Article Review #2: Maximizing the Benefits from Sharing Cyber Threat Intelligence by Government Agencies and Departments

Nicolas R. Stephens

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Diwakar Yalpi

April 15th, 2026

Introduction/BLUF

The article, "Maximizing the benefits from sharing cyber threat intelligence by government agencies and departments," seeks to investigate the economic impact resulting from organizations receiving unclassified CTI (Cyber Threat Intelligence) from the United States Government. Specifically, the study addresses a common public and private misconception that government agencies and departments should only prioritize CTI sharing regarding the most severe vulnerabilities, instead arguing for strategies to be based upon how CTI updates the target organization's internal risk assessment (Dykstra et al., 2023).

According to the authors, the greatest economic benefit for any given organization occurs when government-provided CTI explicitly contradicts internal security beliefs, more so when the organization previously believed that a threat level was low or a vulnerability was at low risk of exploitation. Thus, leading to more efficient, effective, and impactful internal cybersecurity technical adjustments, and more accurate cybersecurity spending.

Relation/Connection to Social Science Principles

This article elegantly incorporates all seven social science principles to scientifically examine the impact of government cyber threat intelligence sharing. First, the study utilizes relativism to show the direct impact of government shared information with the economic decision-making and the subsequent impact on collaborating private organizations. Second, the study is parsimonious, or simple, as the authors reduce complex human behaviors related to security investment to a few key variables. Third, the authors remain objective throughout the entire article, meaning they focus on data-driven statistics, economic modeling, and mathematical modeling to study the often-biased and emotionally charged sector of business that

is cybersecurity budgeting. Similarly, the authors implement the fourth element of the social sciences principles, which is empiricism, or the idea that findings are based on measurable data points like investment amounts (*z)*, probability of attack (*p)*, and financial gain (*G)*. Ethical neutrality, the fifth principle, is upheld through the research for this article being conducted in a value-free way that respects the balance between private sector concerns about confidentiality and data privacy and the government's mission to protect American citizens and maintain national infrastructure security. The sixth principle, determinism, is the foundation for the author's economic model, since they believe that an organization's economic impact and investment behavior is not random, but is influenced by factors relating to internal prior security beliefs and government CTI. Through rigorous identification of these causal factors, the authors can map out conditions that will result in the highest possible financial gain for the organization. The last principle, skepticism, is among the very foundation of the paper, as the researchers chose to critically examine the concept that government CTI should only be shared on the most severe vulnerabilities. After careful examination and rigorous mathematical proofs, the researchers were able to scientifically refute that belief and instead concluded that only sharing government cyber threat intelligence on critical vulnerabilities is detrimental to national cybersecurity, and sharing information more frequently that updates an organization's underestimated risks is the correct approach to maintain nationwide cyber stability.

Research Question /Hypothesis/ Independent Variable/Dependent Variable

In this article, the researchers address a major research question: Under what specific conditions can an organization maximize the economic benefits gained from receiving and

processing unclassified cyber threat intelligence (CTI) shared by the United States Government? To answer this question, the authors test and propose several different hypotheses.

The first hypothesis, presented in Lemma 1, states that the optimal cybersecurity budget for an organization increases as its belief in the likelihood of an attack increases. This essentially means that if government cyber threat intelligence successfully convinces an organization that a cyberattack is more likely than that organization previously thought, a rational business would increase its cybersecurity budget to combat that vulnerability; conversely, the same scenario applies as well. The second hypothesis, defined in Proposition 2, states that an organization's economic benefit increases as the difference between its data or prior belief and the government CTI increases. Essentially, this means that if the government shares information the business already knows, the business doesn't gain an economic benefit. But if the government shares information that the business doesn't know, then the company receives better economic output. The third hypothesis is the most substantive of the three, with this hypothesis stating that the benefit is at its absolute greatest when the organization's prior belief of a threat was either low or non-existent. This hypothesis relates to the concept of diminishing returns. Essentially, if a company already knows a threat is high and has already invested heavily into reducing that threat, adding more money only slightly improves the situation, while investing in a threat that a company was previously underestimating or unaware of provides a greater economic gain to be had.

