CYBER POLITICS AND POLICIES

CHAPTER 11: CONFLICT

AT THE END OF THIS CHAPTER, STUDENTS WILL BE ABLE TO:

- Describe key terms related to cyber warfare including information warfare, advanced persistent threat, and crisis stability
- 1.Describe unique features of the cyber warfare environment
- 1.Discuss proposed solutions to regulating or decreasing conflict in the cyber environment including weapons bans, and the use of deterrence

PART ONE: DEFINITIONS AND HISTORY OF INFORMATION WARFARE

COMPUTER SECURITY AS NATIONAL SECURITY

- Computer security is part of national security more broadly
- Failing to protect a state's data and critical infrastructure can impact a state's economy, political system and society.
- A state's cybersecurity posture—its strengths and weaknesses, the size of its force and the tools and assets which its commands -- can affect other elements of its overall military.

WHOLE OF NATION APPROACH

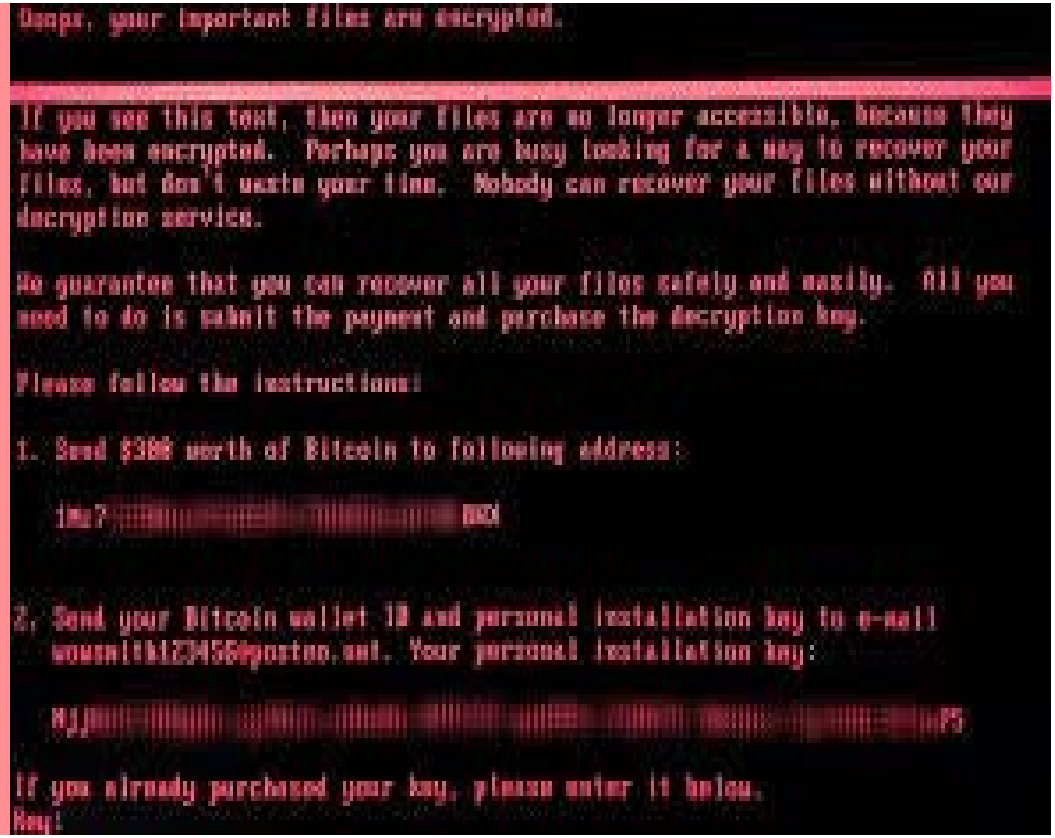
- actions carried out by military assets as well as commercial and business interests – aimed at securing data and information from adversaries
- Contains both offensive and defensive strands

INFORMATION WARFARE IS NOT NEW

- Surprise
- Deception
- Disinformation (Active Measures)
- I**nformation warfare is** 'an extension of ordinary warfare in which combatants use information and attacks on information and information systems as tools of warfare.'

