

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

Student Name: AJ Guevara

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 02/26/26

### **Introduction/BLUF**

The article “Cybercrime Risks in Cross-Border Investment Contracts: Legal Challenges and Regulatory Responses in Commercial and Investment Law” by Hamza E. Albaheth, which examines how increasing cyber threats are disrupting international investment agreements in today’s digitized global economy. The study research how cyberattacks, digital evidence manipulation, and jurisdictional challenges affect the enforceability of cross border contracts. The author argues that current international legal frameworks, like UNCITRAL, ICSID, and Bilateral Investment Treaties, are not fully equipped to address cyber enabled risks, and significant legal modernization is necessary to protect digital investments and maintain investor confidence.

### **Relation/Connection to Social Science Principles**

The article relates to a lot of key principles of social science. First, relativism is reflected in the way the author shows that cybersecurity is interconnected with economic, political, legal, and technological systems. As digital technologies such as blockchain and smart contracts expand, changes in the technological system directly influence international investment law and dispute resolution processes. Second, the principle of empiricism is demonstrated through the article’s reliance on documented arbitration cases and real world cyber incidents rather than opinion. The study evaluates observable legal disputes involving digital evidence to assess weaknesses in current frameworks. Third, skepticism appears in the author’s critical questioning of whether existing treaties and arbitration systems are truly capable of addressing cyber enabled harms. By analyzing cybersecurity as a systematic and evidence based issue, the article applies social sciences principles to understand how digital threats reshape global investment law.

### **Research Question /Hypothesis/ Independent Variable/Dependent Variable**

The main research question in the article is how cybercrime affects cross border investment contracts and whether current international legal systems are prepared to handle these digital risks. The author suggests that existing legal frameworks, such as UNCITRAL and ICSID, are not fully equipped to deal with cyber related disputes. Although the article does not state a formal hypothesis, it argues that increasing cyber threats create weaknesses in international investment enforcement. The independent variable in the study is the rise of cybercrime risks, including cyberattacks and digital evidence problems. The dependent variable is the effectiveness of international investment agreements and dispute resolution systems. So, as cybercrime increases, the ability of legal systems to protect digital investments becomes more difficult.

### **Types of Research Methods used**

The study uses qualitative research methods rather than quantitative analysis. The author does not collect numerical data or conduct surveys. Instead, the research is based on legal analysis and case studies. The article examines existing international legal frameworks, arbitration cases, and documented cyber incidents to understand how cybercrime affects cross border investments contracts. The data was collected from scholarly sources, legal treaties such as UNCITRAL and ICSID, and real dispute resolution cases. Overall, the study relies on document analysis and comparative legal reviews to evaluate weaknesses in current international investment law.

### **Types of Data Analysis used**

The article mainly uses descriptive and diagnostics analysis. It uses descriptive analysis to summarize existing legal frameworks, arbitration cases, and examples of cyber incidents

affecting cross border investment contracts. It then applies diagnostic analysis to explain why current legal systems struggle with cyber related disputes and offers perspective recommendations for improving cybersecurity protections in international investments law.

### **Connections to other Course Concepts**

The article connects to the course that cybersecurity is an interdisciplinary field that combines social science and technology. It shows that cybersecurity problems are not only technical but also supports the idea of human-centered cybersecurity, which explains that human behavior and institutional responses affect security outcomes.

### **Connections to the Concerns or contributions of Marginalized Groups**

The article does not directly focus on marginalized groups, but it still affects them. Developing countries may have weaker cybersecurity systems, making them more vulnerable to cybercrime in international investment agreements. If cyber risks reduce foreign investment, marginalized communities could lose jobs and economic opportunities. Improving cybersecurity laws can help create more fairness and stability for vulnerable populations.

### **Overall societal contributions of the study/Conclusion**

In conclusion, the study contributes to society by showing that cybercrime is not only a technical issue but also a legal and social problem that affects global economic stability. It highlights weaknesses in current international investment laws and explains why legal systems must adapt to digital threats. The article advances our understanding of cybersecurity by connecting technology with social institutions such as law, politics, and economics. Overall, it demonstrates that protecting digital investments requires both technological solutions and strong legal frameworks.

### **Reference**

Albaheth, Hamza. "A Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License Cybercrime Risks in Cross-Border Investment Contracts: Legal Challenges and Regulatory Responses in Commercial and Investment Law." *International Journal of Cyber Criminology*, vol. 19, 2025, <https://doi.org/10.5281/zenodo.476619107>. Accessed 27 Feb. 2026.

**Article Link:**

<https://cybercrimejournal.com/menuscrypt/index.php/cybercrimejournal/article/view/457/138>