Cyber War

Objectives

TOWSON UNIVERSITY

- Understand cyberwarfare.
- Understand cyber terrorism.
- Identify the US's four primary Nation State cyber adversaries.
- Describe the significant cyberwarfare issues relevant today.
- Understand the basics of information warfare.

The History

- Communications interception evolved into cyberwar.
  - *Civil War*: Generals sent fake messages to throw off enemies.
  - *World War II* – Enigma.
  - *Cold War* – intercept phone lines and radio signals.
- President Obama received daily cyber attack briefings.
- Established the "Cyber Command".

Eligible Receiver Attack (NSA ,1997)

TOWSON UNIVERSITY

- Clinton administration minimized the 'cyber problem'.
- NSA launches the "eligible receiver":
  - Simulated attack.
  - Goal: penetrate all department of defense (dod) networks in 2 weeks.
  - Exercise completed in 4 days.
- All DoD networks penetrated
  - Including the national military command center that transmits wartime orders from president.
- Result: DoD installs intrusion detection systems.

Moonlight Maze Attack - 1998

TOWSON UNIVERSITY

- Hackers access files at the Wright-Patterson Airforce Base (OH).
- Attackers were attracted by HoneyPot.
- IP identified to be at the Russian Academy of Sciences.
- A US delegation at Moscow confirms Russian government agents involved in attack.

Political Attacks (2014)

- CEO of Las Vegas Sands, Sheldon Adelson, proposes to detonate a small nuclear bomb in the desert to warn Iran.
- In 2014, Las Vegas Sands is hacked.
- 20,000 machines affected and data destroyed.
- Homepage of company defaced
- Traced to Iran.
- Same year, Sony Motion pictures attacked by North Korea.

Foreign Attacks

- Center for Strategic and International Studies (CSIS) https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents
- 2015: China / U.S - OPM - Theft
- 2014: Anthem / Unknown - Theft 80 mil medical records
- 2013: Iran / U.S - Natanz - Retaliation - Theft / Fraud
- 2010: U.S. / Iran - Stuxnet Worm- Sabotage
- 2007: Russia / Estonia - DDOS – Sabotage

SolarWinds (2020)

- Provides network management software to fortune-500 companies and many government agencies.
- Software update – hackers planted malware.
- **Supply chain attack**, affected:
  - Federal reserve, department of justice, state department.
  - Department of homeland security.
  - National institutes of health, CDC.
  - NSA, NASA and U.S. Nuclear weapons agencies.
  - Just a few of the affected companies include microsoft, visa, at&t, lockheed martin, ernst & young, yahoo!, And the new york times.

Discussion

- What are the traditional battlegrounds for war?
  - Hint (there are 4)
- Why is cyberspace considered the Fifth?
- Do you think we need a national academy for cyber?

Cyberwarfare

- Use of digital attacks by one country to disrupt the vital computer systems of another, with the aim of creating damage, death and destruction.
- 5th Dimension of War, 5th Battlespace.
- Exploit weakness, steal information, or conduct sabotage.
- Significantly increased over the last decade.
- Thousands of attacks daily.

BLUF (Bottom Line Up Front)

TOWSON UNIVERSITY

- Requires minimal cost and effort.
- Can impose a tremendous amount of damage on a global scale.
- Defies traditional strategies of border control and national defense - No borders!
- Anonymous.
- Attack all information systems in the physical world, Including critical infrastructure.
- Equal or supersede conventional weapons of war.

Cyberwar
the 'rules' don't apply

TOWSON UNIVERSITY

- Occurs in a largely ungoverned virtual space.
- Existing protocols fall short.
  - conducting operations in *accordance with the laws and customs of war.*
  - Hague and Geneva Conventions.
  - Tallinn Manual on the International Law Applicable to Cyber Operations (2013).
- No laws for cyberspace arm control.
- Cyber operations = offensive.
- "franchising" out .
  - => increased collateral damage.
  - more risk to civilian populations (e.g.individual citizens, private industry, etc.)
  - Anonymity.

Weapons of cyberwarfare

TOWSON UNIVERSITY

- Software that can be digitally deployed to disrupt an adversary's critical infrastructure.
  - Including viruses, worms, trojans, etc.
- Same weapons for cyber criminals, hacktivists or other malicious cyber actors.
- Standard cyber **intelligence** collection.
- Social engineering techniques.
  - Used to insert malware.
  - Exploit data and system vulnerabilities along a target's supply chain.
  - Phishing and spear-phishing.

Artificial Intelligence

TOWSON UNIVERSITY

- Defense
  - Pattern analysis.
    - Strives to identify any behaviors that are indicative of an attack in progress.
  - Big data.
  - Data analytics.
- Offense
  - Artificial intelligence to scale attacks.
  - Impersonation of trusted users.
    - Deepfakes.
    - Next frontier for financial fraud, hoaxes, and fake news.
  - Blending into the background.
  - Faster attacks with more consequence.

Who is the Enemy?

