Cyber Terrorism Research: Project Instructions

**Selection** Due Sunday of Week 5 at 11:59PM CST  
**References** Due Sunday of Week 7 at 11:59PM CST  
**Outline** Due Sunday of Week 10 at 11:59PM CST  
**Presentation** Due Sunday of Week 15 at 11:59PM CST  
**Vote** Due Sunday of Week 16 at 11:59PM CST

DISCLAIMER WARNING: This is an academic assignment being carried out as a course requirement at Des Moines Area Community College (DMACC).

You are not to do anything which could be considered illegal, malicious, unethical, or harmful. Do not use any surreptitious or unscrupulous means to gather information for your project. This is an open source intelligence (OSINT) and research gathering project. Please do not photograph, record, or make unofficial entry into any location considered to be critical infrastructure, or otherwise sensitive in nature. If you want photos, recordings, or other information involving critical infrastructure, search for the information in the public domain. Do not take any action which could be considered suspicious or illegal, or which could subject you to criminal investigation and prosecution. Use common sense.

**Objectives:**

As part of this course, we will study topics related to the security and protection of the United States from future cyber, criminal, and terrorist attacks. This course is designed to raise awareness to the vulnerabilities, anticipated threats and possible preventive actions regarding cyber crime and cyber terrorism. This project is designed using the CRJ 305 Course Competencies to ensure students successfully complete the following tasks:

1. Categorize cyber-attack scenarios.  
2. Evaluate motivators for cyber terror entities.  
3. Outline vulnerabilities of cyber-related critical infrastructure and key resources.  
5. Analyze methods of information gathering by cyber terror entities.  
6. Examine methods of communication by cyber terror entities.  
7. Relate methods of financial gain by cyber terror entities.  
8. Examine technical "tools" used by cyber terror entities.  
9. Discuss prevention/deterrence/mitigation efforts of cyber terror activities.
Selection: (5 points)

To better understand our vulnerabilities and potential defenses to cybercrime and cyberterrorism, you will pick a topic related to cybercrime, cyberterrorism and/or cybersecurity. You will research the topic of your choice to provide the class with a presentation regarding that topic before the end of the semester. The audience for this presentation will be your instructor and your fellow classmates. The topic must be pre-approved by your instructor prior to commencing with research. A list of potential topics has been provided below in which you may consider.

List of Topics

The Estonian Cyber War
Anonymous Hacking Group
Silk Road Case
Syrian Electronic Army
Iranian Hacking
U.S. Offensive Cyber Capability
Moore’s Law (Technology Expansion)
Deep Web/Dark Web
Chinese Hacking
Hacktivism
U.S. Cyber Command
Cyber Stalking
U.S. CERT
Junaid Hussain, ISIS Hacker
Distributed Denial of Service Attacks (DDoS)
Critical Infrastructure Vulnerability and Protection

Darknet Markets
Stuxnet
Terrorist Use of the Internet
Russian Cyber Attacks
Chaos Computer Club
Social Engineering Attack Techniques
Logic Bombs
Virtual Currency Threats
Malware Attacks
Cyberwarfare
Crimeware (Exploit kits)
Slaughterbots
Cyber or Electronic Jihad
Cyber Terror Bogeyman
SCADA/PLC Vulnerabilities and Protection
Kevin Mitnick, “The World’s Most Wanted Hacker”

You may choose other topics not on this list, but it must be approved by your instructor in advance of the Selection due date. Please email your instructor if you have any questions. This list is considered first come, first served. To identify your selection, please create a thread in the “Cyber Terrorism Research: Selection” discussion board. The topic you have chosen must be in the subject line of your post. The narrative of your post should include a brief description of your topic and why you wish to choose this subject. **Your Selection will be due by Sunday of Week 5.**
References:  

In a continued effort to prepare for the presentation throughout the course, you will submit a minimum of five (5) scholarly research sources regarding your approved topic in an APA formatted References list. Websites with questionable reliability (e.g., Wikipedia, howthingswork.com, Britannica.com, prezi.com, e-how.com, history.com, etc.) are not scholarly in nature and may not be used as cited references. **Your References will be due by Sunday of Week 7.** It must be submitted as a Word document attachment in the “Cyber Terrorism Research: References” **assignment.** Please contact your instruction for guidance and suggestions if you are having issues finding adequate research, or if you have problems formatting your citations.

