**Conduct some research of your own to find and select one act of cyber terrorism or cyberwarfare. In one to two pages, summarize the case. Who was the target of the act? Do we know who committed the act? Were they captured? If yes, how were they captured? Is there any indication of why the act was committed?**

1. This week we will focus on the issues of Cyber Warfare and Cyber Terrorism and how they are a growing threat in today’s world. Let’s start off by defining these terms. Cyber Warfare is using computers over the Internet to conduct acts of warfare against other websites or groups on the Internet. This could include defacing websites, distributing denial of service attacks, distributing propaganda, or gathering classified data over the Internet.

Cyber Terrorism is different from Cyber Warfare. Cyber Warfare can be inconvenient from having to clean up a website from vandalism or suffering from downtime because of a denial of service attack. With Cyber Terrorism, violence can result from an attack. So, as technology advances, there are more and more ways that this new technology can be taken advantage of.

China, Russia, Iran, al Qaeda, domestic right-wing hate groups, and numerous other terrorist or nation-state entities all have access to the Internet and have the tools to perpetrate a variety of cyber-attacks against the United States and/or its allies. By the very nature of these technological attacks, our critical infrastructure is most vulnerable.

There is a great deal of confusion as to what the threats against U.S. information systems really are. There is a tremendous range of domestic and international terror groups, unfriendly nations, and criminals attempting to or successfully subverting U.S. critical and economic infrastructure.

INFORMATION WARFARE is the gathering or use of information to gain an advantage over another party. It is not limited to those things that can be done with computers.
Information warfare consists of six components:

Psychological operations
electronic warfare
military deception
physical destruction
security measures
information attacks

CYBERTERRORISM cannot be concretely defined and has spurred significantly debate over exactly what it means. It is not defined by the group perpetrating it. It is specifically a premeditated, politically, or ideologically motivated attack or threat of attack against information, computer systems, computer programs, and data that can result in violence against civilian targets.

Cyber Warfare and Cyber Terrorism have both similarities and differences. They are similar in that both involve using computer systems against other computer systems, although with Cyber Terrorism the physical system can also be targeted. They are both different because in Cyber Terrorism, violence can occur, such as people be can be hurt or killed.

REASONS FOR ATTACK

There are many reasons why these attacks occur. Probably one of the main reasons is to state a goal or objective that disagrees with a view of another community. For example, an anti- abortion group defacing an abortion clinic’s website, or performing a denial of service against a website so that people cannot access it and receive information from it. These would be acts of Cyber Warfare. Mostly with Cyber Warfare though, some of the defacement and denial of service attacks will come from people who just do that sort of thing for fun because they think they can.

With Cyber Terrorism, these attacks occur because of numerous reasons. The word terrorism itself has the word terror in it, which means to strike fear and dread into an individual. There have been many Terrorism attacks throughout history, including the one on September 11, 2001. With Cyber Terrorism, it uses that fear and dread by utilizing it over the Internet to attack computer systems that control numerous things, hacking government websites and stealing top secret information that could be used against that government by the terrorists. Similar to Cyber Warfare, most terrorist goals, besides striking fear into other groups and nations, is to convey a political message to the government or nation that they oppose.

US NATIONAL INFRASTRUCTURE

The US national infrastructure is critical to day-to-day activities. Without it, airplanes could not fly, banks could not conduct financial transactions, emergency services would cease to function, and the government would lose its control. Therefore, without the national infrastructure, our national security would be in imminent danger.

The Internet is a critical tool for political and social movements of all types around the world. Few Americans have considered a situation involving an attack on our infrastructure. Today, attacks against U.S businesses and governments are commonplace, with an estimated 100 million attempts each day.

The United States has identified itself as the most infrastructure reliant nation on Earth. The following is a list of critical infrastructures each with a brief description that the United States deems to be of extreme importance.

* TELECOMMUNICATIONS: To include Internet, cable, cellular, telephone, satellite, and any other medium that connects systems together.•
* ELECTRIC POWER•
* OIL AND GAS TRANSPORTATION: From the Alaska pipeline to oil refineries to natural•
gas distribution.
* TRANSPORTATION: Ground deliveries, air traffic control, and trains. All of which play a•
huge role in delivering food and materials, driving businesses and tourism.
* BANKING AND FINANCE: The movement of trillions of dollars of virtual money through•
brokerages and banks over computer wires and networks.
* WATER SUPPLY: Managing the water supply and waste disposal is done by electronic•
means.
* EMERGENCY SERVICES: 911, fire and police departments, rescue units all rely upon the•
communications networks to do their job with speed and efficiency.
INFORMATION ATTACKS
Information attacks are less destructive forms of cyber-attack that terrorist groups or adversarial nations could employ that achieve information warfare objectives. Examples of these types of attacks include: 1) web-site defacement, 2) cyberplagues including viruses and worms, 3) distributed denial of service attacks, and 4) unauthorized intrusions.

Assignment

What turns people into terrorists? That question might sound simple, but it's at the heart of the struggle to prevent terrorist attacks. Take a look at some of the people who have tried to do us harm in the last few years.

* Umar Farouk Abdulmutallab, son of a wealthy banker, grew up in Nairobi, attended boarding school and college, and lived in an expensive London neighborhood. Chat room posts show that he worried about his school test scores and about girls — and felt lonely. He traveled to Yemen between high school and college to study Arabic. His classmates at University College London described him as quiet, easy to overlook. He tried to detonate explosives hidden in his underwear while onboard Northwest Airlines Flight 253, Christmas Day, 2009.•
* Najibullah Zazi, born in Afghanistan in 1985, lived in Pakistan before moving to New York with his family when he was 14. Zazi attended a local mosque and dropped out of Flushing High School, and worked at the family's coffee-and-doughnut cart near Wall Street. In his early 20s, he traveled to Pakistan for an arranged marriage, fathered two children and traveled back to New York to work but wound up deeply in debt. Zazi tried to join the Taliban in 2008; Al Qaeda recruited him instead. In 2009, he headed to New York from Colorado with the makings of a bomb intended for the New York subway.•
* Tamerlan Tsarnaev was an angry young man who, according• to the Boston Globe, told his mother he heard voices in his head. He never managed to achieve his own idea of the American dream, and instead turned to a radical form of Islam adopted by fighters in Dagestan, his homeland. In 2013, Tsarnaev and his brother were accused of bombing the Boston Marathon.
* These examples show that moving from radical beliefs (which are protected under the Constitution) to willingness to engage in violence is a highly individualized process. There is no one way to get there, no specific belief that causes someone to turn. It's also difficult to separate psychological issues from political motives.

**Conduct some research of your own to find and select one act of cyber terrorism or cyberwarfare. In one to two pages, summarize the case. Who was the target of the act? Do we know who committed the act? Were they captured? If yes, how were they captured? Is there any indication of why the act was committed?**