- Individual Hackers
  - Lone political actor?
- Hacktivist Groups
- Criminal Organizations
  - Financially motivated
- Corrupt Businesses
- Terrorists
- Foreign Military or Government
  - powerful nation states

Adversaries

- Nation States cyber actors.
  - Foreign countries that are actively attempting to infiltrate US industry and military for nefarious reasons.
- Intelligence briefings list the major cyber threat actors to the US as:
  - **Russia**
  - **China**
  - **Iran**
  - **North Korea**

Cyber Terrorism

TOWSON UNIVERSITY

- According to the definition of the FBI:
  - Premeditated.
  - Politically motivated.
    - Attack against information, computer systems, computer programs, and data.
  - Typically, loss of life in a cyber attack would be less than in a bombing attack.
- Simply stated:
  - The use of computers to launch a terrorist attack.
  - Like other forms of terrorism, only the milieu of the attack has changed.

Cyber Terrorism

- Significant economic damage.
- Disruptions to communications.
- Disruptions in supply lines.
- General degradation of the national infrastructure.

All possible via the Internet.

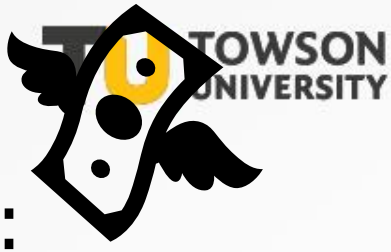
All these could lead to significant deaths: train wrecks, hospital deaths, loss of air traffic control resulting in plane crashes, and so forth.

Motivation for attacks

TOWSON UNIVERSITY

- Radware(2018), showing the motives behind why hackers hack:
  - Ransom (41%)
  - Insider threat (27%)
  - Political reasons (26%)
  - Competition (26%)
  - Cyberwar (24%)
  - Angry user (20%)
  - Motive unknown (11%)
- Over 80% of security breaches were a result of phishing attacks.
- 60% of security breaches occurred due to unpatched vulnerabilities.
  - CSO Online reports.
- Attacks on IoT devices grew threefold in early 2019.
- Office files comprised 48% of malicious email attachments (Broadcom).

Economic Attacks



- Cyber attacks cause economic damage:
  - Lost files and records.
  - Destroyed data.
  - Stolen credit cards.
  - Money stolen from accounts.
  - Time the IT staff spends cleaning up.
- These cyber attacks are not necessarily terrorist attacks.
- Concerted and deliberate attack against a particular target
- Exclusive purpose of causing direct damage.

Economic Attacks (cont.)

TOWSON UNIVERSITY

- Any organization wanting to do harm could set up a group with:
  - Computer security experts.
  - Programming experts.
  - Networking experts.

Ransomware – Baltimore

- Ransomware variant Robinhood, May 7 2019.
- Demanded 13 bitcoin (roughly $76,280 in 2019. Today ~ $336,714)
- Shut down government servers, other applications:
  - Employee email systems.
  - Phone lines.
  - Online billing systems used by the city.
- Cost $18 million.

Military Operations Attacks

TOWSON UNIVERSITY

- Hack into dod, CIA, or NSA systems:
  - Ultra-secure.
  - Would be met with immediate arrest.
- Other attacks on less secure systems:
  - Systems that protect the logistics programs.
  - Could also put our country at risk.
- These agencies are well protected. But how about lower levels, which can be used by hackers in reconnaissance to glean info for social engineering?
- Describe the difference between **offensive** and **defensive** cyber activities.

Information Warfare

TOWSON UNIVERSITY

- Attempt to manipulate information in pursuit of a military or political goal:
  - Use computers to gather information.
  - Use computers to disseminate propaganda.
- Information control.
  - Since world war ll, part of political and military conflicts.
- Democratic national convention hack.
- Election compromise.

Information Warfare (cont.)

TOWSON UNIVERSITY

- **Propaganda**
  - Information, ideas, opinions, or images, often only giving one part of an argument, which are spread with the intention of influencing people's opinions.
  - "Fake news"
  - People often believe and repeat what they see online.
- **Information Control**
  - Closely related to propaganda.
- **Disinformation**
  - False information planted in relatively secure systems.
  - More difficult to acquire, implies more value.

Actual Cases

- In Tehran [Iran],
  - Armed forces and technical universities join.
  - Create independent cyber R&D centers.
  - Train personnel in IT skills.
  - Try to buy it technical assistance and training from Russia and India.
- Russia
  - Armed forces have a robust cyber warfare doctrine.
  - Moscow also has a track record of offensive hacking into Chechen web sites.
  - Assumed that Russia's intelligence services or armed forces would attack U.S. Networks.

Actual Cases (cont.)

TOWSON UNIVERSITY

- Russia's armed forces have developed a robust cyber warfare doctrine.
- Moscow also has a track record of offensive hacking into Chechen Web sites.
- Available evidence is inadequate to verify whether Russia's intelligence services or armed forces would attack U.S. networks but it is assumed.

Defense Against Cyber Terrorism

TOWSON UNIVERSITY

- Research and academic programs dedicated to security.
- Computer crime recognized.
- Computer crime specialists – used by police departments and military.
- Forums used by security professionals to report and discuss emergencies. (US CERT)

Elections

- More than 80 elections held all over the world in 2020.
- Both politicians and hackers will try to meddle with voters' choices.
- What cyberwar activities occurred during the 2016 elections?
- What can I do??
  - "Voters should stay vigilant and double-check all the news coming their way."

Today- COVID-19

- Lockdown.
- WFH – remote work is more vulnerable.
- More phishing.
- cyberattacks **targeting organizations** have increased considerably.
- Nation-state cyber activity has surged in intensity and severity.

Summary

The bad guys look like good guys.

Training and vigilance is needed at all ages.

This is the future of Terrorism and War.