Cyber and Cross-Domain Deterrence

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

Cyberspace Deterrence: Two Sides

1. Cross-domain deterrence of cyberspace operations

2. Cyberspace operations as a tool of cross-domain deterrence

- ***What are the unique challenges for cross-domain deterrence within and from cyberspace?***

Can we use traditional models of deterrence?

- **No: technologists**
  - Attribution uniquely difficult
  - Covert nature of cyber and signaling
  - Uncertainty about effects
  - Interdependency of civilian and military
  - Proliferation of actors

- **Yes: policy/political science**
  - Emphasize human behaviors
  - Attribution is not unsolvable or unique to cyberspace
  - Limited amount of significant actors

Deterring Cyberspace Operations: Who to Deter?

- **The attribution problem**
  - Cynics: Problem with ability to attribute, timeliness
  - Optimists: Attribution is what states make of it (Rid and Buchanan 2015), analogies in other realms
    - Importance of context

- **Proliferation of actors**
  - Cynics: lowered barrier to access, decreased physical risk
  - Optimists: thresholds for significant activity limit actors

Deterring Cyberspace Operations: What to Deter?

- **Computer network exploitation**
  - Vast majority of cyberspace operations
  - Prolific and of varying levels of sophistication
  - Can states deter CNE?
  - The case for targeted deterrence of CNE

- **Cyber "attack"**
  - Low-level vs. significant
  - Virtual vs. physical
  - Is the importance the target or the scale?

Deterring Cyberspace Operations: Deterrence by Denial

- **Pros**
  - Augments both tailored and general deterrence
  - Does not require high thresholds for attribution
  - Useful for wide variety of threats and actors
  - Does not require political will
- **Cons**
  - Technical capability (offense-dominance?)
- **Cross-Domain Deterrence by Denial:**
  - Defending physical components of cyberspace
  - Sub patrols, space defenses, hardening of C2 facilities

Deterring Cyberspace Operations: Deterrence by Punishment

- **Pros**
  - Large inventory of punishment options
  - More discernible signal, therefore potentially more credible and more effective
- **Cons**
  - Proportionality
  - Escalation Concerns
- **Cross-Domain Deterrence by Punishment:**
  - Sanctions
  - Kinetic strikes

Policy Application for Deterrence within Cyberspace Challenges

- **Technologist-based deterrence**
  - Strategically ambiguous
  - Focused on defense and resiliency
  - Invest in attribution instead of punishment

- **Policy/political science based deterrence**
  - Declaratory
  - Thresholds for action
  - Mix of deterrence by denial (investments in resiliency and defense) and cross-domain deterrence by punishment

Cross-Domain Deterrence from Cyberspace: Signaling and Secrecy

- **Cyber Skeptics:**
  - Perceptibility
  - Saliency
  - Uncertainty about effects
  - Inability to tie domestic promises with cyber punishment

- **Cyber Optimists:**
  - Analogies with covert operations and deterrence
    - Credible signals to tailored audiences
  - Potential for overt uses of cyber in the future

Cross-Domain Deterrence from Cyberspace: Escalation Control

- **Cyber Skeptics:**
  - – Uncertainty about collateral damage
  - – Uncertainty about adversary perceptions
  - – Vulnerabilities in critical infrastructure and linkages to conventional power may lead to inadvertent escalation
    - Ex. Nuclear C3

