Notes on *Deterrence of Cyber Attacks* by Richard Kugler

John MacCormick, Spring 2013

Introduction

- Claims we can meaningfully discuss deterrence of cyber attacks despite the well-known difficulty of attributing cyber attacks
- Summarizes main arguments:
  - Many cyber attacks will have objectives "beyond the cyber domain," so we can consider "multifaceted" deterrence
  - Recommends "tailored" cyber deterrence with specific strategies for different adversaries and attack types

Cyber deterrence strategy in official US documents

- Public official documents (up to 2006, which is where this analysis ends) provide essentially no details on the US strategy for cyber deterrence
- Note the discussion of 2006 QDR (p312), which led directly to the publication of the collection in which this article appears

Growing vulnerability to cyber attacks in a globalizing world

- Emerging cyber threats include large powers (e.g. China, Russia) and many smaller ones due to the "southern arc of instability" (e.g. Middle East) and economic "empowerment" (e.g. Iran, Venezuela)
- Attribution isn't a prerequisite for a deterrence strategy, because US need only deter *potential* adversaries (para 2, p318)
- In any case, US should certainly have a deterrence strategy for responding to an attack whose source *is* known

Contributions from deterrence theory: past and present

- "the issue of cyber deterrence strategy cannot be separated from the rest of US national security policy" (p321)
- Cold War deterrence strategy evolved significantly, becoming a balance between "warning the adversary" and "unwarranted escalation."
- Today, the US faces many types of threats, requiring "tailored deterrence"

Toward a general model of tailored cyber deterrence

- Deterrent responses to cyber attacks need not be cyber; could be, e.g. kinetic, political, economic
- "Diverse responses may be needed in order to have different types of effects"

This section seems short on specifics. It appears to repeatedly state the obvious point that different situations will require different responses. Is there a more subtle point here?

Strategic requirements for cyber deterrence: assets and capabilities

- Lists seven requirements for US, including:
  - "A clear and firm declaratory policy spelling out the US intention to deter cyber attacks"
  - "Effective cyber defenses," protecting military and non-military targets, especially infrastructure
  - "A wide spectrum of counter-cyber offensive capabilities"

Anything surprising here? In many ways, these are obvious goals, but it's important to understand why they are relevant to deterrence.

Issues for further analysis

- The "declaratory policy" for cyber deterrence must address different "focused" messages to different audiences
- The attribution problem must be addressed to the greatest extent possible

Conclusion: toward a spectrum of cyber deterrence options

- Describes a spectrum of three cyber deterrence strategies:
  - "limited": mainly defensive
  - "more ambitious": relies on defense and offense, and requires "rapid improvements in … offensive capabilities"
  - "highly ambitious": include extensive collaboration and planning with allies
- Warns that "the United States cannot afford to risk drift in this arena"