**Literature Review and Variables**

Britain Cox

The University of Arizona Global Campus

HSM 497: Homeland Security & Emergency Management Capstone

Kenneth Jenkins

August 16, 2021

**Literature Review and Variables**

 Cybersecurity refers to the protection of individuals’ electronic data against criminal or unauthorized use of the data. It also encompasses the measures taken to achieve this. In the United States, the Department of Homeland Security (DHS) has a central role to play in cybersecurity. In as much as Homeland Security has the lead for the federal government to secure public government computer systems, it appears to have no formal authority to probe federal government agencies to apply recommended cybersecurity mitigation measures. This lack of clarity on the nature and implication of authorities presents a loophole for potentially dangerous mission failure. Due to lack of clarity, judging the adequacy of the department and the fundamental nature and extent of the role played by the DHS in securing cyberspace security is difficult. There are legal authorities in place that prove the DHS can act. These authorities fall under two categories namely; primary and secondary authorities. Primary authorities include the U.S constitution, legislation, executive orders, administrative regulations, court opinions, and treaties, among others. These authorities carry the force of law and can bring perpetrators to justice. Cyberspace continues to evolve quickly, meaning that current cyberspace authorities are increasingly outdated. The United States lacks an integrated cybersecurity strategy that can stand if the nation passes laws that ensure effective regulations by the administration. There is a higher need to develop, promulgate, and update guidelines, codes, rules, and accepted standards that ensure confidentiality, integrity, and availability of systems, networks, and data without impairing innovation.

**Research variables**

Research variables are entities that can take on different values, which means they are typically any entity in research that varies under different conditions. In this research, the variables selected will help collect, analyze and interpret available data. They will also help validate my hypothesis.

**Research variable 1: Survey on the activities of homeland security**

As the independent variable, the survey put into action by investigative research to help determine the efficiency and adequate preparedness of Homeland security in cybersecurity matters. Contrasting the independent and dependent variables, (effect of homeland security activities on their efficiency in reducing cybercrime) will help bring out the truth of this research.

**Research variable 2: Outcome of homeland security activities on cybersecurity**

This intervening variable cuts across both independent and dependent variables to bring out the link between the two. It reflects on the measures in place and factors that reduce or increase cybercrime. The variable helps predict the outcome of the research.

**Research variable 3: Understanding cybercrime-related activities**

This antecedent variable plays a part to help justify the hypothesis. It brings to light the crime and explores the causes of cybercrime as a phenomenon on its own. According to the coursebook, Empirical Political Analysis, hypotheses statements represent the relationships between variables. Based on this statement, using both intervening and antecedent variables in the research will help thoroughly explain the hypothesis. The use of these research variables plays a major role in answering the hypothetical questions that could help create strategies to ensure preparedness for homeland security in dealing with cybersecurity in the future.

Annotated bibliography

Brians, C.L. (2016) Empirical Political Analysis: Pearson new international edition course smart e-textbook. Routledge.

The book introduces the research of social science. It prepares readers to conduct both qualitative and quantitative research offering basic concepts that apply to a wide range of research settings. The book has been particularly useful in the research as it has provided an in-depth understanding of the research process- from hypotheses formation all the way to research report writing.

Centre for Strategic and International Studies (CSS) Commission on cybersecurity for the 44th presidency. 2011. Cybersecurity two years later. Washington, DC: CSIS, 2008. Securing cyberspace for the 44th presidency.

The article authored by Lawrence J Trautman provides a clear description of the role of Universities in cybersecurity research. Here, different universities such as Harvard, Massachusetts Institute of Technology (MIT), Stanford University, the University of California, and South Methodist University have immense contributions in research on cybersecurity and the different articles published by scholars from these institutions.

Craigen, Dan, Nadia Diakun-Thibault and Randy Purse “Defining cybersecurity. “Technology innovation management review” 4(10).

This review seeks to give an in-depth definition of cybersecurity. Discussions with practitioners, academics, and graduate students helped gather multiple perspectives in defining cybersecurity. It also looks at the role of technology in the rise of cybercrimes.

Lehmann, P., Beck, S., de Brito, M. M., Gawel, E., M, Haase, A., &Thran., D (2021). Scrutinizing popular hypotheses from a social science perspective. Sustainability, 13(16), 8679.

The authors of the book provide a basic understanding of the different research concepts associated with social sciences. It explores each concept briefly to impart skills to students researching in the field of social sciences. The author explores different approaches to conducting research and conceptualizing topics.

Singer, P., & Friedman, A. (2014). Cybersecurity and cyberwar (1st Ed.). New York:

 This book provides information necessary to understand the basics of cybercrimes and cyberwar. It is pertinent to our research topic since it explores different aspects of cybersecurity. As the title suggests, this book offers what individuals need to understand and secure their cyberspace.