SOME TACTICS ARE NEW

- ‘cyber hostage taking’
- Advanced Persistent Threat
- “Hold targets at risk” in order to extract concessions, including real world concessions
- False flag activities
- **subversion** – undertaken to weaken the west through splitting the Western community (including such organizations as the European Union and NATO



PART TWO: HYBRID WARFARE AND THE CHANGING BATTLEFIELD

HYBRID WAR


Special forces
Irregular forces
Support of local unrest
Information warfare propaganda
Diplomacy
Cyber attacks
Economic warfare
Regular military forces
Hybrid Warfare =
Combination of multiple conventional and unconventional tools of warfare

WHAT IS AMERICA'S TIPPING POINT?

- Russian planners describe how it is possible to find the 'tipping point' where a state could become destabilized and 'tip over' into anarchy.
- What if unemployment rises as the result of widespread adoption of robotic technologies?
- What sort of social media and disinformation campaigns might be sufficient to achieve this 'tipping point'?
- What cracks exist in our societies that an adversary could capitalize on, in order to splinter a state apart?

DEFINING ACTS OF WAR

- Cyberweapons are **dual use technologies**, since they may have different uses and different utility in different situations.
- Challenging for states to create laws and regulations regarding such dual use technologies, since doing so requires establishing and regulating who will have access to this technology, as well as how people will use this technology and under what circumstance

REAL VS. DIGITAL BATTLEFIELD

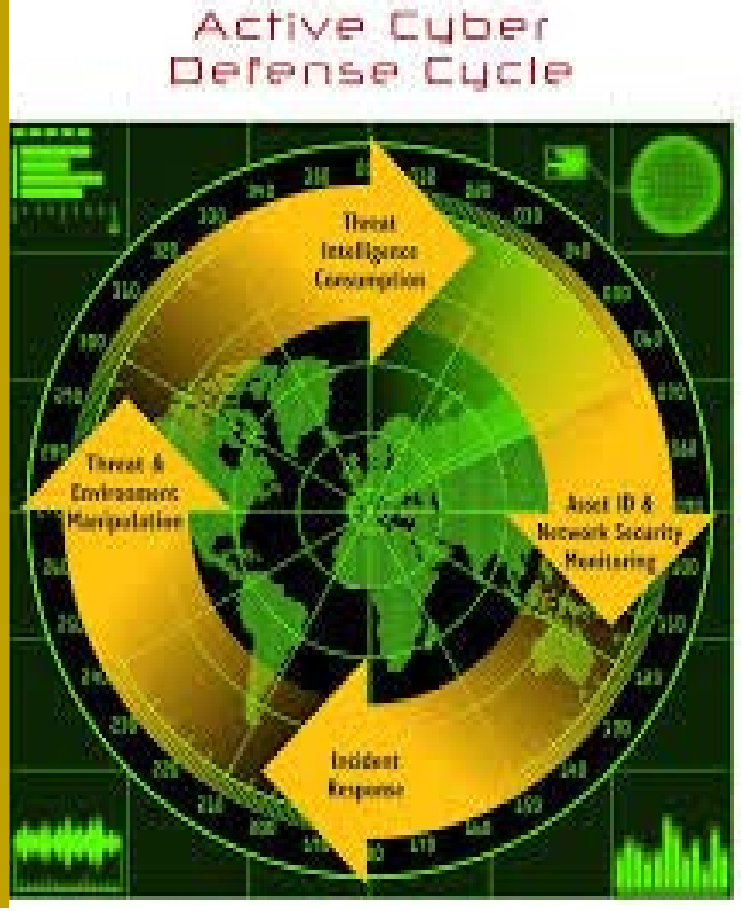
- Harder to determine if an action is preemptive – due to speed at which digital battle occurs
- What does it mean to 'declare war' in cyberspace?
- Borders between civilian and military territory are much less defined
- How to secure civilians from harm in digital battles?

