CMSC 304 Computer Ethics

Slides drawn from:
Cyberwarfare and Cyberterrorism: In Brief, Theohary & Rollins
Ethics of Cyberwar Attacks, Rowe
Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate - Foltz

1

What is cyberwarfare?

- **State-on-state action equivalent to an armed attack or use of force**
  - Actions by a nation-state to penetrate another nation's computers or networks for the purpose of causing damage or disruption
- Must be performed by legal states or state-supported/condoned actor
- Intended to create damage or disruption
- Targeted at another state/political entity
- May trigger a military response with a proportional use of force
- Distinguishable from cyberterrorism; can argue about cyberspying

Clark & Knake 2010

2

Legal framework

- Legislation has not kept pace with technology
- States are reluctant to sign treaties that constrain their own operations
- Relevant warfare frameworks: Hague Conventions; Geneva Conventions
- Prohibit:
  - Weapons that cause unnecessary suffering
  - Attacks whose effects cannot be controlled
  - **Disproportionate civilian damage** (collateral damage)
- The UN charter: Members shall refrain … from the threat or use of force against the territorial integrity or political independence of any state

3

Types of cyberattacker

- Cyberwarriors: agents or quasi-agents of nation-states who undertake cyberattacks in support of a country's strategic objectives
- Cyberterrorists: non-state actors who engage in cyberattacks to pursue their objectives
  - "State sponsored" actors usually fall here unless formally acknowledged by a government – this is a gray area because it's easy to disavow cyber actors
- Cyberspies: steal protected, cla
- Cyberthieves: engage in illegal c
- Cyberactivists: hackers, hacktivi financial reasons

- Not mutually exclusive
- Not clearly delineated/defined

4

What is a cyberattack?

- **Severity: the more severe the results, the more likely to qualify**
- Immediacy: Consequences that manifest quickly are more likely to be an attack
- Directness: attacks are more immediately responsible for damage
- Invasiveness: attacks impair the territorial integrity or sovereignty of a state/enter more secure or separated systems
- Measurability: attacks have quantifiable, identifiable consequences
- Presumptive legitimacy: if something is legitimate outside the cyber domain, it remains legitimate (e.g., propaganda, espionage)
- Responsibility: created and propagated by state actors

Schmitt 2011, Foltz 2012

5

Counter-attacks

- Form of attack most widely considered "ethical"
- Counter-attacks permitted even during peacetime
- Complicated for cyberattacks:
  - Difficulties in attribution: are you counter-attacking the right people?
  - Difficulties in control: possibility of collateral damage
  - Difficulties in timeliness: large-scale cyber-attacks must be prepared in advance
  - And the usual: what counts as a cyber-(counter)attack?

6

6

Interpreting cyberattacks

- Spread, scope, and severity of damage are not always obvious
  - Hard to tell when computers are affected/infected and by what
  - Some attacks are self-deleting after some time or number of actions
- May lead to over-large attacks / lack of "pinpointing"
- Attacker is not always obvious: plausible deniability
  - Attacker can be made to look like someone else
    - This is probably illegal
- Intended victim is not always obvious
  - Who is entitled to counterattack?

7

7

When is an attack ethical?

- When it is **justified** (counterattack, attacks during war, …)
- When there is no (or very limited) collateral damage: Noncombatant immunity during the attack
- When the attack is appropriate to the provocation: Proportionality of the size and scope of the attack
- When the attack does more good than harm
- We are not sophisticated enough to guarantee any of these in cyberwarfare

Arquilla, 1999

8

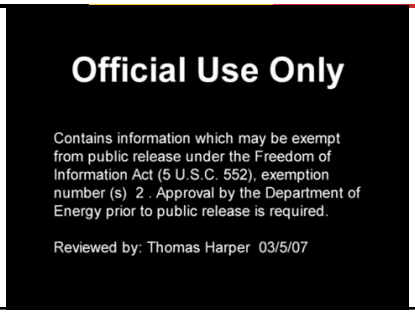
Collateral damage

- It's hard to reduce/prevent collateral damage
  - Computers under attack are rarely or never isolated
    - In fact, attacks usually depend on a route through many systems
    - Considerable exploratory attacking needed to even find the route
  - Cyber-attacks can be conducted by small groups that don't have the resources to ensure precision
- There are still mechanisms to do so
  - Precisely targeting payloads: be selective in what is attacked/affected
  - Design damage to be repairable by the attacker
    - This one is more theoretical

