this work focuses on dangerous agents and potential countermeasures (confidentiality). Some components of the public health supply chain could be rendered unusable by cyber threats, such as elements of the Strategic National Stockpile (Lister, 2005) that require refrigeration or electricity (physical destruction). Finally, the availability of command and control infrastructure could be impaired during cyber attacks, limiting HHS's ability to coordinate public health response and conduct surveillance on the progress of efforts (availability/integrity). Indeed, the critical analytical role of health informaticians in public health surveillance and analysis (Centers for Disease Control and Prevention, 2012) could be disrupted through threats to data collection, storage, and analysis similar to those faced by businesses.

In the context of the seven-actor framework discussed above (Altevogt et al., 2008), we note that perhaps the most vulnerable components, significantly exposed to all four types of cyber threats, are those of the Health Care Delivery System, Businesses and Employers, and the Governmental Public Health Infrastructure. Indirectly, long-term burdens on communities due to cyber threats that disable communication and public utilities can tax the other public health actors such that their best efforts could be insufficient in controlling community discontent. While disruptions to media and academia may be less overtly deleterious to public health, they nonetheless pose serious risks as noted above. Thus, disruptions in any of the seven actors due to cyber threats have potentially serious consequences for public health, though these consequences are currently ill-defined due to a dearth of peer-reviewed literature in this area.

Cyber Security and Essential Public Health Services: A Crosswalk Analysis

A crosswalk analysis of the potential impacts of cyber threats on essential public health services further highlights the extensive implications of cyber security for population health and wellbeing (Figure 2). The CDC-defined 10

1. **MONITOR health status to identify and solve community health problems**

- Key activity affected: Health surveillance
    - Computer systems that collect, transfer, and store data are vital for both active and passive surveillance. Loss of these systems through direct attack or loss of infrastructure would limit the ability of public health to track and monitor diseases and health conditions of importance.

2. **DIAGNOSE AND INVESTIGATE health problems and health hazards in the community**

- Key activity affected: Analysis of health information
    - Loss of access to information hinders the ability of health departments to diagnose problems in the community. While health investigations may continue, loss of infrastructure, such as communications channels, could prevent timely analysis of health problems and access to laboratory and hospital data.

3. **INFORM, EDUCATE and empower people about health issues**

- Key activity affected: Delivery of health information
    - Attack on public health information dissemination systems could limit the ability of the health department to disseminate information. Loss of infrastructure could prevent people from receiving important information.

4. **MOBILIZE community partnerships and action to identify and solve health problems**

- Activities in this area may provide resilience in the face of cyber threats
    - Coalitions, partnerships, and motivated stakeholders may be able to continue communication and activity through relationships formed before disaster. These activities may help communities weather the loss of infrastructure or provide alternate conduits of information flow. However, the loss of electronic communication could reduce the effectiveness of coalitions such as hospital coalitions when they are needed the most.

5. **DEVELOP POLICIES AND PLANS that support individual and community health efforts**

- Activities in this area may improve both prevention and response in the face of cyber threats
    - Educating policymakers on the public health effects of cyber threats to formulate better policy and planning for possible response activities before disaster could reduce the effects of cyber threats.

6. **ENFORCE laws and regulations that protect health and ensure safety**

- Activities in this area could help to reduce the impact of cyber threats
    - Encouraging hospitals and other relevant organizations to improve practices and reduce vulnerabilities could reduce impacts of cyber threats. However, loss of infrastructure could reduce the ability to communicate notifiable diseases or health violations.

7. **LINK people to needed personal health services and assure the provision of health care when otherwise unavailable**

- Key activity affected: Increased need to respond to public health emergencies in order to provide people with necessary health services
    - Loss of infrastructure would cause the denial of utility services needed to maintain the health of the public. Loss of electricity or water during heat waves or cold spells will require response from public health to prevent loss of life. Similarly, cyber attacks may result in the failures of industrial safety systems (e.g., in chemical manufacturing) that could cause widespread illness and possibly death, requiring response from public health entities.
- Key activity affected: Loss of access to appropriate medical care
    - Hospitals may encounter reduced capacity to provide medical care through the loss of hospital systems. Additionally, loss of access to health records limit public health's ability to provide appropriate care, shelter, and medicine in times of need. Damage to infrastructure such as transit or insurance/payment methods could also prevent people from accessing necessary medical care.

