Cyber-Terrorism: A Question of Intent

What is Cyberterrorism?

* No concrete definition – it is difficult to determine the identity, intent, or political motivations of an attacker.
* The use of computers as weapons.

Types of Cyberterrorism

* Use of technology to supplement terrorist activities such as recruitment, propaganda, communication

Hybrid Cyberterrorism

* Propaganda
  + Social media platforms such as Facebook, Twitter, and YouTube are being used to spread terrorist propaganda.
  + ISIS owns seven media agencies that broadcast to various countries including the United States
  + Telegram – an communication app known for its privacy – has become widely adopted by terrorists after Facebook and Twitter began cracking down on accounts.
* Communication
  + Messaging apps such as Kik, WhatsApp, and Telegram have been used to coordinate attacks and issue instructions.
    - The Reina nightclub attack in Turkey that left 39 dead and at least 70 wounded was coordinated using Telegram.
    - The St. Petersburg metro bombing that killed.
* Fundraising
  + Donations are collected through crowdfunding platforms that lack proper security and verification.
  + Bitcoin and other cryptocurrencies are popular among terrorist groups due to their anonymity.
* Data Mining
  + Terrorist groups use the Internet to collect information on places and individuals.
  + In the September 11 attacks, al-Qaeda
* Recruitment
  + Social media platforms have been used to recruit members from around the globe.
  + Recruiters analyze Facebook profiles and conversation threads to find potential recruits.

Pure Cyberterrorism

* Physical Attacks
  + The use of conventional weapons or direct manipulation of equipment on a computer system.
  + Meant to disrupt the reliability of computer equipment and the availability.
* Electronic Attacks
  + Can penetrate computer facility walls and erase electronic memory, upset software, or permanently disable electronic components.
  + Military experts have stated that the United States is perhaps the most.
* Cyberattacks
  + Attacks that use malicious code to alter program logic.
  + Usually requires the target computer to have a flaw in security that can be exploited.

Why Cyberterrorism?

* Gathering and sharing information over Internet is faster and easier.
* Increased physical security may encourage terrorists to look for lower-risk alternatives.
* The high rate of information exchange makes it easier to spread the effects of a cyberattack.

Susceptible Technology

* Supervisory Control and Data Acquisition (SCADA) systems may be vulnerable as they are typically fully automated.
* Commercial technology used by the government is especially vulnerable.
  + The cost of security may be too high to meet demands.
  + Offshore outsourcing to foreign countries could result in malicious code inserted into a system.

SCADA Cyberattacks

* In December 2015, a cyberattack on a Ukrainian power grid shut down 30 substations and left 230,000 citizens without power.
* Using spear – phishing emails containing malware, hackers seized SCADA control, disabled critical components, and destroyed files.
* In 2013, Iranian hackers accessed the core control system of a dam in Rye Brook, New York using only a cellular modem.
* This attack targeted administrative and business sectors in an attempt to steal employee login information.

Preventing Cyberterrorism

* Regulate social media to detect terrorist propaganda, communications, and recruitment.
* Restrict sensitive information online to prevent terrorist data mining.
* Strengthen cooperation between the government and private companies.
* Promote cybersecurity awareness.
* Detect and remove vulnerabilities in critical systems.
* Develop trust between citizens and government.

Questions

* Do you think that the average person should be concerned about a cyberterrorist attack?
* Do you think that privacy is a necessary sacrifice in preventing cyberterrorism?
* How much of a role do you think the government should play in regulating security for new technology?
* To what extent do you think the government would use a serious cyberterrorist attack to impose regulations on the Internet?

What is the Silk Road

* First modern darknet market

Tor and Bitcoin

* Tor is a free web browser often used to navigate the darknet due to its ability

Ross Ulbricht

* Pseudonym was “Dread Pirate Roberts”
* $28.5 million net worth
* Currently serving life in prison
* Libertarian
* Physics student turned self-taught programmer

Things Available on Silk Road

* Almost every known drug
* Drug paraphernalia
* Medical Supplies
* Rare energy drinks
* Fake IDs

Things Banned on Silk Rad

* Child pornography
* Stolen credit cards
* Hitmen
* Weapons

Features of Silk Road

* Detailed guide available to all sellers showing them various things such as how to vacuum seal their goods to avoid detection in the mail.
* Seller reviews to allow buyers to find the best sellers and avoid the scammers
* Anonymous payment system
* A book club

How Silk Road Handled Funds

The Silk Road Book Club

* A new book was chosen weekly in an attempt to provide some form of community and discourse
* Some of the books that were read were: Anatomy of the State, The Color Purple, The Invisible Man, The Absolutely True Diary of a Part-Time Indian, The Anarchist Cookbook.

Enter the Hitman

* Silk Road user “FriendlyChemist” managed to get a list of Silk Road customers and demanded $500,000 to keep quiet
* Ulbricht then hired a hit on “FriendlyChemist”
* In the available transcript, Ulbricht said that he had already commissioned another hit before FC
* Other hit attempts were made after including

How Ulbricht was brought down by Google

Ulbricht’s Parents

Darknet After Silk Road

* After the Silk Road shutdown, it left the framework for other sites to follow in its place
* AlphaBay was one of the more prominent successors

Discussion Questions

* If drug trafficking could be kept online and off the streets, do you believe that drug violence would be lowered?
* Thoughts on the Silk Road/Ross Ulbricht?
* Thoughts on how two years of FBI investigation was beat by a guy on Google for a weekend?