Regarding variables, this study has two independent variables, which are used as inputs into the researcher's economic model to see how they change an organization's behavior. The two primary independent variables are the organization's prior belief, represented as $\bar{p}$, and threat level, indicated by cyber threat intelligence (CTI), represented as p. The organization's prior

beliefs represent the probability that an organization initially assigns to a threat vector before they receive government intelligence. The threat level indicated by CTI is the probability of an attack as reported by the U.S. cyber threat intelligence report.

Regarding the dependent variable, or the result of the change from the independent variable the two main dependent variables are optimal level of cybersecurity investment, represented as z^* and economic benefit or gain represented as G. The Optimal level of cybersecurity investment is the amount of money or resources that an organization chooses to spend on cybersecurity after analyzing the government CTI report and the economic benefit or gain represents the total financial value or cost-savings an organization obtains by adjusting their security stance based on the government's CTI report.

Types of Research Methods used

The researchers utilized quantitative research methods, specifically, formal economic modeling and information theory instead of obtaining their data through direct surveys or field experiments. The researchers developed a generic mathematical model to simulate how a rationally operated organization adjusts its behavior when receiving government cyber threat intelligence.

Types of Data Analysis used

The researchers utilized quantitative research methods, specifically, formal economic modeling and information theory, instead of obtaining their data through direct surveys or field experiments. The researchers developed a generic mathematical model to simulate how a rationally operated organization adjusts its behavior when receiving government cyber threat intelligence.

Connections to other Course Concepts

This study directly embodies several key concepts from the course presentations. Firstly, the paper addresses the human factors of cybersecurity by highlighting scenarios that could have been potentially caused by information overload or just simple human error. The study could also be compared to a cost-benefit analysis, as the authors create a systematic approach to weighing the costs of security investment against financial benefit, and potential losses if the CTI report is not handled correctly. The article also relates massively to the realm of risk management through careful examinations of prior beliefs and internal risk assessments, which are updated based on newly acquired government knowledge.

Connections to the Concerns or contributions of Marginalized Groups

This paper highlights concerns about cybersecurity, mainly regarding small to medium-sized companies, which are often marginalized through resource constraints, technological capacity, employee experience, etc. This paper does not and should not be hyper-focused on ultra-large corporations with thousands of IT and Cybersecurity personnel, as they are not as constrained when it comes to the previously mentioned factors. Of course, they should still receive CTI reports, but that's not what the study was about, as it focused on cost-saving techniques and economic gain for smaller companies that need more government assistance when it comes to security. Furthermore, the article indirectly addresses the marginalization of human factor experts as intelligence sharing requires a deep understanding of the human brain, especially around prior beliefs and changing organization-wide cybersecurity strategy.

Overall societal contributions of the study/Conclusion

In conclusion, this paper makes significant societal contributions by providing a data-driven, simulated roadmap for enhancing national cyber-stability through improved information-sharing tactics with United States Government agencies and departments. The biggest contribution this paper makes is a scientific, data-driven refutation of the belief that federal agencies should prioritize information sharing only for high-level vulnerabilities. This study shows that organizations gain the greatest benefit from updating underestimated risks identified by government agencies, allowing the government to focus intelligence on areas that will have the greatest impact on American businesses. Ultimately, this paper advances the social sciences by reinforcing the idea that cybersecurity isn't just a technical domain, but one shaped by human beliefs and incentives that determine the safety of our interconnected digital world and the stability of the American economy

Reference

Josiah Dykstra, Lawrence A Gordon, Martin P Loeb, Lei Zhou, Maximizing the benefits from sharing cyber threat intelligence by government agencies and departments, *Journal of Cybersecurity*, Volume 9, Issue 1, 2023, tyad003, https://doi.org/10.1093/cybsec/tyad003