8. **ASSURE competent public and personal health care workforce**

- Creeping losses in this health service will exacerbate problems posed by cyber threats
    - The continuing loss of staff and funding make it difficult for health departments to meet community needs for public and personal health services. Increased strain on the system due to cyber threats will only magnify this problem. Additionally, cyber threats may reduce workers' ability to access just-in-time training.

9. **EVALUATE effectiveness, accessibility, and quality of personal and population-based health services**

- Key activity affected: Assessment of public health interventions
    - Evaluation of health interventions requires data storage and communication to measure progress towards goals. In an information- or communication-poor environment it may be difficult to know if the work public health is doing is making a difference.

10. **RESEARCH for new insights and innovative solutions to health problems**

- Activities in this area will help to identify gaps, harden public health systems, and build coping strategies for vulnerabilities that cannot be addressed. However, research during a cyber crisis may be limited due to loss of infrastructure and records.

Figure 2. Ten Essential Public Health Services and Cyber Threats Crosswalk.

essential public health services include: (i) *monitor* health status to identify and solve community health problems; (ii) *diagnose and investigate* health problems and health hazards in the community; (iii) *inform, educate, and empower* people about health issues; (iv) *mobilize* community partnerships and action to identify and solve health problems; (v) *develop policies and plans* that support individual and community health efforts; (vi) *enforce* laws and regulations that protect health and ensure safety; (vii) *link* people to needed personal health services and assure the provision of health care when otherwise unavailable; (viii) *assure* competent public and personal health care workforce; (ix) *evaluate* effectiveness, accessibility, and quality of personal and population-based health services; and (x) *research* for new insights and innovative solutions to health problems (Centers for Disease Control and Prevention, 2010).

As Figure 2 illustrates, virtually every essential service of public health may face significant operational impacts from cyber security vulnerabilities. While a more granular discussion of the numerous specific activities impacted within each essential service is beyond the scope of discussion here and insufficiently addressed by the peer-reviewed literature to date, this paper nonetheless reveals critical challenges that cyber security poses to both routine and emergent public health activities and systems.

Discussion

In this paper we have taken initial steps to examine intersections between cyber security and public health, through the lenses of the public health emergency preparedness system and the essential services of public health. Given the paucity of rigorous research to date on this nascent public health threat, any formal policy recommendations would be premature. However, our preliminary analyses described above permit at least a broad-based discussion of vital policy and research considerations moving forward, which we describe below.

Improved Private–Public Partnership

As we have noted, the public health emergency preparedness system is comprised of an array of different stakeholders. It should come as no surprise that increasing the resilience of the public health system to cyber-attack will require partnership between the private sector and government (Centers for Disease Control and Prevention, 2012). Improved information sharing between different entities is an important step towards creating a unified set of objectives pertaining to cyber security. Additionally, members of the health care delivery system, homeland security and public safety, employers and businesses, the media, communities, and academia should work with public health to ensure that any government policy in cyber security takes into account the broad set of interests that make up the public health emergency preparedness system. Finally, the innovative capacity of the private sector should be leveraged to address cyber security concerns (Lord & Sharp, 2011).

Recognition of Public Health Aspect of Cyber Security by Policymakers

It is clear that a cyber attack could have far-reaching consequences on the nation's economy, intellectual property, sensitive military information, and critical infrastructure. Here, we add another dimension—the health of the public. Recently, the Secretary of Defense, Leon Panetta stated, "The collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life" (Panetta, 2012) Our analysis supports this premise, highlighting how cyber attacks may critically endanger vital public health elements, possibly resulting in serious health consequences. Policymakers should understand the consequences of a lack of preparedness for cyber attacks. Future legislation and regulations in this space should also account for the interactions between cyber security and public health.

