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

Undergraduate Research in Progress

Undergraduate Researchers: Paul Wilmoth (Information Systems), Griffin Gerry (Computer Science)
Graduate Mentor: Julia Stachofsky (Information Systems)
Faculty Advisor: Robert E. Crossler, 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 does perception of cyberwarfare threats impact individual security decisions?

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.
- The remaining papers were read and sorted to develop the themes in Figure 1 and Figure 2.
- Themes are tentative and may change through further literature review cycles.

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

LITERATURE REVIEW RESULTS

Information Systems Literature Themes

Research focus: Cyberwarfare is still in its infancy as an area of study for Information Systems. Focus is still upon cybercrime and cyberterrorism rather than cyberwarfare generally (Hui et al. 2017), Bandyopadhyay and Mattord, 2008). Public perception of cyberattacks may be inaccurate due to skewed data impacting focused research. (Pipyros et al., 2016)

Regulation: Research focused on cyberwarfare tends to focus on development and adoption of regulation to solve the issue. Enforcing existing international regulations and the development of new international treaties (Ruohonen and Kimppa, 2019, Shin et al., 2018, Strouble and Carroll, 2008, Roche,2019). This incorporates a need for identification and classification of cyberwarfare as 'a use of force' and advocate for cyberwarfare as positive new step in conflict escalation (Heffter and Goel, 2018, Baskerville, 2010)

Policy – External: Policies dealing with management of external information/actors focuses upon deterrence and collaboration. Much of the research recommends having visible indicators of strong security as attackers target perceived weaker targets, (Cremonini and Nizovtsev, 2009) while others focus on agile active deterrence and information collection (Baskerville, 2004, Niakanlahiji et al., 2020). The other focus of information sharing shows stronger benefits for larger organizations and supports value of federally recommended programs such as Information Sharing and Analysis Centers. (Gal-or and Ghose, 2005, Smith et al., 2010)

Policy – Internal: Majority of research regarding policy focuses on internal security factors in the realm of cyberwarfare are in alignment with standard Information System Security standards. Addressing intentional and accidental misuse of information through access control, training on security procedures, and well-known sanctions. (Bhatt et al., 2020, D'Arcy et al., 2009, George et al., 2008, Lowry et al., 2015) The research shows a narrow zone where internal policy is particularly effective with strong user access controls (Bhatt et al., 2020) the threat of severe sanctions being more effective than certainty of sanctions (D'Arcy et al., 2009) and the point where strict policies backfire and increase instances of misuse (Lowry et al., 2015). A nuanced, well-balanced internal policy is preferable and sits in this narrow effective range.

Figure 1: Information Systems Literature

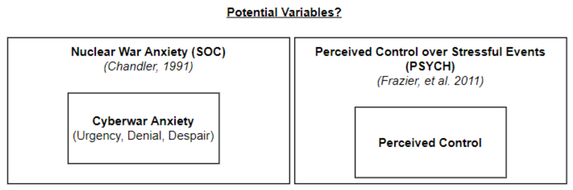
Political Science Literature Themes

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 unlikely. Paired with the attribution problem, this could decrease the possibility of further hostilities developing (Brantly and Smeets, 2020, Shandler et al., 2021)

Education/Knowledge: Military and political leaders require education on the capabilities and options that become available through cyberweapons. With education of the public, the escalatory possibilities of cyberweapons are likely to become limited. Cyber warfare, attacks, and weapons deserve appropriate definitions and refinement, for political and military purposes (Hare, 2019, Shandler et al., 2021).

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, Siroli, 2018).

Figure 2: Political Science Literature



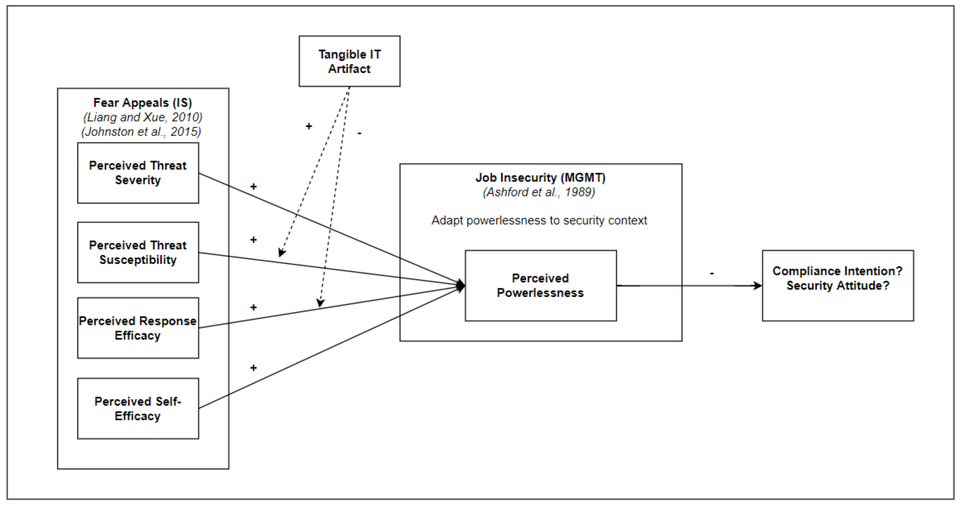


Figure 3: Preliminary Model

ACKNOWLEGEMENTS AND FUNDING

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

References
Brantly, A., & Smeets, M. (2020). Military operations in Cyberspace. *Handbook of Military Sciences*, 1–16. https://doi.org/10.1007/978-3-030-02866-4_19-1
D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98. https://doi.org/10.1287/isre.1070.0160
Hare, F. (2019) Precision cyber weapon systems: An important component of a responsible national security strategy?, Contemporary Security Policy, 40:2, 193-213, DOI: 10.1080/13523260.2018.1529369
Shandler, R., Gross, M. L., & Daphna Canetti (2021) A fragile public preference for cyber strikes: Evidence from survey experiments in the United States, United Kingdom, and Israel, Contemporary Security Policy, 42:2, 135-162, DOI: 10.1080/13523260.2020.1868836
Siroli, G. P. (2018) Considerations on the Cyber Domain as the New Worldwide Battlefield, The International Spectator, 53:2, 111-123, DOI: 10.1080/03932729.2018.1453583

Carson College of Business, Washington State University
Voiland College of Engineering & Architecture, Washington State University