



A primary resource for reliable information on the application and use of information technology in all aspects of health and health care nationally, regionally and internationally.

Cyberterrorism in Telemedicine: A New Threat to Computer-Mediated Communication Systems

Gerald-Mark Breen¹, Jonathan Matusitz, PhD¹, Aileen Sousa¹

¹University of Central Florida

This article is available from: <http://www.ehealthinternational.org/>

Abstract

This paper analyzes telemedicine, the application of distant computer-mediated communication technologies in healthcare, and its permeability and susceptibility to cyberterrorist attacks. Although telemedicine has the ability to transcend geographical boundaries to escape the constraints of temporal boundaries, to lower financial costs in medical care exchange and delivery, to boost patient comfort, satisfaction, and security, and to digitize health communication and relevant information via web-based services, telemedicine is also dangerously vulnerable, as it is open and exposed to devious, computer-savvy individuals waging attacks via computer technologies. Those individuals are also known as cyberterrorists. Their main objective is to alter information and impede normal communication channels in this vital health communication context. This could have a detrimental effect on an entire community.

Introduction

This paper describes the potential of electronic threats in telemedicine, (i.e., Matusitz, 2008). After describing briefly past and current telemedicine applications, we discuss the unique needs, problems, opportunities, and resources relative to telemedicine services. Although telemedicine has the ability to transcend geographic boundaries, lower financial costs in medical care, boost patient comfort, satisfaction, and security, and digitize health communication and relevant information via web-based services, it is also vulnerable to electronic breaches by individuals known as cyberterrorists. Their main tactic is to alter information and impede normal communication channels in this vital health service. When it happens, it has detrimental effects on the patients and their providers. While Matusitz and Breen (2007a, 2007b) identify a variety of challenges that endanger the advancement and success of telemedicine, this analysis focuses

on a new threat that demonstrates telemedicine's vulnerability to cyberterrorism.

One section is devoted to explaining how cyberterrorists may prey on telemedicine, particularly e-health, in order to do their misdeeds against a computerized global healthcare delivery and exchange system. The paper concludes with suggestions on how specialists in the area of counter-cyberterrorism can combat this problem so that this vital healthcare network can remain intact and free from disruption. Ultimately, we should be prepared to deal with this form for terrorism and be cognizant of strategies to counteract the problem once it occurs.

Cyberterrorism

One of the first analyses of cyberterrorism in medicine and medical settings was published in 2003 by Clem, Galwankar, and Buck. Their

analysis focused on the health effects of cyberterrorism on individuals (i.e., cyberterrorists could kill a hospital patient by changing the liquid dosage [being administered to the patient] after delving through the hospital computer network). Yet, their analysis was also limited for two reasons: first, it only concentrated on the health implications of hacking attacks if these were perpetrated against hospitals; second, it did not focus on telemedicine. For these reasons, we wish to bring fresh insight into these issues. Before a discussion of the potential for cyberterrorism in telemedicine, we provide an overview of the definition of telemedicine. This may explain how these technologies that comprise telemedicine are susceptible to intrusion by cyberterrorists.

In line with descriptions provided by prominent scholars in the computer-mediated communication (CMC) field (Walther, 1996; 1997; Walther, Gay, & Hancock, 2005), telemedicine is the employment of advanced and CMC technologies, within the context of clinical care. It delivers care over long distances (Doolittle et al., 2005). It facilitates the delivery of healthcare to benefit patients suffering from with serious conditions or diseases (Cermack, 2006; Matusitz & Breen, 2007a, 2007b). The technology ranges from the telephone to state-of-the-art equipment that allows physicians, nurses, and other allied health professionals to provide healthcare at a distance (Breen & Matusitz, 2007; Mort, May, & Williams, 2003; Turner, Thomas, & Reinsch, 2004).