Future Research Avenues

Ultimately, significant new research is required to more thoroughly understand the complex risk relationships between cyber security and public health; and to develop rigorous evidence-based policy and practices to address this multifaceted public health threat. Such efforts will necessarily entail identifying public health indicators of relevance to cyber security threats; assessing public health system functioning based on these indicators (and potentially new indicators as they arise); providing health practitioners, policymakers, and researchers with timely access to these indicators; and facilitating cyber security-related public health risk communication activities for these respective stakeholder audiences. Additionally, interdisciplinary research collaborations will be essential to bringing stakeholders with vastly different experience together around this multidimensional public health threat.

Daniel J. Barnett, MD, MPH, is an Assistant Professor in the Department of Environmental Health Sciences, with a joint appointment in Health Policy and Management, at the Johns Hopkins Bloomberg School of Public Health.
Tara Kirk Sell, MA, is pursuing a PhD at the Johns Hopkins Bloomberg School of Public Health in the Department of Health Policy and Management. She is also a Senior Analyst at the Center for Biosecurity of UPMC.
Robert K. Lord, AB, is a medical student at the Johns Hopkins University School of Medicine.
Curtis J. Jenkins, BS, MA, CDR USN, is the director of Strategic Communication and Public Affairs for the Navy's Information Dominance Corps Reserve Command and supports special projects at NORAD and U.S. Northern Command in Colorado Springs, Colorado.
James W. Terbush, MD, MPH, CAPT MC USN, currently serves as the medical lead for Innovations and Experimentation in the Science and Technology Directorate for NORAD and the United States Northern Command, Colorado Springs, Colorado.

Thomas A. Burke, PhD, MPH, is Professor and Associate Dean for Public Health Practice and directs the Risk Sciences and Public Policy Institute at the Johns Hopkins Bloomberg School of Public Health.

Notes

The opinions expressed in this article are those of the authors and do not necessarily reflect the views of the Department of Defense or the U.S. Navy.

Conflict of interest: None declared.

References

Altevogt, Bruce M., Andrew M. Pope, Martha N. Hill, and Kenneth I. Shine, eds. 2008. *Institute of Medicine. Research Priorities in Emergency Preparedness and Response for Public Health Systems: A Letter Report*. Washington, DC: The National Academies Press.

Anonymous. 2009. "Wanted: Cyber-Czars [Editorial]." *Nature* 458 (7241): 945.

Avancha, Sasikanth, Amit Baxi, and David Kotz. 2012. "Privacy in Mobile Technology for Personal Healthcare." *ACM Computing Surveys* 45 (1): 1–54.

Centers for Disease Control and Prevention. 2010. "National Public Health Performance Standards Program. 10 Essential Public Health Services." http://www.cdc.gov/nphpsp/essentialservices.html. Accessed September 21, 2012.

———. 2012. "CDC's Vision for Public Health Surveillance in the 21st Century." http://www.cdc.gov/mmwr/pdf/other/su6103.pdf. Accessed August 1, 2012.

Choo, Kim-Kwang. 2011. "The Cyber Threat Landscape: Challenges and Future Research Directions." *Computers and Security* 30: 719–31.

Clem, Angela, Salgar Galwankar, and George Buck. 2003. "Health Implications of Cyber-Terrorism." *Prehospital and Disaster Medicine* 18 (3): 272–75.

Colias, Mike. 2004. "Cyber Security." *Hospitals and Health Networks*. http://www.hhnmag.com/hhnmag/jsp/articledisplay.jsp?dcrpath=HHNMAG/PubsNewsArticle/data/backup/0405HHN_FEA_Cyber_Security&domain=HHNMAG. Accessed August 1, 2012.

De Oliveira, Gildasio S., Jr., Luke S. Theilken, and Robert J. McCarthy. 2011. "Shortage of Perioperative Drugs: Implications for Anesthesia Practice and Patient Safety." *Anesthesia and Analgesia* 113 (6): 1429–35.

Gellman, Barton. 2002. "Cyber Attacks by Al Qaeda Feared." *Washington Post*. http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711.html. Accessed August 5, 2012.