DEFENDING CYBERSPACE: PASSIVE DEFENSE

- passive defense: "software or hardware added to the architecture that increased security without consistent and direct interaction from personnel, even if updates and tuning are required over time (i.e. firewalls, anti-malware software, intrusion detection and prevention systems, and application whitelisting)." legal and ethical
- Cyber hygiene

DEFENDING CYBERSPACE: ACTIVE DEFENSE

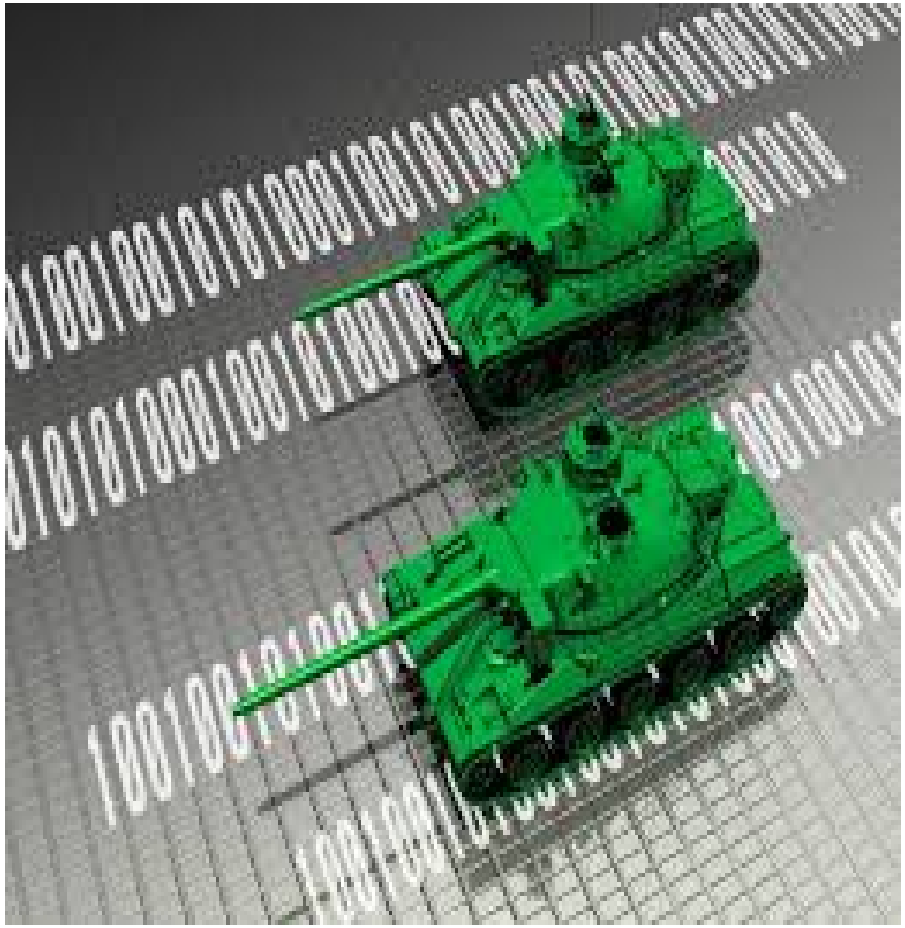
- Situations in which security personnel take an active, often preemptive role, in countering threats to their system, seeking to neutralize threats before they can impact an organization's operations.
- Includes carrying out intelligence activities to understand who might be targeting your system, and what their objectives are.
- Personnel engaged in active cyber defense will often act to turn an attack around, sending elements of the attack back to the site from which it originated.
- Such actions are referred to as 'hack backs



OFFENSIVE OPERATIONS

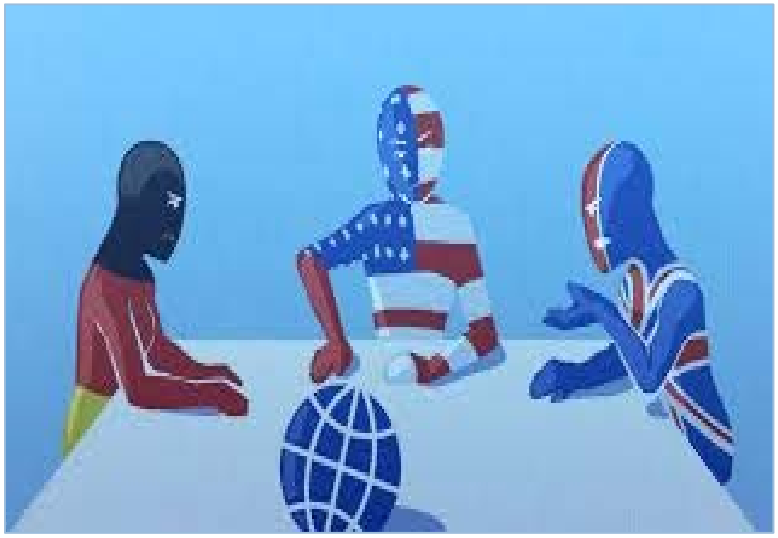
- aimed at defacing or altering the equipment or terrain belonging to one's adversaries in cyberspace.
- include acts like web defacement; Distributed Denial of Service attacks (including botnet attacks), or the uploading of malware including zero-day exploits to an adversary's system.

