FIELDING Graduate University

Psychological Effects of Cyberterrorism

FIELDING Graduate University

Kelly N. Williams, M.A., & Kristine M. Jacquin, Ph.D.

ABSTRACT

Since the mid-2000s, cyber attacks have increased in sophistication. In today's cyber world, organizations and persons are targets for cyberterrorists, who may be state entities or individuals. Cyberterrorism is used to inflict maximum chaos and confusion through the use of fear. However, the psychological costs of cyberterrorism upon the victims of the attack are widespread. Further research into the implications of cyberterrorism and the psychological toll these attacks can take is recommended.

INTRODUCTION

- Recent cyber attacks affecting the National Health Service of Great Britain, credit reporting agency Equifax, the transportation and logistics company Maersk, the U.S. Office of Personnel Management, Yahoo, and the governments of Ukraine, Estonia, and the Republic of Georgia, among others, have raised public awareness about cyberterrorism.
- The idea of an individual or state actors discovering health, financial, or other personal information is frightening.
- One study found 83% of respondents agreed that states such as China, Russia, and North Korea could and do engage in cyberterrorist activities (Jarvis, Macdonald, & Nouri, 2015).
- However, debate exists about whether cyberterrorism can be perpetuated by individuals.
- Additionally, confusion arises about the difference between hacking and cyberterrorism (Matusitz, 2014).
- While previous efforts to combat cyberterrorism focused on building better infrastructure, security experts are now studying the psychological factors behind the attacks.

- Hacking = attack on computer systems that do not destroy them
- Cyberterrorism = deliberate electronic act to coerce governments or persons for a specific objective; results in harm and generates fear (Klein, 2015; Matusitz, 2014)

PSYCHOLOGY OF CYBERTERRORISM

- In 2000, during testimony before the U.S. House Armed Services Committee, Dorothy Denning, an information security researcher on cyberterrorism, defined the act as one where the "attack should result in violence against persons or property, or at least cause enough harm to generate fear" (Klein, 2015, p. 24).
- The description of cyberterrorism is similar to terrorism as the goal is to create fear or terror or the anticipation of such a state in a civilian population for political or social gain.
- The proliferation of social media and the availability of mass media via the Internet allows cyberterrorists to take advantage of normal human psychological processes.
- For example, decreasing attention span across a busy day increases the likelihood of falling for a cyberterrorism attack.
- Frequently, people receive email or messaging requests from a seemingly trustworthy source; without thinking, many click the link and unwittingly unleash malware looking for personal or organizational material.
- The cyberterrorist plays on the person's instinctive deference to authority while supporting a lowered capacity for skepticism when the person is busy (Waldrop, 2016).
- Because cyber attacks can happen at any time, anyplace, to anyone, the psychological weight of the unknown can affect potential victims in a variety of ways.
- Although individuals are aware of the possibility of cyberterrorism, the idea that "it cannot happen to me" is at play until they are faced with the reality of such a situation.
- Recent research found that participants' fear markedly increased after watching a video clip about a weaponized computer virus that got into a cyberterrorist's hands and could be used to cause them or their families physical harm (Ayres & Maglaras, 2016).

AREAS OF FUTURE RESEARCH

- Because cyberterrorism is a relatively new concept, as opposed to hacking, further research is warranted in the area.
- Considering the underlying shared objectives, the question surfaces whether cyberterrorism is an evolution of terrorism or a separate entity.
- Additionally, as individuals tend to click on links through social media -- especially those posted by friends -- without thinking, the possibility of spreading a cyberterrorist attack increases.
- Research is needed to help social media organizations mitigate such a possibility.
- Similarly, research is needed to help identify the postings of cyberterrorists on social media sites without infringing on individuals' rights of free speech.
- Additionally, more understanding is needed of the role culture plays in the development of cyberterrorists, including state actors.
- With increasing globalization, the boundaries between gangs, criminal enterprises, terrorists, and political actors continue to blur.
- As such groups develop new alliances with each other, governments must discover new ways to determine the connections amid groups with seemingly little in common.

CONCLUSION

- Cyberterrorism is a post-modern reality meant to cause maximum chaos among the population and create situations of mass confusion, disorder, and fear (Matusitz, 2010).
- While individuals and organizations can ensure a robust infrastructure, including regular virus scans and strong passwords, cyberterrorists will still play on psychological reactions and fears to obtain their objectives.
- Every individual leaves a digital trail easy enough for a cyberterrorist to follow and exploit.
- Even if every precaution is taken, those bent on creating psychological harm will find new ways to instill fear in their victims, increasing the need for governments and companies to find new ways to stop cyberterrorism attacks.

REFERENCES

Ayres, N., & Maglaras, L. A. (2016). Cyberterrorism targeting the general public through social media. *Security and Communication Networks, 9*, 2864-2875. doi:10.1002/sec.1568

Klein, J. (2015). Deterring and dissuading cyberterrorism. *Journal of Strategic Security, 8*, 23-38. doi:10.5038/1944-0472.8.4.1460

Macdonald, S., Jarvis, L., & Nouri, L. (2015). State cyberterrorism: A contradiction in terms? *Journal of Terrorism Research, 6*, 62-75. doi:10.15664/jtr.1162

Matusitz, J. (2008). Cyberterrorism: Postmodern state of chaos. *Information Security Journal: A Global Perspective, 17*, 179-187. doi:10.1080/19393550802397033

Matusitz, J. (2014). The role of intercultural communication in cyberterrorism. *Journal of Human Behavior in the Social Environment, 24*, 775-790. doi: 10.1080/10911359.2013.876375

Waldrop, M. M. (2016). How to hack the hackers: The human side of cybercrime. *Nature, 533*, 164-167. doi:10.1038/533164a