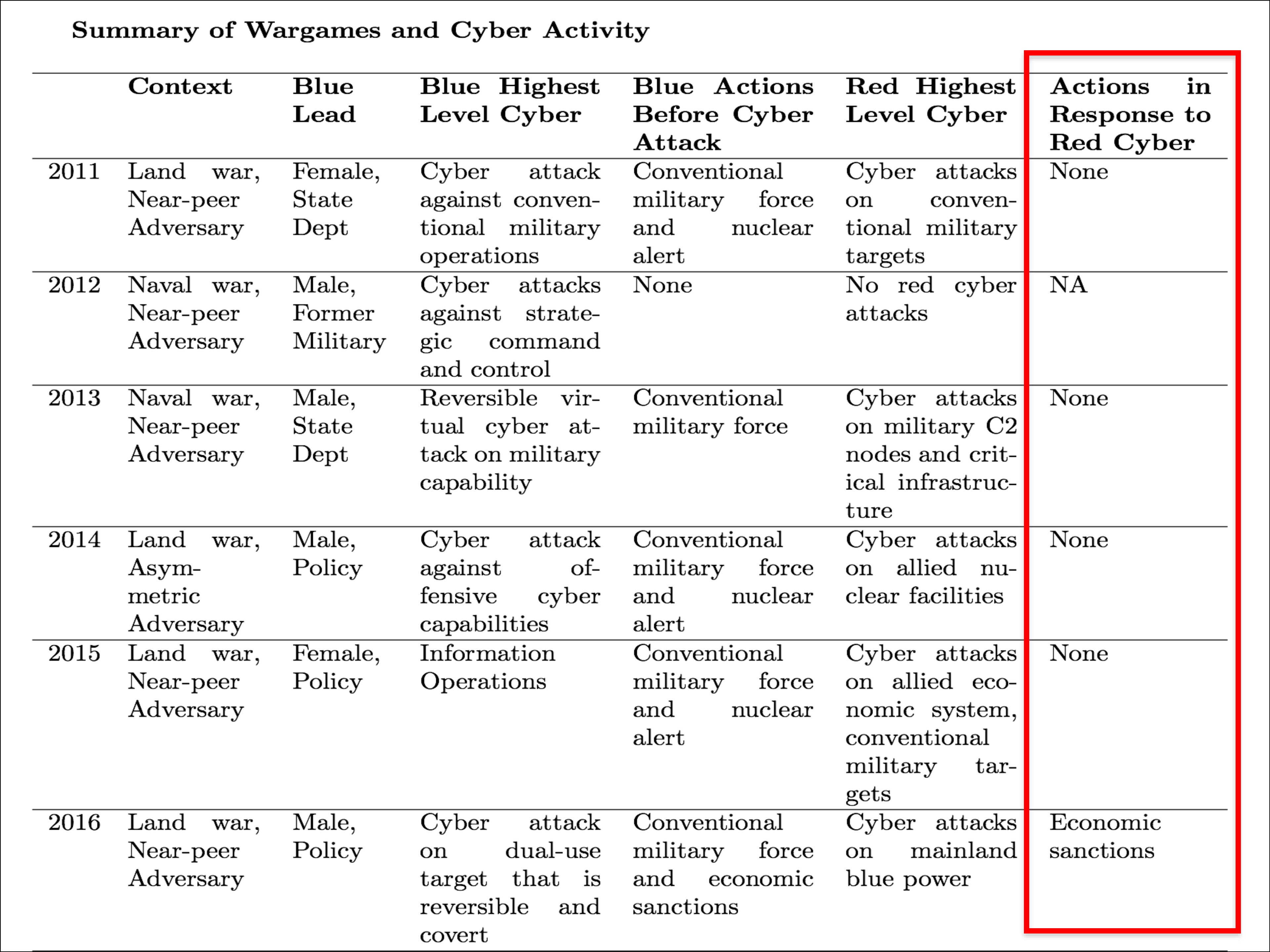
- **Cyber Optimists:**
  - – Flexible options to limit escalation
  - – Provide means to respond credibly to threats short of kinetic response

Cross-Domain Deterrence and Cyberspace: Evidence

- **On Escalation**
  - Unclassified quantitative evidence shows no signs of escalation in response to cyber operations
    - Valeriano, Jensen, and Maness (2018)
    - Kostyuk and Zhukov (2017)
  - War gaming and survey experiments on American populations also show no signs of escalation
- **On Signaling**
- **On Deterring Cyber Actions**

