National Security Cyber Strategy

Erik Gartzke
UCSD
Center for Peace and Security Studies (cPASS)

Cybersecurity of Critical Infrastructure Summit
Texas A &M University
12 January 2017

CROSS-DOMAIN DETERRENCE

MINERVA INITIATIVE DEPARTMENT OF DEFENSE

DEPARTMENT OF THE NAVY ONR Science & Technology

UC San Diego

UNIVERSITY OF TORONTO

Berkeley UNIVERSITY OF CALIFORNIA

UNIVERSITY OF MARYLAND 1856

Lawrence Livermore National Laboratory

Los Alamos NATIONAL LABORATORY

The research presented here was supported in part by: “Deterring Complex Threats: The Effects of Asymmetry, Interdependence, and Multi-polarity on International Strategy”
#N00014-14-1-0071 (6.1, DoD Minerva)

Erik Gartzke

Jon Lindsay

Michael Nacht

When it comes to cyberspace, some people think the sky is falling...

Cyber Strategy–National Security

Concerns about cyber insecurity have led to a small but growing literature that has begun to apply and extend classic insights from security and strategy to cyberspace

- Means are only part of equation . . . what are the ends?
  - No defense against nuclear attack (deterrence "success")
  - Anyone can attack you at any time. Why don't they?
- Use narrow lens of work by myself and collaborators.

Cyber Pearl Harbor

Question: Is cyber a "game changer"?
(Short answer: No. Evolutionary, not revolutionary)

* "The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth." 2013. *International Security*, 38(2):41–73.
* Lindsay, Jon. 2013. ?Stuxnet and the Limits of Cyber Warfare.? Security Studies 22(3):365-404.

Cyber complements other modes of conflict (not a substitute)

- Coercion: Must <u>tell</u> target to coerce. Problem: credibility compromises exploits (contrasting attribution problem).
- Conquest: Must produce lasting harm to weaken opponent
  - What happens the day *after* a zero day?
  - Exploit not useful unless it can be exploited
  - More useful to powerful than weak
  - Pivotal for information (espionage), not destruction

Deception

Question: Should one deter or defend in cyberspace?
(Short answer: Each flawed. Both improved by deception)

* "Weaving Tangled Webs: Offense, Defense & Deception in Cyber space." With Jon Lindsay. 2015. *Security Studies*, 24(2):316-348.
* "Windows on Submarines: The Dynamics of Deception in the Cyber and Maritime Domains," With Jon R. Lindsay in *Maritime Cyber Security: Threats, Vulnerabilities, and Consequences*, ed. Nicole Drumhiller and Fred Roberts. Forthcoming.

Deception for cyber ⟺ deterrence for nuclear
Summary:

- Attack attacker's gains from cyber aggression
  - Real trojan horse – adversary brings malware home
  - Defense/deterrence improved, become screening device

Cyber Coercion

Question: How does cyber aggression work?
(Short answer: Cyber "reshapes" conflict behavior)

* "Coercion through Cyberspace: The Stability-Instability Paradox Revisited." With Jon R. Lindsay, in *The Power to Hurt: Coercion in Theory and Practice*, ed. Kelly Greenhill and Peter J. P. Krause. New York: Oxford University Press, Forthcoming.
* "Mining Cyberspace." Jon Lindsay & Martin Libicki. In process.

Cyber affected by "stability-instability paradox" (Snyder).
Summary:

- If cyber is offense-dominant → it should be unstable.
  - Pardox: lots of low-level conflict, few high level conflicts
  - "Big" attacks are difficult to execute/not that fruitful

Cross-Domain

Question: How does cyber function across domains?
(Short answer: It depends. Sometimes really scary)

* "Thermonuclear Cyberwar." With Jon R. Lindsay. 2015. *Journal of Cybersecurity*. Forthcoming.
* "Cross-Domain Deterrence and Cybersecurity: The Consequences of Complexity," in *National Security and Cybersecurity*, ed. Damien van Puyvelde. New York: Routledge. Forthcoming.

Summary:

- Cyber instability can stabilize or destabilize other domains.
  - Nuclear transparency undermined by cyber conflict
  - Can lose deterrent and not know (enemy cannot reveal)
  - Cyber can stabilize in other domains (lose initiative)

Attribution

Question: Isn't attribution a problem?

(Short answer: Yes and no)

Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyber Attack," Journal of Cybersecurity 1, no. 1 (2015): 53?67

Summary:

- The attribution problem is a variable, not a constant.
  - Large for small/cursory attacks (many, low impact)
  - Smaller for few intense attacks (tied to consequences)
  - Attackers face attribution problem for coercive attacks

Space

Question: Can we achieve deterrence from space?
(Short answer: Yes, Reconnaissance Satellites)

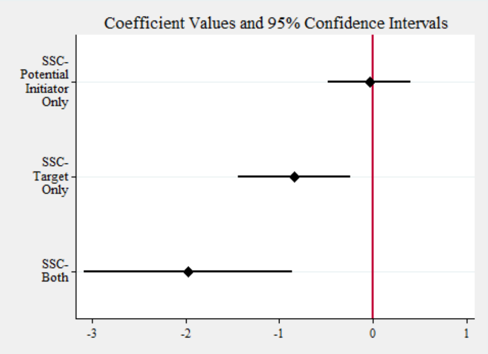
"Offense, Defense and Reconnaissance: Technological Espionage and Interstate Disputes." With Bryan Early. In process.

"..photo-reconnaissance satellites, for example, are enormously important in stabilizing world affairs and thereby make a significant contribution to the security of all nations." – President Jimmy Carter (1981, p. 146)

Summary:

- Reconnaissance satellites give early warning of attack
  - Minimize surprise, reducing impetus for some conflicts
  - Do not increase incentive for initiator to attack

Figure 1: Comparing the Effects of the Surveillance Satellite Variables



Notes: This figure was created using the results from Model 3.

Military Automation

Question: What are the effects of military automation, such as UAVs? (Short answer: More war)

"No Humans Were Harmed in the Making of This War" In process.
"Drones and their Drawbacks: The Effects of RPVs on Escalation and Instability in Pakistan." With James Walsh. Under review.

Summary:

- Primary effect of military automation is to reduce war cost
  - No "skin" in the game, literally.
  - Deployed where "boots on the ground" too costly/risky
- Also displaces conflict away from the battlefield (terrorism)
- General tendency to relax laws of war –> target civilians

Conclusions

Implications:

- Deterrence in cyberspace will not occur in cyberspace
  - Offense dominant domain (like nuclear)
  - Think cross-domain and strategically about cyber
- In national security, cyber is mostly evolutionary
  - Threat is greatest to the meekest, not to strongest
  - Implications of cyber tied to exploitation of exploits
- Unpacking attributes is valuable (force multiplier)
  - Part of third offset may be better strategic thinking