Article Review #1: Cybercrime Risks in Cross-Border Investment Contracts

Matthew Chestnut

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Yalpi

02/27/2026

Introduction

The article, *Cybercrime Risks in Cross-Border Investment Contracts*, goes over how cybercrime is an increasing threat in international economic agreements in an online economy. In his article, Hamza argues that an underdeveloped legal framework and weak enforcement procedures allow more cybercrime to be committed without proper prosecution.

Relation to Social Science Principles

Relativism is related to the article due to how cybersecurity is interconnected with political, economic, legal, and technological systems. More reliance on a developing cyberspace in economic use has caused a grey area where cybercrime hasn't yet been defined and doesn't have a good legal system in place yet, causing many issues internationally. This article demonstrates how a weakness in one system, such as cybercrime laws being developed, has directly affected other systems like global economic stability.

Skepticism also plays a big role in this article in the sense that society needs to question current international cybercrime laws to progress it. If users only assume that there is a set framework, then criminals can keep on using these loopholes without punishment.

The principle of determinism is shown in the article that cyber risks are influenced by earlier technological and legal developments. The vulnerabilities in international contracts are not random but are shaped by how countries have developed and enforced their cybercrime laws over time. This shows that cyber problems are from prior conditions and structural decisions rather than happening randomly.

Research Question: How do cybercrime risks affect the international economy, and why is the current cybercrime legal system not good enough?

Hypothesis: Inconsistencies in cybercrime laws and weak international enforcement increase the risk for international deals

Independent Variable: The ability to use national cybercrime laws and international enforcement mechanisms.

Dependent Variable: The level of risk and vulnerability in international deals

Research Methods used

This article mainly uses qualitative research methods through reliance on legal analysis, policy review, and examination of international frameworks from past cybercrime and economic deals. The author doesn't use any experiments or surveys but focuses more on the research side of analysis.

Outside Course Concepts

This article demonstrates that cybersecurity should be examined from an interdisciplinary approach. Legal studies, economic policies, and technological advancements contribute to cyber risk, which supports the course's emphasis on the importance of a social science approach to cybersecurity.

Conclusion

In conclusion, this study contributes to our understanding of cybersecurity as a global structural problem, not just a local technical problem. It shows that cybercrime risks in international contracts are determined by legal loopholes between nations. The article contributes to our knowledge by relating cybersecurity, international law, and economic systems, and by underscoring the importance of global policies to support digital security in the international economy.

References

https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/download/225/87/419