9

9

Cyberattacks on physical systems



Project Aurora: Opening circuit breakers on a 27-ton diesel generator

https://youtu.be/LM8kLaJ2NDU

10

Other ethical problems with cyberattacks

- **Wasteful of resources:** Expensive to develop and can generally be used only once
- **Depends heavily on secrecy:** encourages internal lack of clarity about actions of a government, leads to disconnect between a government and the people governed
- **Difficulty of precise targeting:** many cyberattacks have ended up "out of control" and doing extensive collateral damage
- **None of these is characteristic of a good weapon**

11

11

Stuxnet

- August 2010 – Stuxnet Virus:
- Americans and Israelis collaborated to stop Iran from producing Uranium that could be used in nuclear weapons
- A computer worm known as Stuxnet was placed on an infected USB stick and used to gain access to the Iranian computer systems
  - Specifically, attacked programmable logic controllers (PLCs) **manufactured by Siemens** which controlled frequency converter drives that, in turn, controlled the speed of the centrifuges
- Destroyed nearly 1,000 uranium enriching centrifuges (~20% of the total)
- **Significantly reduced Iran's nuclear capabilities**

https://www.metacompliance.com/blog/irans-cyber-attack-timeline-2009-2020/

12

Stuxnet as Cyberattack: Directness

- Directness: attacks are immediately, directly responsible for damages
- **Was Stuxnet direct?**
- Yes – the worm targeted the specific centrifuge hardware/software configuration and directly caused centrifuges to fail

Foltz 2012

13

Stuxnet as Cyberattack: Immediacy

- Immediacy: consequences that manifest quickly leave little time for de-escalation or mitigation of effects
- **Was Stuxnet immediate?**
- No – it took a year for the attack to play out, and weeks or months for the centrifuges to fail

Foltz 2012

14

Stuxnet as Cyberattack: Invasiveness

- Invasiveness: attacks impair the territorial integrity or sovereignty of a state; the more secure the system, the more invasive the attack
- **Was Stuxnet invasive?**
- Yes – crossed international borders and targeted highly secure systems
  - Had to be carried in via thumb drive to air-gapped computers
  - However, cyberespionage that collected information from those computers would be equally invasive and not an attack

Foltz 2012

15

Stuxnet as Cyberattack: Measurability

- Measurability: attacks have quantifiable, identifiable consequences
- **Was Stuxnet measurable?**
- Yes – consequences of the attack appear to be directly identifiable
  - Even though those centrifuges were already prone to failing

Foltz 2012

16

Stuxnet as Cyberattack: Presumptive legitimacy

- Presumptive legitimacy: if something is legitimate outside the cyber domain, it remains legitimate (e.g., propaganda, espionage)
- **Was Stuxnet legitimate?**
- No – there is no legal justification for damaging another state's nuclear facilities
  - "Short of UN Security Council authorization or actions taken in self-defense … there is no customary acceptance within the international community for damaging another state's nuclear facilities."
  - However, Iran's centrifuges were operation in violation of UN Security Council Resolutions and in the face of sanctions, which may make it *more* legitimate

Foltz 2012

17

Stuxnet as Cyberattack: Responsibility

- Responsibility: created and propagated by known state actors
- **Does responsibility for Stuxnet lie with the state?**
- Yes – although responsibility has not been officially claimed, it is clear that Stuxnet was created by Israeli and American forces

Foltz 2012

18

Stuxnet as Cyberattack: Severity

- Severity: the more severe the results, the more likely something is to qualify as a "use of force"
- **Was the Stuxnet attack severe?**
- Yes – anything that results in significant physical damage qualifies

Conclusion: Stuxnet was a cyberattack (and one of the first deployed cyberphysical attacks).

Foltz 2012

19

Stuxnet: collateral damage

- Stuxnet is not known to have damaged anything beyond the intended target
- However, it spread far beyond the intended computer spaces
- What if it had affected non-Iranian targets? What if it had affected non-nuclear enrichment targets, such as legitimate scientific labs or water treatment facilities?
- Reprisals: Stuxnet led directly to a series of Iranian counter-attacks and arguably the development of Iran's sophisticated cyberwar infrastructure

20

20

Ethical Analysis: Stuxnet

- **Should Stuxnet have happened?**
- Use the ethical analysis framework (loosely) to discuss:
  - What policy should govern whether an attack like Stuxnet should happen again?
  - Who are the major types of stakeholders?
  - What are the ethical principles and values at stake?
  - What are the tradeoffs and principles in conflict?
  - How do professional codes of ethics come into play?
  - **Would your policy have allowed Stuxnet to go forward?**

21

21