Escalation Management in Cyber Conflict: A Research Proposal

Robert Reardon, ECIR Postdoctoral Associate, Political Science, MIT

Explorations in Cyber International Relations
Massachusetts Institute of Technology Harvard University

Workshop on
People, Power, and CyberPolitics
MIT, December 7 and 8, 2011

Research Questions

- *Under what conditions is cyber conflict most likely to lead to uncontrolled escalation?*
- *Under what conditions is cyber conflict likely to lead to escalation in other domains (conventional, nuclear)?*
- *What steps are most affective at the reducing the risks of escalation?*
- *How relevant are existing theories of deterrence and escalation management to cyber conflict?*

Relevant Attributes of Cyber

- Constant background of attacks
- Diversity of actors (state and non-state)
- Diverse motives for attacks
- Difficult to identify attacker
- Difficult to identify the source, purpose of attack.

ATTACKERS

- *State*
- *Non-State Proxy*
- *Autonomous Non-State Actor*
- *Domestic*

ROLE OF STATE

- *Attack Conducted by State*
- *State Directs Proxy Attack*
- *State Encourages Private Attackers*
- *State Proxy Attacks Without State Direction*
- *Private Attackers Not Directed by State*

MOTIVES

- *Preparation for Kinetic Attack*
- *Hacktivism*
- *Terrorism*
- *Cybercrime*
- *Espionage*

Implications

- Avoid framing cyber defense in military terms, and avoid defining threshold for cyber "act of war."
- Declaratory policies should remain ambiguous (could perversely encourage other parties, create credibility trap)
- Efforts to deter through retaliation are likely to be self-defeating.
- Important role for international coordination and foreign capacity building.
- Strengthen lines of communication and promote international dialogue.
- Deterrence by denial has limited utility, and can risk unacceptable or self-defeating costs.

Analytic Framework

- Most Analyses Have Looked to Theories Developed for Cold-War Nuclear Deterrence as Model to Understand Escalation in Cyber

- A Number of Characteristics of Cyber Conflict Suggest Irregular Warfare May be a Better Framework for Analysis:

  - *Combatants are extremely difficult to deter*
  - *Many have no interest in managing conflict intensity.*
  - *Asymmetries of information, interest, and capabilities are present.*
  - *Escalation management is set in a context of overlapping and simultaneous conflicts.*

Escalation Management in Different Forms of Conflict

	Nuclear (Cold War)	Irregular Warfare	Cyber
Paths to Escalation	Few	Many, Diverse, Multiple Conflicts Exist Simultaneously	Many, Diverse, Multiple Conflicts Exist Simultaneously
Relevant Actors	Small Number of States, Global Interests	Many, Diverse, Often with Regional or Local Interests	Many, Diverse, Often with Regional or Local Interests
Knowledge of Other Actors' Intentions and Capabilities	High, Signals Relatively Easy to Send, Receive, and Interpret	Low, Signal-to-Noise Problem	Low, Signal-to-Noise Problem
Ability to Accurately Attribute Attacks	High	Low	Low
Risk of Deliberate Escalation	Low	High	Unknown
Risk of Proxy Attacks	Low	High	High
Frequency of Attacks	None	High	Constant
Damage from Attack	Extremely High, Symmetric Vulnerability	Variable, Asymmetric Vulnerability	Extremely Variable, Typically Low, Asymmetric Vulnerability

Research Plan

- Explore existing literature on deterrence and escalation management in irregular warfare.
- Identify key areas of similarity /difference between cyber and other forms of irregular warfare.
- Develop comparative case-study analysis, drawing from four different types of conflict: irregular warfare, nuclear, conventional, and cyber.

Author and Affiliation

Robert Reardon is a postdoctoral associate with the ECIR project at MIT. He received his PhD in political science from MIT in 2010, and spent the 2010-2011 academic year as a Stanton Nuclear Security Fellow at RAND, where he continues to work as an adjunct political scientist.

This work is funded by the Office of Naval Research under award number N00014-09-1-0597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author alone and do not necessarily reflect the views of the Office of Naval Research or any other organization.