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

Student Name: Christopher Hilliard

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date:4/3/26

Introduction/BLUF

This article talks about how cybercrime is becoming a big problem in international business and investment contracts. The main idea is that as more business moves online cyberattacks are making it harder to keep contracts safe and enforce them properly. This article shows that current laws are not fully ready to deal with these new digital threats.

Relation/Connection to Social Science Principles

The article connects to all 7 social science principles in different ways. It shows empiricism because it uses real case studies and legal examples instead of just options. It also shows objectivity since the author focuses on facts about cybercrime and laws without bias. Relativism is shown because different countries have different laws and ways of handling cybercrime which makes global agreements harder. It also connects to determinism because human behavior and the growth of technology both influence the rise of cybercrime. Parsimony is shown since the article explains that as technology grows cyber risks increase which is a simple but strong idea. Ethical neutrality is present because the author explains cybercrime without judging people and focuses more on the issue itself. Lastly it shows skepticism because the article questions if current laws are really strong enough to handle modern cyber threats.

Research Question /Hypothesis/ Independent Variable/Dependent Variable

- Research Question: How does cybercrime affect cross-border investment contracts and are current legal systems strong enough to handle these threats

•

- Hypothesis: The author suggests that current laws are not prepared to deal with modern cybercrime in global investments
- Independent Variable: Increase in cybercrime and use of digital technology in business
- Dependent Variable: Security and reliability of cross border investment contracts

Types of Research Methods used

The study used qualitative research methods. The author looked at legal systems case studies and past research instead of doing surveys or experiments. This helped show real examples of how cybercrime affects investment contracts.

Types of Data Analysis used

The article uses legal and document analysis. It looks at patterns in cybercrime cases and compares how different legal systems respond. The focus is more on explaining the problems instead of using numbers or statistics.

Connections to other Course Concepts

The article shows that social cybersecurity matters because cybercrime in global investments involves human trust and behavior, not just technology. Social engineering, weak governance, and mistakes in human behavior create openings for criminals across countries. Overall it shows that cybersecurity depends on people, rules, and teamwork, not just technical systems.

Connections to the Concerns or contributions of Marginalized Groups

This topic affects marginalized groups because smaller countries or developing nations may not have strong cybersecurity systems. This makes them easier targets for cyberattacks. Smaller businesses can also be affected more because they do not have the same resources as big companies. This can increase inequality and make it harder for them to compete.

Overall societal contributions of the study/Conclusion

In conclusion this study helps people understand how cybercrime is affecting global business and investments. It shows that current laws are not strong enough and need to be improved. It also explained how countries need to work together more to solve this problem. This is important because cybercrime does not just affect one person it affects the whole economy and society.

Reference

Albaheth, H. E. (2025). Cybercrime risks in cross-border investment contracts: Legal challenges and regulatory responses in commercial and investment law. *International Journal of Cyber Criminology, 19*(1), 138–153.

Article Link: https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/457/138