CYBER CONFLICT & CRITICAL INFRASTRUCTURE

CS 610 TERM PROJECT – THOMAS LIAO

TABLE OF CONTENTS

CYBER ESPIONAGE

US F-22

China J-20

CYBER ESPIONAGE

	US F-22	China J-20
Top speed	1,498 mph	1,305 mph
Range	1,839 mi	2,113 mi
Length	62’	67’
Wingspan	44’	42’
Weight	43,430 lbs.	43,000 lbs.
Manufacturer	Boeing Defense, Space & Security, Lockheed Martin Aeronautics	Chengdu Aircraft Industry Group

STUXNET

- [covered in class]
- 3 components:
  - Worm: payload of attack
  - Link file: executes propagated copies of the original attack
  - Rootkit: hides the malware from detection
- Attack 0 – suspected US and Israel attack on Iran's nuclear facilities (Natanz)
  - Used 4 zero-day exploits, present on 300,000+ devices, only attacked specific systems in Iran
  - Unclear impact on nuclear program (some claim success, others failure) – but, triggered a cyberweapons race

NORTH KOREAN ATTACKS

- ICS (Industrial Control Services) attack
  - Attempted but ultimately unsuccessful attempts to disrupt American utilities companies
  - Gained entry to 16 company's systems (FireEye) through phishing
- WannaCry attack
  - Ransomware affecting over 200,000+ legacy Windows systems internationally
    - Known issue where Microsoft had released patches – many victims had not updated
  - Requested Bitcoin to unlock the computer, ultimately received $130,000 in 137 payments, but accrued up to $4 billion in economic damages (Cyence)

RUSSIAN ATTACKS

- Context: 2014 invasion of Crimean Peninsula, part of war with Ukraine
- State-sponsored group: Sandworm
- (2015) Black Energy
  - Targeted ICS / SCADA, energy, government and media in Ukraine
  - Caused outages for 225,000 customers with Oblenergos; other companies and government also affected
- (2016) Industroyer
  - Highly sophisticated, adaptable, automated grid-disrupting piece of code used on Ukrenergo
  - Introduces backdoors on power distribution companies and sets up communication with a remote server; maliciously uses communication protocols in their intended fashion

CRITICAL INFRASTRUCTURES INCLUDE…

"those used for, inter alia, the generation, transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health—and the critical information infrastructures that increasingly interconnect and affect their operations".

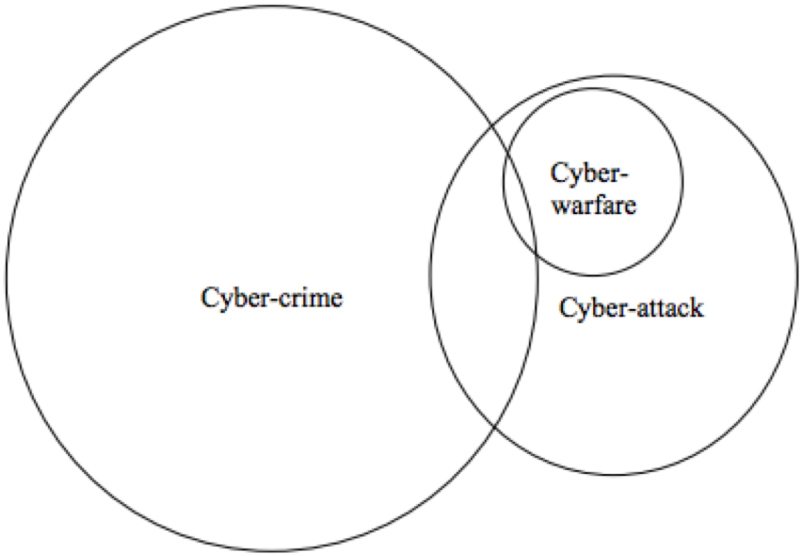
- UN General Assembly

THE FOCUS

TABLE 1: Essential characteristics of different cyber-actions

	Type of cyber-action		
	Cyber-attack	*Cyber-crime*	*Cyber-warfare*
Involves only non–state actors		√	
Must be violation of criminal law, committed by means of a computer system		√	
Objective must be to undermine the function of a computer network	√		√
Must have a political or national security purpose	√		√
Effects must be equivalent to an "armed attack," or activity must occur in the context of armed conflict			√

FIGURE 1: Relationship between cyber-actions



QUESTIONS

Cyber attacks on critical infrastructure…

- How should we best prevent an attack on critical infrastructure?
  - Domestic + foreign policy relationships
  - Perspectives on cyber defense
- How should we respond to cyber attacks on critical infrastructure?
  - Foreign policy response

US RELATIONSHIPS…

- Domestic policy
  - Private corporations
  - Private consumers
- Foreign policy
  - Allies (NATO, etc.)
  - Russia, China, Iran, and North Korea

PREVENTING ATTACKS – DOMESTIC POLICY

- Regulation on corporations mostly geared towards disclosure of data breaches
- in utilities, Federal Energy Regulatory Commission uses the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Version 5 standards
- Expectations of security come when choosing contractors for military deals
- Difficult with companies and consumers because…
  - Lack of trust, liability concerns and ill-defined objectives
  - Consumers have incentive to favor functionality and convenience over safety

PREVENTING ATTACKS – FOREIGN POLICY

- Only foreign policy at stake
- International law is ambiguous
  - Fundamental question: Can cyber operations trigger an armed conflict?

FOREIGN - US NORMS (2015)

Nations should…

- **Not launch or support cyberattacks that intentionally damage or impair other nation's critical infrastructure;**
- Not launch cyberattacks that intentionally prevent other nations' cyber emergency responders from dealing with cyber incidents or use their own such teams to launch cyber attacks; and
- Cooperate with other nations' law enforcement investigations into cybercrime, or efforts to stop cyberattacks, launched from their territories

Not included:

- Reference to Article 51

PREVENT ATTACKS – TECHNICALLY (FINANCIALLY)

- Best practices:
  - Red-team (penetration testing) + blue-team (live network defense)
  - air gaps between critical information storage
  - Employee training – re: phishing
- How much money should companies invest?
  - Depends (on what is being protected and the current state of affairs) – mostly about shoring up the weakest links
  - Up-to-date hardware and software

POST-ATTACK: RELATING CYBER TO KINETIC OPERATIONS

- *Tallinn Manual* put forth 8 non-exclusive factors to guide inquiries:
  - Severity
  - Immediacy
  - Directness
  - Invasiveness
  - Measurability of effects
  - Military character
  - State involvement
  - Presumptive legality
- International Court of Justice: "scale and effects"
- How to balance harm to systems/economies versus harm to individuals and lives?
- Shortcomings of the effects test and intent (foreseeable consequences)
  - Potential for damage – difference between kinetic operations and cyber operations

OTHER COMPLICATING FACTORS

- Idea of self-defense in cyberoperations
  - Pre-emptive retaliation
  - temporal issues?
- Who may be targeted in a cyber attack? Civilians?
- Neutrality and obligations?

CONCLUSION

- Prevent cyber attacks
  - Invest in cyber security based on what is being protected, and how its currently being protected
- Proportional response post-attack
  - 8 factors of the *Tallinn Manual*, + potential for damage?
    - Inherent limitations

QUESTIONS?