Harries, David, and Peter M. Yellowlees. 2013. "Cyberterrorism: Is the U.S. Healthcare System Safe?" *Telemedicine and e-Health* 19 (1): 61–66.

Hathaway, Melissa. 2009. The President's Cyberspace Policy Review. http://www.whitehouse.gov/CyberReview. Accessed August 1, 2012.

Institute of Medicine. 2002. *The Future of the Public's Health in the 21st Century*. Washington, DC: The National Academies Press. http://iom.edu/Reports/2002/The-Future-of-the-Publics-Health-in-the-21st-Century.aspx. Accessed August 1, 2012.

Kun, Luis G. 2002. "Homeland Security: The Possible, Probable, and Perils of Information Technology. Information Technology is a Key Component in Both Defending Against and Aiding Terrorism Threats." *IEEE Engineering in Medicine and Biology* 21 (5): 28–33.

Kramer, Daniel B., Matthew Baker, Benjamin Ransford, Andres Molina-Markham, Quinn Stewart, Kevin Fu, and Matthew R. Reynolds. 2012. "Security and Privacy Qualities of Medical Devices:

An Analysis of FDA Postmarket Surveillance." *PLoS ONE* 7 (7): 1–7. http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0040200. Accessed August 6, 2012.

Lichtenfels, Rick. 2012. "US Department of Homeland Security's Cybersecurity and Communications Integration Center." Presented at Spring Conference of Information Systems Audit and Control Association; April 30, 2012; New York, NY. http://www.isaca.org/chapters2/New-York-Metropolitan/membership/Documents/2012-04-30%20Spring%20Conference-Meeting/2%20Lichtenfels%20DHS%20NCCIC%202.pdf. Accessed August 2, 2012.

Lister, Sara A. 2005. Congressional Research Service. *An Overview of the U.S. Public Health System in the Context of Emergency Preparedness*. http://www.fas.org/sgp/crs/homesec/RL31719.pdf. Accessed August 3, 2012.

Lord, Kristin M., and Travis, Sharp eds. 2011. Center for a New American Security. *America's Cyber Future: Security and Prosperity in the Information Age: Volume 1*. http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20I_0.pdf. Accessed August 4, 2012.

Martin, Robert A. 2001. "Managing Vulnerabilities in Networked Systems." *Computer* 34 (11): 32–38.

McGowan, Julie J., Caitlin M. Cusack, and Meryl Bloomrosen. 2011. "The Future of Health IT Innovation and Informatics: A Report From AMIA's 2010 Policy Meeting." *Journal of the American Medical Informatics Association* 19: 460–67.

Panetta, Leon E., Secretary of Defense. 2012. *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security*. http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136. Accessed November 28, 2012.

Schneier, Bruce. 2012. "Securing Medical Research: A Cybersecurity Point of View." *Science* 336 (6088): 1527–29.

Scully, Tim. 2011. "The Cyber Threat, Trophy Information and the Fortress Mentality." *Journal of Business Continuity & Emergency Planning* 5 (3): 195–207.

U.S. Army Training and Doctrine Command. 2005. *Cyber Operations and Cyber Terrorism. DCSINT Handbook No. 1.02*. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA439217/. Accessed August 4, 2012.

U.S. Department of Homeland Security. 2012. *National Preparedness Report*. http://www.fema.gov/library/viewRecord.do?id=5914. Accessed August 3, 2012.

U.S. Government Accountability Office. 2012a. "Cybersecurity: Threats Impacting the Nation." http://www.gao.gov/products/GAO-12-666T. Accessed August 1, 2012.

———. 2012b. "Cybersecurity: Challenges in Securing the Electricity Grid." GAO-12-926T. http://www.gao.gov/products/GAO-12-926T. Accessed August 1, 2012.

Wray, Ricardo J., Matthew W. Kreuter, Heather Jacobsen, Bruce Clements, and R. Gregory. Evans 2004. "Theoretical Perspectives on Public Communication Preparedness for Terrorist Attacks." *Family and Community Health* 27 (3): 232–41.