Outline:  

You can use the outline template provided to guide your research and presentation. However, you are not bound to use this outline verbatim. Each line or category of your outline should contain a short two to four sentence explanation of the information you found on that section of your outline. Because of the varying type of research topics, you should develop an outline on your own which adequately details your research, and which effectively addresses how your topic affects our current and future cyber security.

This is an open source intelligence gathering project for the preparation of a meaningful and knowledgeable presentation on either cyber terrorism, cyber crime, or cyber security. This is not a “paper” and should not be submitted in narrative format. Correct grammar, spelling, and punctuation is expected, and scholarly research sources (minimum of 5) will need to be cited in a References list in proper APA format. The reference list should appear at the end of your outline. Websites with questionable reliability (e.g., Wikipedia, howthingswork.com, e-how.com, Britannica.com, prezi.com, history.com, etc.) are not scholarly in nature and may not be used as cited references. **Your Outline will be due by Sunday of Week 10.** It must be submitted as a Word document attachment in the “Cyber Terrorism Research: Outline” **assignment.**

Presentation:  

You will create a presentation for your peers to review. It should be fact-based, interesting, and informative.
PowerPoint is the required format for the presentation (optionally with video) and it should NOT be saved on any public websites. Use the provided PowerPoint template with the same opening and closing disclaimer slides. Do not change the design of the opening and closing disclaimer slides. Feel free to adjust the design of the slides between the disclaimer slides that contain your presentation content. If you also choose to create and use your own video, you will need to read the provided disclaimer statement from the PowerPoint template at the beginning and end of the video. Any video you make for the presentation will need to be uploaded through Blackboard to Kaltura, DMACC’s private video server (it should not be saved on any public websites).

The PowerPoint should not exceed 15 slides, not including the two disclaimer slides. (Death by PowerPoint is discouraged!) Include interesting graphics, images, and/or videos to support and enhance your presentation. All the topical areas from your outline must be included in summary form within your presentation. Your presentation must likewise include at least five (5) scholarly research sources in APA format in a References section at the end of the presentation. Presentations will be graded on content, mechanics (e.g., spelling, typos, grammar, APA format), and graphic design. Please see the grading rubric for details.

The presentation PowerPoint must be submitted in the “Cyber Terrorism Research: Presentation” discussion board as an attachment, optionally including the Kaltura Mashup for your video. Type your own name in the subject line of your post. Your Presentation will be due by Sunday of Week 15.

Vote: (5 points)

Each of you will be required to go into all of your classmates’ discussion board threads and view their presentations. You will have one week to accomplish this task. I strongly encourage you to offer feedback on each of them, as I’m sure you will also appreciate feedback.

After you review each of the presentations, you will vote for the person you believe did the best job, based on the content and delivery of his or her presentation. Your Vote will be due by Sunday of Week 16. It must be submitted as an entry in the “Cyber Terrorism Research: Presentation Vote” journal. This vote will be confidential between you and the instructor. The student who receives the most votes will be awarded extra credit. In the event of a tie, each winning student will be awarded extra credit points.
Grading Recap:

Your project will be graded on content as well as grammar, spelling, and punctuation. A grading rubric is provided for guidance. Use APA citations when directed and include a References list at the end in proper APA format. You are required to use a minimum of five (5) scholarly research sources for the outline and presentation. If required components are missing, your project will not be graded.

<table>
<thead>
<tr>
<th>Project Part</th>
<th>Points Possible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selection</td>
<td>5 points</td>
</tr>
<tr>
<td>References</td>
<td>10 points</td>
</tr>
<tr>
<td>Outline</td>
<td>25 points</td>
</tr>
<tr>
<td>Presentation</td>
<td>50 points</td>
</tr>
<tr>
<td>Vote</td>
<td>5 points</td>
</tr>
</tbody>
</table>

**Total:** 95 points