Measuring the size and severity of the integrated cyber attack surface across US county governments

Koren Brahm

The School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

March 27, 2025

Cybersecurity and the Social Sciences: An Exploration of County-Level Vulnerabilities

Introduction

The article “Measuring the size and severity of the integrated cyber attack surface across US county governments” by Harry, Sivan-Sevilla, and McDermott offers a detailed examination of cybersecurity vulnerabilities at the county government level. By employing an interdisciplinary approach that combines technical expertise and social sciences, this study offers valuable insights into systemic risks and policy implications. This essay explores the study’s relevance to social sciences, its research framework, methods, findings, and societal contributions (Harry et al., 2025).

Principles of the Social Sciences

The article relates to various social science fields such as criminology, anthropology, economics, geography, political science, psychology, and sociology. It investigates cyber vulnerabilities that lead to crimes, aiding in understanding criminal behaviors and creating strategies for prevention. It considers how cultural and behavioral patterns in communities influence their approaches to managing cybersecurity challenges. The study addresses how financial resources are distributed to enhance cybersecurity and the economic consequences of cyber-attacks on local governments. It examines the differences in cybersecurity risks and resources across counties, highlighting spatial patterns. The article evaluates how governance and policies at the county level impact cybersecurity preparedness and resilience. It focuses on human elements like risk awareness and decision-making among government officials, which affect cybersecurity implementation. It explores how social structures and community interactions shape the cybersecurity environment and vulnerabilities. Social sciences offer a framework to examine the societal and organizational behaviors that influence vulnerabilities and resilience (Harry et al., 2025).

Research Questions and Hypotheses

The study seeks to determine the extent of county-level cyber vulnerabilities and identify the factors influencing these risks. It primarily investigates the following questions: What is the size of the cyber attack surface at the county government level? What factors influence the diversity and vulnerability of internet-facing devices? It hypothesizes that disparities in resources and infrastructure contribute to variations in the size and diversity of the attack surfaces (Harry et al., 2025).

Research Methods

The authors gathered data on 42,735 internet-facing devices within U.S. county governments. The authors utilized Open Source Intelligence (OSINT) to gather data on these internet-facing devices across 3,095 counties. This mixed-methods approach, combining quantitative and qualitative analyses, captures both the technical and sociopolitical dimensions of cybersecurity (Harry et al., 2025).

Data and Analysis

The authors collected comprehensive data on 42,735 internet-connected devices from 3,095 U.S. county governments, covering 98% of counties. This data enabled them to assess vulnerabilities, identify trends, and evaluate risk factors. They measured the size and diversity of exposed infrastructures, identifying risks. Relationships between factors such as county population sizes and cyber vulnerabilities were explored to uncover patterns. Common Vulnerability Exposures (CVEs) were analyzed to estimate potential exploitation risks, providing insights into misconfigurations and weaknesses. The study examines the configurations and exposure of devices, identifying trends in size, diversity, and susceptibility to cyber-attacks. By

employing statistical tools and comparative analyses, the authors uncover disparities in vulnerabilities, emphasizing the critical need for equitable resource distribution and policy interventions (Harry et al., 2025).

Relevance to Class Concepts

The article reflects class concepts such as cybersecurity and social sciences, social science principles and methods, human factors, psychological aspects of cyberoffending and victimization, cybersecurity's social dimensions, and social dynamics and structures in cybersecurity. The research merges technical assessments with social science insights to explore the impact of local government vulnerabilities on national resilience, displaying the intersection of technology and societal structures. The study employs empirical research methods, including data collection and analysis of vulnerabilities, which align with standard social science practices of systematic investigation. By addressing service misconfigurations and risk management, the article indirectly highlights the role of human error and decision-making in cybersecurity. While focusing on infrastructure, the research provides insight into how vulnerabilities may be exploited by offenders, leading to potential victimization – topics that can be explored through psychological lenses. The study underscores how local government vulnerabilities contribute to risks at a national level, emphasizing the interconnectedness of systems and collective consequences. The research points out the role of county governments within the broader social structure, where their cybersecurity practices are both shaped by and influential to larger national policies and dynamics (Harry et al., 2025).

Impact on Marginalized Groups

The research sheds light on how marginalized communities are disproportionately affected by cyber-attacks on county services like healthcare and social programs. They are

affected by interruptions in healthcare, disruption of social services, data privacy risks, digital divide effects, and trust in institutions. Cyber-attacks can disrupt medical services, delay treatments, and compromise patient records. Cyber incidents can hinder essential programs like housing assistance or food support. Personal and sensitive information, such as health or financial data, can be exposed during cyber-attacks. Limited access to technology and cybersecurity awareness puts marginalized communities at a disadvantage, making it more difficult for them to handle or recover from the aftermath of cyber-attacks. Frequent cyber-attacks can reduce confidence in public services, discouraging marginalized groups from seeking the help they need due to concerns about data security. The article advocates for addressing systemic inequities to ensure the resilience of systems serving vulnerable populations (Harry et al., 2025).

Societal Contributions

The research offers significant benefits to society by improving cyber resilience, informing policy, raising awareness, and promoting collaboration. Identifying localized vulnerabilities helps enhance national cybersecurity. The findings assist policymakers in prioritizing resources and designing effective cybersecurity strategies. The study underscores the critical role of local governments in protecting national infrastructure. It highlights the need for an integrated approach, viewing counties as part of a larger cybersecurity ecosystem (Harry et al., 2025).

Conclusion

Overall, the article highlights how technical vulnerabilities are deeply intertwined with organizational and societal factors, offering a multidimensional understanding of cybersecurity challenges. By exploring the interplay between social sciences and cybersecurity, this research

emphasizes the value of interdisciplinary approaches in addressing systemic vulnerabilities. This study not only illuminates the cyber vulnerabilities at the county level but also reinforces the importance of an interdisciplinary approach. Its findings contribute significantly to policymaking and societal resilience, underscoring the importance of equitable resource allocation and collaboration across disciplines (Harry et al., 2025).

References

Harry, C., Sivan-Sevilla, I., & McDermott, M. (2025). Measuring the size and severity of the integrated cyber attack surface across US county governments. *Journal of Cybersecurity*, 11(1), tyae032. https://academic.oup.com/cybersecurity/article/11/1/tyae032/7959399.