

Cyber and Crisis Escalation: Insights from Wargaming

*Jacquelyn G. Schneider
Naval War College*

*The views represented here are the author's alone, and do not
reflect those of the Naval War College or US Navy.*



U.S. NAVAL WAR COLLEGE
— Est. 1884 —
NEWPORT, RHODE ISLAND



Does Cyber Increase the Chance of Inadvertent Conflict?

- **No: academics**
 - Complexity and interdependence= caution
 - Civilian vulnerabilities lead to risk adverse cyber operations
- **Yes: U.S. policymakers**
 - Uncertainty, speed of capabilities, perceptions of offense dominance
 - De-stabilizing incentive for cyber first strikes

Little consensus in academia and policy community about the effects of cyber operations on crisis stability



Wargaming as a Method to Understand Cyber and Conflict

- **Lack of empirics to test conflicting hypotheses about cyber and escalation**
 - **Therefore, perceptions more important than actual capabilities**
 - **Wargaming as a method to understand perceptions and motivations**
 - Limited ability to reveal adversary patterns
 - But can illuminate patterns of behaviors for U.S. decision-makers
-



Deterrence and Escalation Game and Review: 2011-2016

- **Strategic Command-sponsored war game conducted at Naval War College**
 - Focus on crisis decision-making

 - **Benefits:**
 - Data drawn from six years (longitudinal analysis)
 - More realistic sample than academic research
 - Cyber as a tool within conventional scenario

 - **Limitations:**
 - Not experimental: different scenarios, players, etc.
 - Little ability to divine adversary intentions/behaviors
-



Hypotheses: Cyber and Stability

- ***Blue Perceptions:***

- *Hypothesis 1: Blue perceives blue cyber operations will lead to crisis escalation.*
 - *Hypothesis 2: Blue perceives blue cyber operations lead to crisis de-escalation.*
 - *Hypothesis 3: Blue perceives cyber operations have no effect on crisis escalation.*
-



Hypotheses: Cyber and Stability

- ***Blue Actions in Response to Red Cyber Operation:***
 - *Hypothesis 4: Blue takes cyber action*
 - *Hypothesis 5: Blue takes conventional kinetic*
 - *Hypothesis 6: Blue takes nuclear action*
 - *Hypothesis 7: Blue takes diplomatic/economic action*
 - *Hypothesis 8: Blue takes no action*
-



Hypotheses: Motivations for Blue Cyber Operations

- ***Hypothesis 9: Organizational influences***
 - ***Hypothesis 10: Capability development***
 - ***Hypothesis 11: Situational context***
 - ***Hypothesis 12: Individual decision-maker personality***
 - ***Hypothesis 13: Cognitive variables***
-

Summary of Wargames and Cyber Activity

	Context	Blue Lead	Blue Highest Level Cyber	Blue Actions Before Cyber Attack	Red Highest Level Cyber	Actions in Response to Red Cyber
2011	Land war, Near-peer Adversary	Female, State Dept	Cyber attack against conventional military operations	Conventional military force and nuclear alert	Cyber attacks on conventional military targets	None
2012	Naval war, Near-peer Adversary	Male, Former Military	Cyber attacks against strategic command and control	None	No red cyber attacks	NA
2013	Naval war, Near-peer Adversary	Male, State Dept	Reversible virtual cyber attack on military capability	Conventional military force	Cyber attacks on military C2 nodes and critical infrastructure	None
2014	Land war, Asymmetric Adversary	Male, Policy	Cyber attack against offensive cyber capabilities	Conventional military force and nuclear alert	Cyber attacks on allied nuclear facilities	None
2015	Land war, Near-peer Adversary	Female, Policy	Information Operations	Conventional military force and nuclear alert	Cyber attacks on allied economic system, conventional military targets	None
2016	Land war, Near-peer Adversary	Male, Policy	Cyber attack on dual-use target that is reversible and covert	Conventional military force and economic sanctions	Cyber attacks on mainland blue power	Economic sanctions

Cyber Escalation ladders

2011	2012	2013	2014	2015	2016
Computer network defense	Computer network attacks against military C2	Computer network defense	Computer network defense	Computer network defense	Computer network defense
Conventional conflict	Conventional conflict and nuclear alert	Conventional conflict and nuclear alert	Conventional Conflict	Conventional Conflict	Cyber network exploitation for future attack
Cyber attacks against military + dual-use targets	Computer network attacks against economic targets	Cyber-led information operations	Nuclear alert	Cyber-led information operations	Conventional conflict and nuclear alert
Cyber-led information operations	Nuclear and cyber attacks against strategic command and control	Cyber attack, reversible on military target	Cyber attack against adversary cyber offensive capabilities		Cyber attack on military target, reversible and covert
Nuclear conflict	Cyber-led information operations				Cyber attack on dual-use target and Cyber-led information operations



Wargaming Perceptions

-
- **Cyber ops escalate crises, even to nuclear war**
 - Reluctance to use cyber attacks, cyber network exploitation, and often cyber-led information operations.
 - Tight rules of engagement for cyber attacks: including non-attribution and reversibility

 - **Cyber-intel ops both escalatory and attributable**
 - But . . . reluctant to attribute adversary ops

 - **Ability to signal in cyberspace**
 - Signaling belief limited cyber ops, but was never perceived as a signal by adversaries
-



Wargaming Actions

-
- **Unwillingness to take cyber offensive operations, to include information-operations**
 - Extreme reluctance to take actions against nuclear C2
 - Focus on mitigating effect on civilians

 - **Cyber offensive operations most likely in conjunction with conventional strikes**
 - Reversible and covert

 - **Teams more wiling to place nuclear forces on alert than use cyber offensive operations**
-



Why Cyber Risk-Adverse?

- **Perception that U.S. is more vulnerable to cyber attacks than its adversaries**
 - **Concerns about the relationship between cyber and nuclear capabilities**
 - **Concerns about the domestic implications of cyber attacks on adversary populations**
-



Motivations for Cyber Behaviors

- **Little evidence for organizational influences, capability development, and situational context**
 - **Significant role of Presidential personality on cyber behaviors**
 - **Cognitive explanation?**
 - Does cyber create anxiety instead of fear?
 - Can that explain why we are reluctant to take cyber offensive operations *and* to respond to cyber operations?
-



Implications for DoD

- **Are we needlessly concerned about cyber operations leading to escalation?**
 - Concerns about escalation are significantly impacting the effectiveness of offensive cyber operations
 - **Are cyber ops so fundamentally different that they become appropriate grey zone tools?**
 - **Can cyber be both non-escalatory and a tool for deterrence?**
 - Tension between cyber as a strategic tool and cyber as a tool of coercion short of conflict
-



Educating Leaders since 1884

www.usnwc.edu

Also search for us on Twitter and Facebook