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



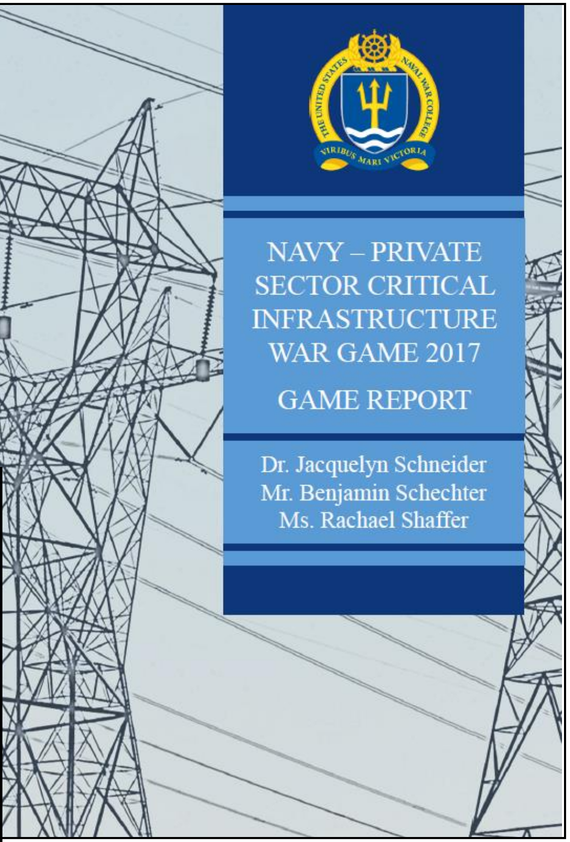
Summary of Wargames and Cyber Activity

	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

Research Question

- **When do cyber attacks on critical infrastructure become a national security problem?**

