Discussion 1.

Cyber Terrorism is nothing more than a set of new tactics to accomplish the same ends. The goals are still to get attention, do economic damage, disrupt daily routines and get revenge for real or imagined slights. What possible measures would you take to stop cyber terrorism? In your answer, anticipate any opposition to the solutions you propose and explain what they might be. (500 words or less)

Discussion 2.

Based on the four assumptions of Deterrence Theory, from your text, would digital criminals be more or less inclined to commit a digital crime? Why or why not? Are there any exceptions?  (500 words or less)

**Written Assignment: Cybercrime**

**Context:** Viruses shutting down the Internet, affiliated financial crime, Steganography, terrorist activity, identity theft, and spamming are just a few of the plethora of criminal activities that pervade the Internet today. The Internet has even been used by Russia to shut down the country of Estonia. It is important that students understand the behaviors of people who commit computer crime.

**Task Description:** Do Internet research on a cybercrime. It may be a denial of service, malicious code, Trojan horse, bullying or any other type of cybercrime. Based on the information given in Chapter 3 of your text, The Criminology of Computer Crime, and two other outside sources analyze the behavior of the person who committed the cybercrime you chose by deciding whether his or her behavior could be classified as Choice Theory, Social Structure Theory, Psychological Theory, et cetera, or a combination of them and write a 5 pages paper in APA style (not counting the title and reference pages) on your classification. Be sure and explain why you believe it fell into the category of behavior that you chose.

Chapter 3 in Taylor, Fritsch, Liederbach and Holt

Taylor, R., Fritsch, E., & Liederbach, J. & Holt, T. (2015). Digital crime and digital terrorism (3rd ed). Upper Saddle River, N.J.: Pearson. ISBN: 13:978-0-13-345890-9

American Psychological Association. (2010). Publication manual of the American Psychological Association (6th ed.). Washington, DC: Author. ISBN: 978-1-4338-0561-5 or 1-4338-0561-8 soft.

**Additional Resources**

Adler, F., Mueller, G., & Laufer, W., (2007). Criminology and the criminal justice system (6th ed). New York, N.Y.: McGraw-Hill Companies, Inc. ISBN: 13: 978-0-07-312447-8

Britz, M., (2009). Computer forensics and cyber crime (2nd ed). Upper Saddle River, N.J.: Pearson Education, Inc. ISBN: 13: 978-0-13-244749-2

Computer crime and intellectual property section. United States Department of Justice. Retrieved from <http://www.cybercrime.gov/>

Douglas, J., Olshaker, M., (2000). The anatomy of motive. New York, N.Y.: Simon and Schuster. ISBN: 13: 978-0-671-02393-5

Martin, G., (2010). Understanding terrorism: Challenges, perspectives and issues. (3rd ed). Thousand Oaks, California: Sage Publications, Inc. ISBN: 978-1-4129-7059-4

Verton, Dan., (2003). Black ice: The invisible threat of cyber-terrorism. Emeryville, California: McGraw-Hill. ISBN: 0-07-222787-7