Telemedicine is used not only in multiple medical contexts, but also to speed up communication between medical practitioners and their patients. It functions between locations of clinical practice in an effort to successfully provide relief and/or education for practitioners carrying out a variety of medical procedures (Matusitz & Breen, 2007a, 2007b). The diversity of applications for telemedicine comprises patient care (Doolittle et al., 2005), research, training, administration, and public health to diagnose pathologies (Conrad, 1998), transmit health information (Wootton, 2001), examine x-rays, provide services (Dickens & Cook, 2006), and train health professionals (Breen & Matusitz, 2007).

The scope of telemedicine has rapidly broadened to include several types of services. This includes use of telemedicine by specialist referral services, where general practitioners may receive assistance from specialists in rendering a diagnosis. Patients may use a live, remote consultation, or the transmission of diagnostic images and/or video conferences along with patient data to “see” a specialist (American Telemedicine Association [ATA], 2006). Telemedicine can also be used to monitor remote patients. Telemonitoring devices collect data, such as blood glucose or heart ECG from homebound patients, and send the data to a monitoring station (ATA, 2006).

Because we are in an era where we depend on personal computers and access to the Internet, telemedicine now utilizes and even includes Internet-based services. Web-based services are known as one form of e-health. E-health refers to not only the use of distant communication technologies in the healthcare context, but, also, as Eysenbach (2001) explains it, to the use of advanced information and communication technologies (i.e., the Internet) to meet the needs of citizens, patients, healthcare practitioners and professionals, as well as policy makers. While the telephone is part of telemedicine, it is not part of e-health. In other words, e-health focuses more on advanced information and communication technologies.

The Advent of Telemedicine: Its First Applications

Examining the history of telemedicine is also a crucial area to cover for the purpose of understanding how and why the practice started and initially developed. By looking at this history of telemedicine through this lens, it becomes clear how the increased computer-mediated communication and technological aspects of telemedicine have given rise to the ability for cyberterrorists to penetrate this delicate and important resource commonly used in society.

The origin of telemedicine, can be informally traced back to when electronic devices were initially brought forth to the general population. From 1900 until now, the employment of radio, telegraphy, telephony, television, and other forms of wireless technology have assisted in the physician-patient communication process (Matusitz & Breen, 2007a).

Telemedicine continued to advance over time. Improvements of telemedicine were later applied in rural medicine context in the early 1970s through the Space Technology Applied to Rural Papago Advanced Health Care (STARPAHC) program, as well as distant areas (Turner, Thomas, & Reinsch, 2004), medically under served, remote locations where care and technology were lacking, and slowly developing and Third World countries (Whitten, Davenport Sypher, & Patterson, 2000). As time progressed, and as technological and medical intelligence and sophistication advanced rapidly, telemedicine became more common in the 1980s when costs decreased and quality improved. These technologies continue to improve based on the continual efforts to enhance the efficiency and accuracy of data transmission.

An Introduction to Cyberterrorism: A Viral Method to Infect Telemedicine Systems

Based on strategies and approaches used by the perpetrators, telemedicine technologies are vulnerable to the cyberterrorists who seek maliciously to alter telemedicine resources. Cyberterrorism can damage telemedicine systems and affect an entire community.

Cyberterrorism is considered a type of terrorism that aims at attacking and damaging computers, computer networks and data (Matusitz, 2005, 2008; Matusitz & O'Hair, in press), information technologies, and the Internet as a whole. Cyberterrorism was coined and given official reference in the 1980s (Alexander & Swetnam, 2001). Cyberterrorism attacks have always been characterized as significant, computer-based strikes on individual computers, institutions, or even governments (Dunnigan, 2002).

Cyberterrorism attacks can be premeditated, politically driven, committed by small bands of people, and/or intended to bring notice to a cause (Arquilla & Ronfeldt, 2001). In addition, by analyzing the likely rise of cyberterrorism, Denning (2001) contends that for terrorists to view attacks against computer networks as effective weapons, the strikes should be destructive or chaotic enough to produce public fear tantamount to those achieved from physical acts of terrorism. Denning (2001) goes on to point out that cyberterrorist strikes that ren-

der mass casualties or bodily harm might become primary aspirations of cyberterrorists.