CREATING RULES TO GOVERN CYBERWARFARE



CREATING INTERNATIONAL RULES GOVERNING CYBERWARFARE

- Difficult for a state to understand exactly why an adversary has entered your system and what its purposes are for being there.
- As a technology matures over time, new methods of defending that technology (or making it resilient) may emerge.
- "Defending" the telegraph from intruders back in the 1800s eventually led to the development of new technologies like encryption



WHAT IS LEGAL AND ILLEGAL?

- Analysts don't agree regarding the legality and ethical acceptability of active cyber defense – or indeed whether it is properly understood as defense.
- Concerns about whether 'hacking back' creates a merely proportional response to an attack by an adversary, or whether a hack back might inflict a disproportionate response on one's opponent.

IS CYBERWARFARE REALLY WAR?

- **"computer network exploitation"** – enabling operations and intelligence collective capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."

Thomas Rid

- code alone cannot kill anyone
- we should abandon any attempt to formulate "rules for cyberwar," or "doctrines of cyberwar."
- cyber operations should be understood merely as a force multiplier for conventional conflicts.

DOES INTERNATIONAL LAW APPLY IN CYBERSPACE?

- Tallinn Manual on the International Law Applicable to Cyber Warfare
- a cyber-attack whose consequences amounted to an armed attack could trigger the right of self-defense under UN Charter Article 51
- international law governing armed conflict (such as the requirement that armed forces distinguish between military and civilian targets) also applied to cyberspace.

2011 United States International Strategy for Operating in Cyberspace:

- "The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior – in times of peace and conflict – also apply in cyberspace."

IS CYBERSPACE "FOR FIGHTING"?

- Hollis and Ohlin:
- creating a strong international consensus about the application of LOAC means that cyberspace is now understood primarily as an arena of conflict, rather than cooperation
- If anyone has a key role to play in governing or regulating cyberspace, then, it is likely to be military actors acting on behalf of legitimate states.
- The Tallinn Manual supports the creation of a Cyber Westphalia model of internet governance over and above the creation of other models, such as multi-stakeholder governance.

PART THREE: RELATION OF CYBERWAR TO CONVENTIONAL CONFLICT

THE UTILITY OF CYBERWEAPONS IN CONVENTIONAL CONFLICTS

- Deterrence
- Nuclear weapons were an effective deterrent in many situations, even though they were never deployed
- Creation of "strategic stability"

WOULD A STATE, AWARE OF THE DANGER OF CYBERWAR, ENGAGE IN THE SAME TYPE OF RESTRAINT WHICH STATES ENGAGED IN IN REGARD TO NUCLEAR WEAPONS?

Axelrod and Iliev

- **Cyberweapons decay quickly.** There is little utility in stockpiling them or waiting to use them.

- RESOLVE: The US may possess a significant cyberweapons arsenal. However, are we committed to engaging in "massive retaliation" against adversaries? (i.e. Crippling their electrical grid for many years, resulting in mass starvation, people freezing to death, etc.)
- Because CODE isn't tangible, hard to frighten your adversaries by SIGNALING your strength (i.e. Not like counting nuclear missile silos)

CONTAINING CONFLICT IN CYBERSPACE

- Cyber arms control treaties
- Confidence building measures
- Banning cyber weapons?

FOR DISCUSSION

- How optimistic or pessimistic are you that a cyber arms control agreement would actually work? Do you regard yourself as a Realist, a Liberal Internationalist or a Constructivist? Give reasons for your answers.

- Think about the political polarization which is currently occurring in the United States and the reasons for it. How might an outside adversary take advantage of such a situation to destabilize the state? Do you consider this a legitimate worry? Why or why not?