- **When do cyber attacks reach the level that DoD should be involved?**



NAVY – PRIVATE SECTOR CRITICAL INFRASTRUCTURE WAR GAME 2017

GAME REPORT

Dr. Jacquelyn Schneider
Mr. Benjamin Schechter
Ms. Rachael Shaffer

Support Requested by Agency

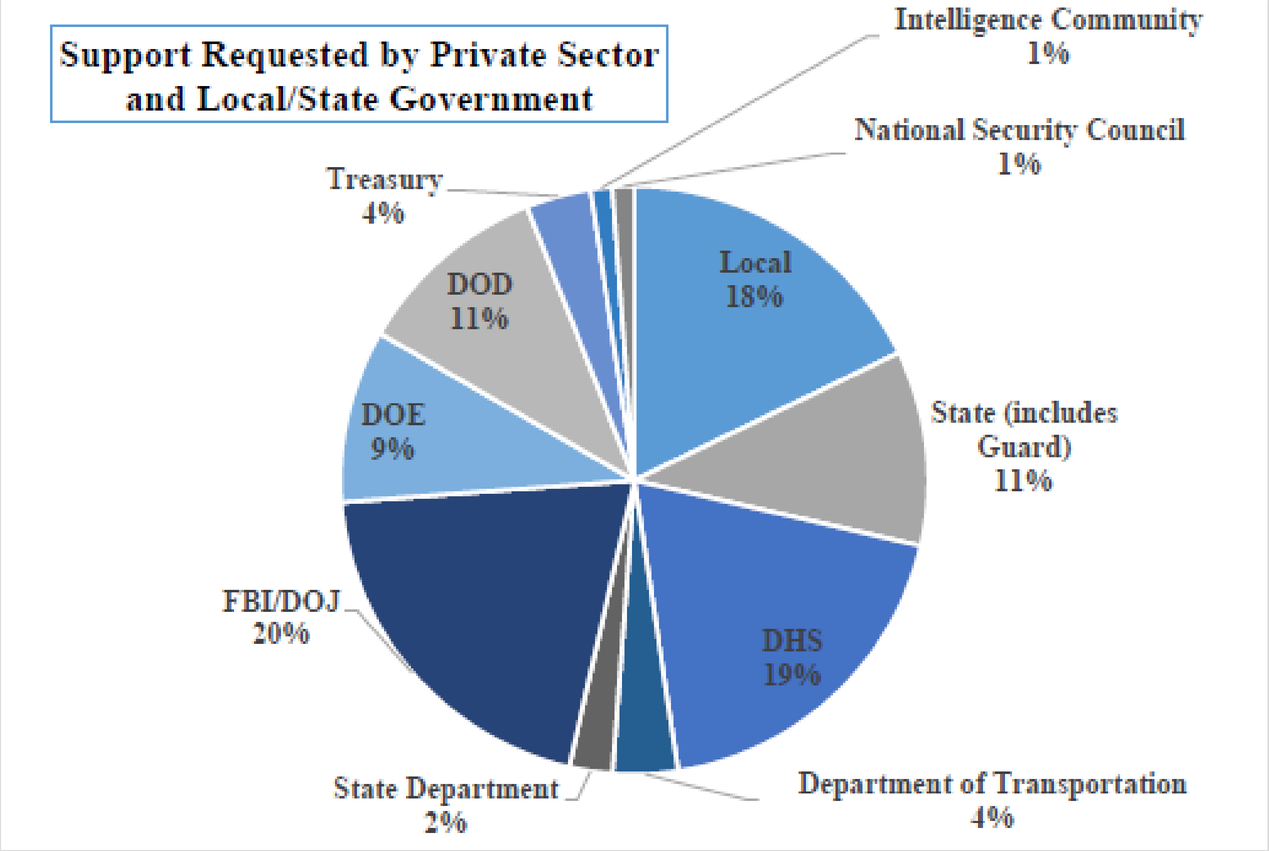
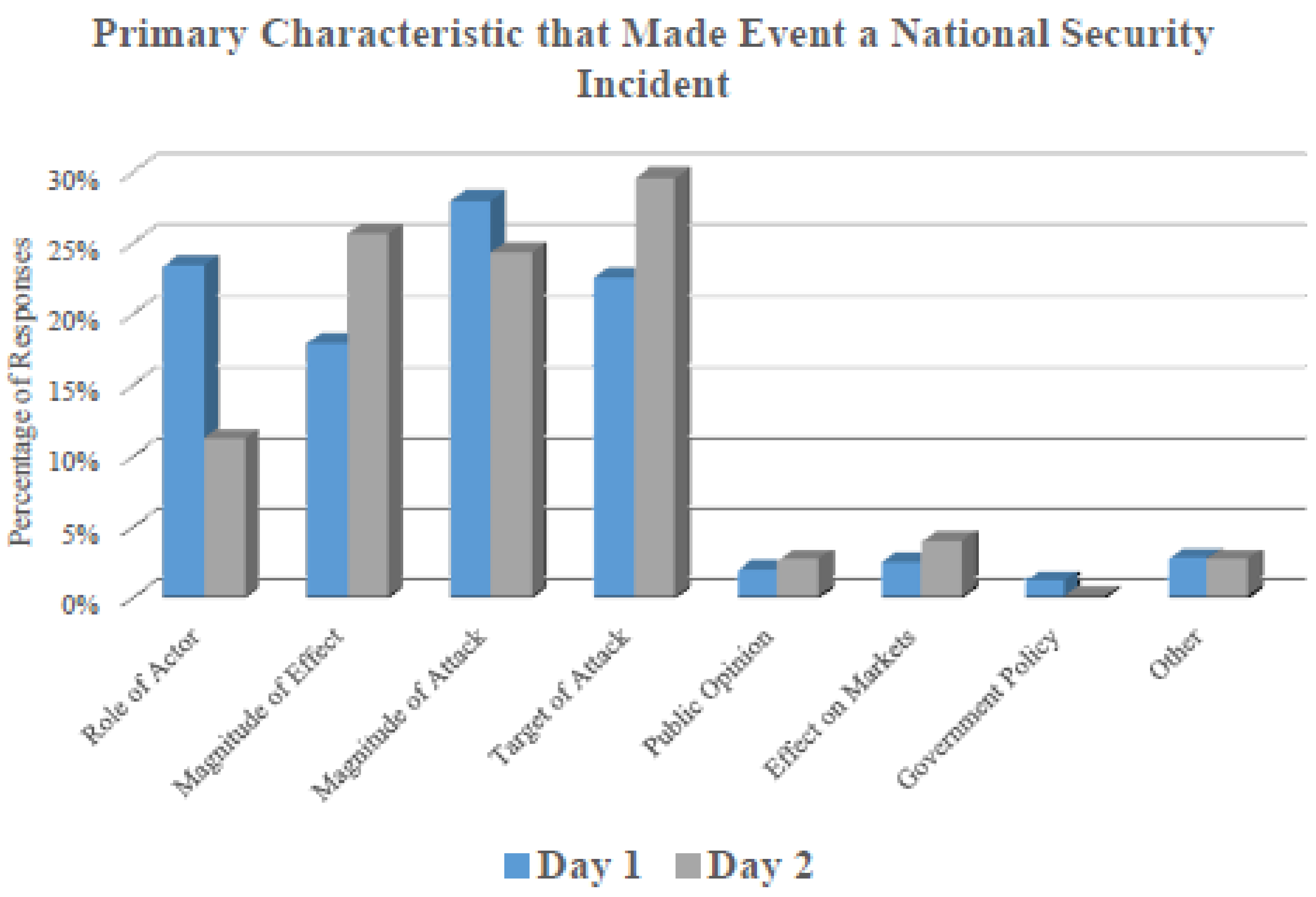


