Threat Morphing in Cyberspace

Susan W. Brenner
NCR Distinguished Professor of Law & Technology
University of Dayton School of Law
Threats
Nation-states

- Territorially-based sovereignty
- Divide threats into
  - Internal
    - Crime
    - Terrorism
  - External
    - War
War, Crime & Terrorism: RW

- **War:** attack = “outside”
  - By another nation-state
  - Goal: Conquest/strategic

- **Crime:** inside attack
  - Civilian on civilian
  - Goal: Profit or passion

- **Terrorism/crime**
  - Historically, inside
  - Civilian on gov’t
  - Goal: ideological
Threat Control =

- Attribution
  - Attack
    - War? Crime? Terrorism?
  - Attacker
    - Nation-state?
    - “Pure” civilian?
    - Terrorist civilian?

- Response
  - Law enforcement
  - Military
Attribution Analysis: RW

- **Markers**
  - Point of attack *origin*
  - Point of attack *occurrence*
  - Motive for attack

- **War**
  - Points of origin & occurrence differ
  - Motive = sovereignty (military targets)

- **Crime/terrorism**
  - Points of origin & occurrence usually same
  - Motive: personal (profit or passion) or ideological
Threat Morphing
E-stonia

- Highly wired country
- All of its 1.4 million residents have free wi-fi
- Wi-fi at home, trains, buses, schools, etc.
- Electronic ID cards mandatory since 2002
- Online banking and commerce common
Tallinn: April 27, 2007

- Authorities moved statue of WWII Russian soldier from park to military cemetery
- Sparked protests among Russian-speaking minority in Estonia
- After 2 nights of riots
- Cyberattacks began...
Russian-language chat rooms

- Posts called for coordinated attack on May 9, day Russia celebrates WWII victory

- “On the 9th of May a mass attack is planned. The action will be massive — it's planned to take Estonnet down :)."
April 29, 2007

- Attacks began with a flood of junk email that shut down Parliament’s email server
- Website hacked and fake letter of apology from Prime Minister posted on it
- Estonia’s CERT director summoned security experts from banks, businesses and police to plan country’s defense
First week . . . To May 9

- Attacks continued on various systems
- Estonians able to keep systems pretty much up and running
- Sacrificed some systems to save others
- Knew it would get worse
May 9 & 10

- Peak: 58 sites down (banks, media, etc.)
- Estonia took some systems offline
- Severed links to outside world
- 128 unique DDoS attacks
- Some lasted an hour, one over 10 hours
War?? Russia?

- Estonians believed attacks were launched by Russia and therefore were cyberwar
- Based that on the facts that
  - Attacks were planned and orchestrated using Russian-language chat rooms
  - Traced IP addresses to Russian agencies, including PM Putin’s office
  - Traced to other Russian servers
“NATO does not define cyber-attacks as military action. This means . . . Article V of the North Atlantic Treaty, or collective self-defence, will not be extended to the attacked country," said Estonian defence minister, Jaak Aaviksoo.
Aftermath . . . . Not-war?

- Attacks used rented botnets
- They ended when the rent ran out
- U.S. analysts: “more like a cyber riot than a military attack”
- Consensus: no state actor
03/10/2009: Responsibility?

- Konstantin Goloskokov said Russian youth group Nashi launched the attacks
- “Taught the Estonian regime a lesson”
- Nashi
  - Works for Kremlin
  - Privately-funded by business owners seeking favor w/Kremlin
Estonian Attribution. ????

- Attack?
  - War?
  - Crime?
  - Terrorism?

- Attacker(s)?
  - Russia? Hackers?
Estonian Response...?
CYB3RCRIM3

http://cyb3rcrim3.blogspot.com

susanwbrenner@yahoo.com