Powerless to Change: Individual Security Policy Compliance in the Age of Cyberwarfare

Undergraduate Research in Progress

Undergraduate Researchers: Paul Wilmot (Information Systems), Griffin Gerry (Computer Science)
Graduate Mentor: Julia Stachofsky (Information Systems)
Faculty Advisor: Robert E. Closser, PhD (Information Systems)

BACKGROUND
- Cyberwarfare has become more prevalent, not just between military targets, but also encroaching into the lives of citizens.
- There are two primary research questions guiding this work:
  - What is the current state of the information systems and political science literature on cyberwarfare?
  - How do perceptions of cyberwarfare threats impact individual security decisions?

LITERATURE REVIEW RESULTS

Information Systems Literature Themes

- Public Awareness and Support / Escalations: The potential for escalation with cyberweapons is limited, as the public is less likely to support retaliation once presented with the lethal capabilities of cyberweapons or in the event of a cyberattack even with damage comparable to a physical strike. In the event of retaliation, it is possible that a retaliatory cyber strike could serve to prevent escalation in the physical domain, as cross-domain strikes in the event of a cyber strike are unlike. Paired with the attribution problem, this could decrease the possibility of further hostilities developing (Brantly and Smeets, 2020; Shandler et al., 2021).

Methods
- To answer the first research question, we conducted a systematic literature review of the information systems and political science literature.

- The top journals in political science and information systems as well as conference papers were searched for topics related to cyberwarfare and cyberterrorism.
- We then reviewed abstracts, resulting in 55 papers kept for further analysis and 27 papers removed for irrelevancy.

Future Work
- Future work will focus on developing a behavioral model to test the affects of cyberwarfare threat perceptions on employee security policy compliance.

- Below is a preliminary model based on our review of the literature.

ACKNOWLEDGEMENTS AND FUNDING
- The authors are grateful for funding from the Griffiss Institute under contract No. SA10012021MM0336.

Figure 1: Information Systems Literature

Figure 2: Political Science Literature

Figure 3: Preliminary Model

References


Cyberspace as a Military Domain: The internet is becoming a valid military domain, along with sea, air, and land. The attribution problem increases the possibilities for attacks, including strikes on those politically recognized as allies. Cyberattacks can be conducted with anonymity, technical and physical. Technology leaders fear the militarization of the internet, along with the possible unintended consequences of cyber strikes. Integrated digital systems mean the possibility for strikes on targets through either physical or digital means (Brantly and Smeets, 2020; Hare, 2019; Shandler et al., 2021, Sirolab, 2018).