Figure 2. Break-out of Support Requested by Agency


Primary Characteristic that Made Event a National Security Incident
Percentage of Responses
30%
25%
20%
15%
10%
5%
0%
Role of Actor
Magnitude of Effect
Magnitude of Attack
Target of Attack
Public Opinion
Effect on Markets
Government Policy
Other
Day 1
Day 2

Cross-Domain Deterrence and Cyberspace: Evidence

- On Escalation

- **On Signaling**
  - – No evidence from war gaming that cyber operations are an effective signal
    - Difficulty linking action to effect (technical and cognitive problem)
    - “Cheap Talk” problem

- On Deterring Cyber Actions

Cross-Domain Deterrence and Cyberspace: Evidence

- On Escalation

- On Signaling

- **On Deterring Cyber Actions**
  - Deterrence by denial:
    - Defense and resiliency
    - What are the trade-offs?
  - Deterrence by punishment:
    - What's credible?

Research Sample 2:
U.S. Public Opinion

- **Does the instrument or the effect of attack matter more for support for retaliation?**

- **Survey experiment of American public**
  - 9 scenarios, attack on U.S. power plant

Cyber Attack, Economic Effects	Conventional Attack, Economic Effects	Nuclear Attack, Economic Effects
Cyber Attack, Loss of Life	Conventional Attack, Loss of Life	Nuclear Attack, Loss of Life
Cyber Attack, Nuclear Fall-Out	Conventional Attack, Nuclear Fall-Out	Nuclear Attack, Nuclear Fall-Out