Cyberterrorism attacks also come in many shapes and forms. First, a typical cyberterrorist action could involve the destruction of the physical machinery through computer manipulation (Kopelev, 2000; Matusitz, 2005, 2008). Second, causing interference with information technology, government computer networks, or critical civilian systems such as financial networks or mass media are also usual acts of cyberterrorism. E-health can be one of these network systems invaded. Third, using computer networks to usurp control over systems that guide traffic lights, power plants, or dams, stealing classified files, as well as to reconstruct the content of Web pages (medical content on e-health sites), spread false information, subvert government or organizational missions, delete data, or threaten to disclose secret information or system weaknesses unless a ransom or political allowance is made are general instances of cyberterrorism (Conway, 2002; Matusitz & O'Hair, in press).

Waging successful cyberterrorist attacks is not an easy task. It requires pinpointing the vulnerable entry points to computer security systems and attacking them by using, computer viruses. (Matusitz, 2005; Matusitz & O'Hair, in press). Clearly, usual outcomes of cyberterrorism include damage to businesses and the usual flow of information. At the macro-level, widespread public fear and a powerful influence on politicians, military, and other authoritative decisions are typical aims and results of cyberterrorism acts (Pineiro, 2004). With respect to e-health, fear may develop from seek in medical guidance and information online, fear of obtaining incorrect or deceptive advice, potentially leading to injury or death.

Cyberterrorism can target and usurp a wide array computer systems (and networks) that the cyberterrorists' ability to tap into nearly database or control system can be devastating and unpredictable. Hence, the next section provides identities and assessments of the types of cyberterrorist threats in order to give the reader a clearer understanding of their information and potential for disruption.

A Significant Challenge to the Development of E-Health: Cyberterrorism

Despite the promise of health communication from e-health, it also raises questions that obstruct or threaten its growth and implementation. Of course, there are other challenges to the advancement and success of telemedicine, including, (1) licensing and legal issues; (2) patient privacy; (3) resistance from health insurance carriers; and (4) limited knowledge and expertise in telemedicine.

Often we hear of web sites being harmed by hackers, and government or political web pages manipulated or altered by cyberterrorists. Most companies today not only use traditional, paper-based catalogues, and postal mail to provide, exchange, and deliver information, but also the Internet to display and exchange information. This is simply the way society and the corporate and general business world are developing in their marketing, advertising, and sales methods. With healthcare services being one such market that heavily uses the Internet as its communication channel and delivery system, e-health is just as vulnerable and equally susceptible to attacks by cyberterrorists.

There are several key e-health companies that have been identified as the most visited, used, and relied upon for healthcare consumers who have access to the sites. These include sites such as WebMD.com, Medlineplus.gov, Medscape.com, and Mentalhelp.net, among others. Given the delicate nature of healthcare information, cyberterrorists could create massive damage by penetrating into these systems and altering them in ways they [cyberterrorists] deem to be the most devastating.

In light of the recent increases of "cyberization" of health (Matusitz & Breen, 2007b; Rusovick & Warner, 1998) and convergence to online healthcare information, medical institutions and companies have created web-based databases and search engines containing an abundance of healthcare information, with practically an endless range of documentation.

Because there is a clear rise in the usage of online sites for medical or healthcare reasons, cyberterrorists can become aware of this fact and selectively choose the maximal target for devastation. The transmission of sensitive

medical data, especially through web-based channels, leaves patients at risk for a cyber attack. Already, there have been several cases of hackers infiltrating patient data systems at hospitals. One such case, at the University of Washington Medical Center, involved a hacker gaining access to 5,000 patient files (Songini, 2000). Using the Internet, the hacker was able to download patient names, conditions, home addresses, and Social Security numbers (O'Harrow, 2000).

