Summary of the second half of Clarke and Knake, “Cyber War”

Each chapter has a discussion group summary, and an instructor’s summary

Chapter 5: defensive strategy

discussion group summary

- On page 174, there are five specific ideas, they seem feasible and a good idea for helping with cyber security:
  - The smart regulation that is raised in the chapter, while also a good idea, could be hard to do since people work around regulations.
  - On page 152, the lack of any real known cyber-war strategy seems impractical.
  - The twenty questions of cyber-war: seem very repetitive and obvious. Seems to be repetitive to stress a point.
  - The defensive triad:
  - tier 1 backbone - Put up a firewall to protect data - disconnect power grids from the internet -DoD

Chapter 5: defensive strategy

instructor’s summary

- Recommend “Defensive Triad”:
  - Harden Internet backbone
  - Secure power grid
  - Upgrade DoD defenses
- Recommend doctrine of:
  - Cyber equivalency
  - National cyberspace accountability
  - Obligation to assist

Chapter 6: offensive strategy

discussion group summary

- Reviewing of the scenario:
- 1) The failure of deterrence: Deterrence theory is probably the least transferable to the cyber world (compares to nuclear deter.) The power of the offensive is largely secret. No real treaties that involve cyber warfare.
- 2) Striking first: US takes the first move in this scenario. Points out that not going first may later affect your ability to conduct a cyber attack.
- 3) Preparation of the Battlefield: Logic bombs
- 4) Global War: No way you can contain within the two countries alone. Hitting US power grids also affects Canada and Mexico.
- 5) Collateral Damage: Where do we draw the line of what we can hit in the infrastructure? Cyber attacks can affect ATC systems and power supply to civilians (hospitals).
- 6) Escalation: Goes along with idea of striking first. Where do you strike, and what should the impact be?
- 7) Positive control: President should have leading authority
- 8)Attribution: Many attacks cannot be traced, therefore although tensions between two major powers are rising, it should not be assumed that an attack that cannot be traced is from that specific country.
- 9) Crisis Instability: “If you don’t make the right decision quickly, you lose, but if you have to make the decision quickly, you may make a losing decision”
- 10 Defensive Asymmetry: The best defense is a good offense, which attributed to China coming out on top in this scenario.

- Reviewing of the scenario:
- 1) The failure of deterrence: Deterrence theory is probably the least transferable to the cyber world (compares to nuclear deter.) The power of the offensive is largely secret. No real treaties that involve cyber warfare.
- 2) Striking first: US takes the first move in this scenario. Points out that not going first may later affect your ability to conduct a cyber attack.
- 3) Preparation of the Battlefield: Logic bombs
- 4) Global War: No way you can contain within the two countries alone. Hitting US power grids also affects Canada and Mexico.
- 5) Collateral Damage: Where do we draw the line of what we can hit in the infrastructure? Cyber attacks can affect ATC systems and power supply to civilians (hospitals).
- 6) Escalation: Goes along with idea of striking first. Where do you strike, and what should the impact be?
- 7) Positive control: President should have leading authority
- 8)Attribution: Many attacks cannot be traced, therefore although tensions between two major powers are rising, it should not be assumed that an attack that cannot be traced is from that specific country.
- 9) Crisis Instability: “If you don’t make the right decision quickly, you lose, but if you have to make the decision quickly, you may make a losing decision”
- 10 Defensive Asymmetry: The best defense is a good offense, which attributed to China coming out on top in this scenario.

Chapter 6: offensive strategy

instructor's summary

- Deterrence "plays no significant role in stopping cyber war today" (p195)
- No-first-use makes sense only in pre-kinetic phase of conflict
- Everyone is "preparing the battlefield"
- Withholding certain types of targets makes sense (e.g. finance, opponent's command and control)
- Cyber weapons probably need "positive control"
  - Multiple people to activate, including a higher-level command
- Attribution is problematic; may require "traditional intelligence techniques"
- First mover advantage contributes to instability

Chapter 7: international cyber treaties

discussion group summary

- Chapter was essentially about regulation of cyber warfare. What treaties, if any, should be introduced to increase global stability with regards to cyber activity?
- US in awkward position with regulation, as the US has the most to lose in a cyber-attack (as the US has a very net-centric infrastructure) but also has a lot to lose in an outright ban (as the US has a powerful arsenal of cyberweapons that could save American lives in a conflict.)
- Lots of options on the table in the discussions on cyber regulation. Different levels of regulation include limits on targets and types of permitted attacks, and some might be more beneficial to the US than an outright ban.
- US has a pivotal choice to make here. Can either go and push for heavier regulation and look like a more peaceful nation at the cost of giving up some of its cyber attack advantage, or look more warlike and keep its advantages. Either way, the US will face international judgement.

Chapter 7: international cyber treaties

instructor’s summary

- “Five broad conclusions” (p254):
  - Cyber arms control can prohibit acts but not capability
  - Banning cyber espionage is not in US interest
  - An international agreement prohibiting “attacks on civilian infrastructure” are in US interest
  - Verification is problematic but can be enabled by a new international agency and/or “obligation to assist” agreements
  - US and others should remove logic bombs from adversaries’ civilian infrastructure

Chapter 8: recommended US strategy

discussion group summary

- What Clarke thought the Government should do in terms of defense à research and understanding of Cyber Warfare:
  - Get the Government more involved.
  - Talked about having more involvement in international discussion, something like the Strategic Arms Limitation Treaty to limit cyber war.
  - Realize the US isn’t in control of the internet anymore
  - Wants to limit cyber war but not intelligence gathering. The Gov should work to reduce civilian cyber crime (anonymous, identity theft) FBI and SS should focus,
  - President should personally improve logic bombs and trap-doors, he has to take control of covert action in terms of any cyber.
  - President should be the one who gives the go ahead for cyber war
  - Redesign the internet à security à encryption, governance
  - Needs to be more public dialogue, seems to be a hidden issue that were ignoring. Regulation

Chapter 8: recommended US strategy

instructor’s summary

- More public and congressional discussion of the issues
- Defensive Triad (harden Internet backbone, electric grid, and DoD networks)
- Fight cyber crime with dedicated federal agency
- Pass a cyber war limitation treaty
  - bans first use against civilian targets and attacks on financial institutions
  - Establishes national cyber accountability and obligation to assist
- Create new “intranets” for critical infrastructure and other components
- Annual presidential review of battlefield preparations and readiness

Appendix: Stuxnet

discussion group summary

- Stuxnet worm against Iran, legitimized cyber war, everyone realized it’s a tool of attack. Worm designed to disable nuclear equipment

Appendix: Stuxnet

instructor’s summary

- Stuxnet is a confirmed example of a cyber weapon causing physical harm to an adversary’s equipment
- Delayed Iran by “months”
- Released a weapon that could be retargeted and used by others