Findings:
Support for Retaliatory Air Strikes

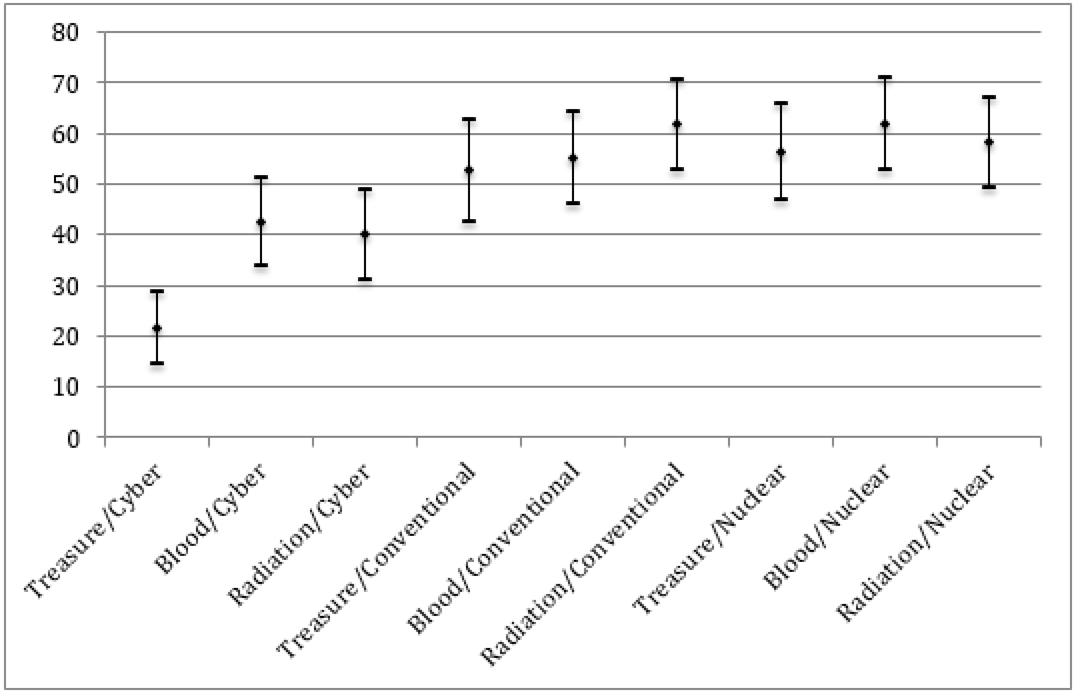
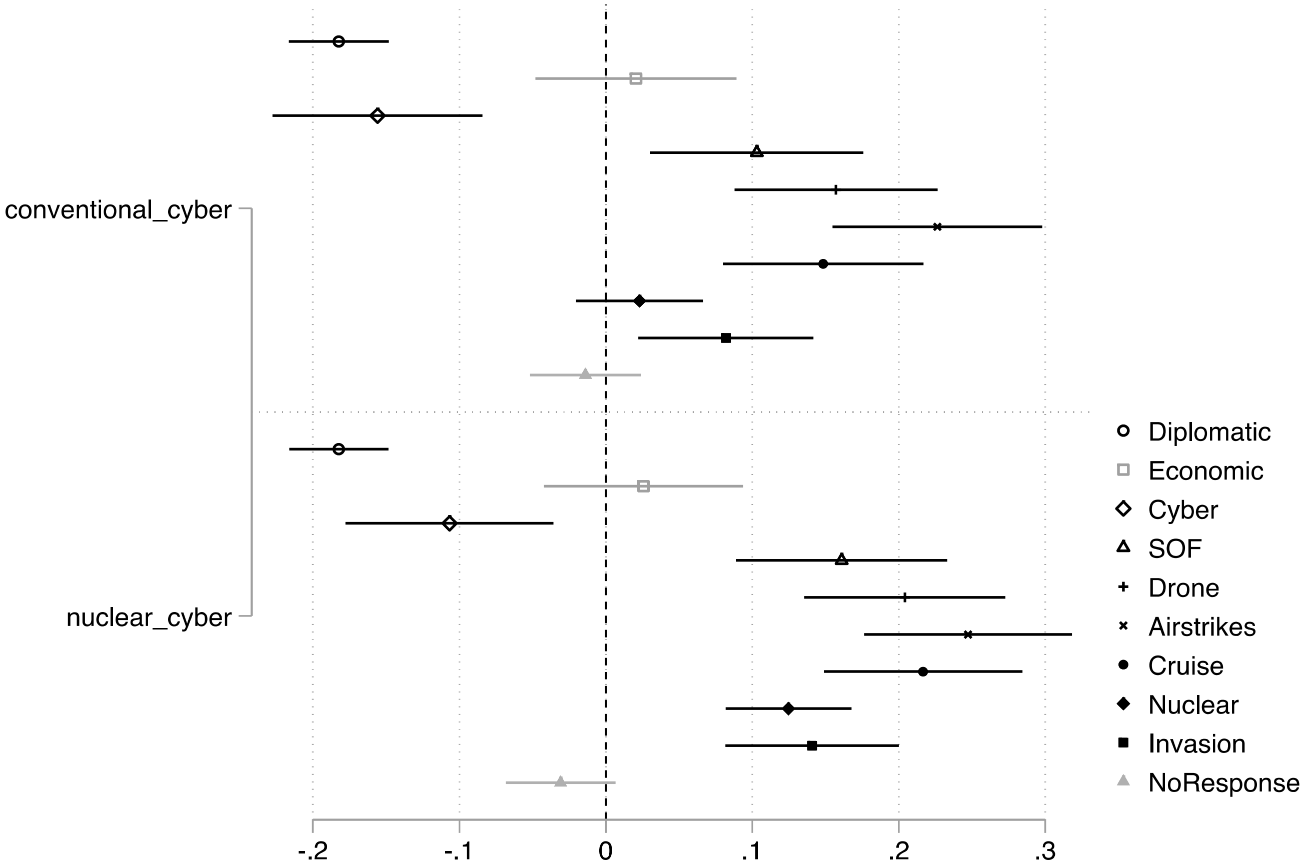


Figure 1. Overall levels of support across nine treatment groups, using airstrikes as the dependent variable (95% confidence intervals shown).

Findings: Support for Retaliatory Air Strikes



Cross-Domain Deterrence and Cyberspace: Policy Implications

- **Deter less with more credible punishment**
  - Focus on state actors
  - Limit deterrence to specific targets
  - Ambiguous on effects?

- **Counter-cyber operations to degrade adversary cyber capabilities**

- **Cyberspace ops not optimal for deterring across domains**

A large role for deterrence, but cyber strategy must move beyond just deterrence and instead think about what we value most and how we can actively use nation state instruments of power to retain what we value in cyberspace.

THE UNITED STATES NAVAL WAR COLLEGE

VIRIBUS MARI VICTORIA

Educating Leaders since 1884

www.usnwc.edu

Also search for us on Twitter and Facebook