Discussion

This paper focuses on a potentially significant threat to telemedicine and particularly e-health. Telemedicine has faced evolutionary hurdles and impediments, but the types of menace achievable by cyberterrorists is in a league of its own, a way to misinform, misguide, and ultimately harm consumers who may frequently depend upon healthcare information.

Due to the rise of cyberterrorism, it is crucial for health communication, computer-mediated communication, terrorism and cyberterrorism, and general communication scholars to explore the potential vulnerability of telemedicine services (particularly those on the Internet) as targets for terrorism and mischief. To confirm the clear and strong connection and relevance of telemedicine as a field and system is to the discipline of communication, thereby justifying and warranting such an analysis in a fashion oriented toward communication researchers, scholars, and practitioners, (Matusitz & Breen, 2007a; Mort, May, & Williams, 2003; Turner, Thomas, & Reinsch, 2004; Walther, Gay, & Hancock, 2005).

Pernicious hackers have already been known electronically to alter and mutilate Internet sites, including web sites health information (see Conway, 2002; Verton, 2003). Other past cases that may show a growing reason for potential plots may include, ex-patients who are angry with certain doctors. Some irate have been known to send harassing and intimidating messages to their providers (Lion & Herschler, 1998).

Another major concern lies in the deficiency of qualified or unprepared support personnel to monitor these web sites, check and install the latest anti-virus software, maintain existing hardware continuously to prevent a threat that could occur at any time. Due to these general and complicated flaws in web system support, higher levels of virus and worm infections of electronic patient data may result (Rigby, 2002). In sum, telemedicine services such as the ones listed above are susceptible to such attacks. Thus, protective measures should be developed and implemented in order to prevent such problems.

As both healthcare providers and recipients, we are in a position to appreciate the benefits of telemedicine, but also be aware of the risk and threats, that may be encountered.

Acknowledgments

This research is, in part, supported by the National Institute of Nursing Research, NIH, under research grant number R01 NR008226-01A1

References

2. Alexander, Y., & Swetnam, M. S. (2001). Usama bin Laden's al-Qaida: Profile of a Terrorist Network. Ardsley, NY: Transnational.
5. American Telemedicine Association [ATA] (2005a). Telemedicine defined. Retrieved September 8, 2006, from <http://www.atmeda.org/news/definition.html>.
8. Arquilla, J., & Ronfeldt, D. (Eds.) (2001). Networks and netwars: The future of terror, crime, and militancy. Santa Monica: RAND.
17. Breen, G. M., & Matusitz, J. (2007). An interpersonal examination of telemedicine: Applying relevant communication theories. *eHealth International Journal*, 3(1), 18-23.
21. Cermack, M. (2006). Monitoring and telemedicine support in remote environments and in human space flight. *British Journal of Anaesthesia*, 97(1), 107-114.
22. Clem, A., Galwankar, S., & Buck, G. (2003). Health implications of cyber-terrorism. *Prehospital and Disaster Medicine*, 18(3), 272-275.
23. Conrad, S. K. (1998). Making telehealth a viable component of our national health care system. *Professional Psychology: Research and Practice*, 29(6), 525-526.
24. Conway, M. (2002). What is cyberterrorism? *Current History*, 2, 436-440.
30. Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism. The internet as a tool for influencing foreign policy. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars* (pp. 239-288). Santa Monica, CA: RAND.
31. Dickens, B., & Cook, R. J. (2006). Dimensions of informed consent to treatment. *International Journal of Gynecology and Obstetrics*, 85, 309-314.
32. Doolittle, G. C., Whitten, P., McCartney, M., Cook D., & Nazir, N. (2005). An empirical chart analysis of the suitability of telemedicine for hospice visits. *Telemedicine Journal and eHealth*, 11(1), 90-97.
33. Dunnigan, J. F. (2003). The next war zone: Confronting the global threat of cyberterrorism. New York: Citadel Press.
36. Eysenbach, G. (2001). What is e-health? *Journal of Medical Internet Research*, 3(2), e20.
47. Kopelev, S. (2000). Cracking computer codes. *Law Enforcement Technology*, 27(1), 60-67.
50. Lion, J. R., & Herschler, J. A. (1998). The stalking of clinicians by their patients. In J. R. Meloy (Ed.). *The psychology of stalking: Clinical and forensic perspectives* (pp. 163-173). San Diego: Academic Press.
52. Matusitz, J. (2005). Cyberterrorism: How can American foreign policy be strengthened in the Information Age? *American Foreign Policy Interests*, 27(2), 137-147.
53. Matusitz, J. (2008). Postmodernism and networks of cyberterrorists. *Journal of Digital Forensic Practice*, 2, 1-10.
54. Matusitz, J., & Breen, G. M. (2007a). E-health: A new kind of telemedicine. *Social Work in Public Health*, 23(1), 95-113.
55. Matusitz, J., & Breen, G. M. (2007b). Telemedicine: Its effects on health communication. *Health Communication*, 21(1), 73-83.
56. Matusitz, J., & O'Hair, D. (in press). The role of the internet in terrorism. In D. O'Hair, R. Heath, K. Ayotte, & G. R. Ledlow (Eds.), *Terrorism: Communication and rhetorical perspectives*. Cresskill, NJ: Hampton Press.
59. Mort, M., May, C. R., & Williams, T. (2003). Remote doctors and absent patients:

