SPECIAL TOPIC

Cyber Warfare/Terrorism

PURDUE UNIVERSITY | Polytechnic Institute

Objectives

- Differentiate between warfare and terrorism and other mechanisms for social change
- Identify examples of potential cyber warfare activities
- Define criteria for determining if a cyber attack is an act of cyber warfare
- Utilize adversarial thinking to identify methods of manipulation by attackers

Warfare V. Terrorism – Agents of Change

	Using solely peaceful means to affect political change	Using violence as a means to affect political change
Working within the structures of formal government	Creation of laws, policies, governing bodies, etc.	Traditional warfare
Working outside the structures of formal government	Civil disobedience, conscientious objection, peaceful protest, etc.	Terrorism

Terrorism is a relative term

Terrorists are labeled as such because they are working against the formal/official governing body. When such agents use violence to bring about political change, they are labeled by the governing body as terrorists

That does not mean they are not working to right some wrong – the official governing body could be torturous, corrupt, human rights violators – it just means they are not the official governing body.

When people support the legitimate government, they see the terrorists as wrong. As an alternative point of view, the British citizens who fought for independence on the American continent were, by this definition, terrorists. We see them as on the moral/right side.

Possible Examples of Cyber Warfare

- Estonia
  - Beginning in April 2007, the websites of a variety of Estonian government departments were shut down by multiple DDoS attacks immediately after a political altercation with Russia.
- Iran
  - The Stuxnet worm attacked a particular model of computer used for many production control systems, and all the infections could be traced back to domains within Iran linked to industrial processing.
- Israel and Syria
  - Missiles fired in 2007 by Israeli planes did not show up on Syrian radar screens because software had replaced live images with fake, benign ones.
- Canada
  - In January 2011, the Canadian government revealed that several of its national departments had been the victims of a cyber attack traced back to servers in China.
- Russia
  - According to the *New York Times*, Russian hackers infiltrated the computers of various national governments, NATO, and the Ukraine.

Mechanisms of Change – Psychological Manipulation

- Tactic of Russian cyberwarfare includes Troll Farms
- Individuals who are fluent in English go to work for eight hour days.
- They have studied US culture carefully
- They know what issues divide us
- They post in social media forums inflammatory posts to enrage all sides of the political spectrum
- They light a match, and watch it burn
- We are being manipulated and we need to exercise caution about information we consume
- This is a highly successful method of social change

Election security as a response to cyber warfare

Discussion

Cyber Warfare

- Open questions:
  - When is an attack on cyber infrastructure considered an act of warfare?
  - Is cyberspace different enough to be considered a separate domain for war, or is it much like any other domain (e.g., land, sea, or air)?
  - What are the different ways of thinking about cyber war offense and defense?
  - What are the benefits and risks of strategic cyber warfare and tactical cyber warfare?