Acting at a distance in telemedicine? *Science, Technology and Human Values*, 28(2), 274-295.

66. O'Harrow, R. (2000, December 9). Hacker accesses patient records: Thousands of files easily downloaded. *WashingtonPost.com*. Retrieved September 23, 2006 from <http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A46320-2000Dec8¬Found=true>.

69. Pineiro, R. (2004). *Cyberterror*. New York: Routledge.

71. Rigby, M. (2002). Impact of telemedicine must be defined in developing countries. *British Medical Journal*, 324(7328), p. 47.

73. Rusovick, R. M., & Warner, D. J. (1998). The globalization of interventional informatics through Internet mediated distributed medical intelligence. *Journal of New Medicine*, 2, 35-45.

76. Songini, M. L. (2000, December 15). Hospital confirms copying of patient files by hacker. *CNN.com*. Retrieved September 23, 2006 from <http://archives.cnn.com/2000/TECH/computing/12/15/hospital.hacker.idg/index.html>.

Squibb, N. J. (1999). Video transmission for telemedicine. *Journal of Telemedicine and Telecare*, 5, 1-10.

86. Turner, J. W., Thomas, R. J., & Reinsch, N. L. (2004). Willingness to try a new communication technology: Perpetual factors and task situations in a health care context. *Journal of Business Communication*, 41(1), 5-26.

89. Verton, D. (2003). *Black ice: The invisible threat of cyber-terrorism*. New York: McGraw-Hill.

90. Walther, J. B. (1996). Computer-mediated communication: Impersonal, interpersonal, and hyperpersonal interaction. *Communication Research*, 23, 3-43.

91. Walther, J. B. (1997). Group and interpersonal effects in international computer-mediated collaboration. *Human Communication Research*, 23, 342-369.

92. Walther, J. B., Gay, G., & Hancock, J. T. (2005). How do communication and technology researchers study the Internet? *Journal of Communication*, 55, 632-657.

95. Whitten, P., Sypher, B. D., Patterson, J. D. (2000). Transcending the technology of telemedicine: A case study in North Carolina.

Journal of Health Communication, 14, 109-135.

98. Wootton R. (2001). Telemedicine. *British Medical Journal*, 323, 557-560.

Address reprints to:

*Dr. Jonathan Matusitz, PhD,
Assistant Professor,
Nicholson School of Communication,
University of Central Florida,
1176 Amanda Kay Circle
Sanford, FL 32771*

E-mail: matusitz@gmail.com