Article Review 2: Cybercrime Risks in Cross-Border Investment Contracts

Alex G Bretana

Old Dominion University

CYSE201S: Cybersecurity and the Social Sciences

Prof. D. Yalpi

11/14/2025

This review looks at a 2025 article by Hamza E. Albaheth that explores how cybercrime is creating serious problems for international business deals. As more companies use digital contracts and online systems for their investments, criminals are finding new ways to attack these systems. The study shows that current laws are not keeping up with these fast changing digital threats and suggests ways to fix this growing problem.

The article connects to several important social science ideas. It examines how laws and legal systems work across different countries, which is a key topic in political science. It also looks at how trust between business partners can be broken when cyber attacks happen, which relates to economics. The research shows that when countries have different rules about cybercrime, it becomes very hard to punish criminals who operate across borders. These national differences in definitions of cybercrime and standards of evidence undermine effective international collaboration.

The main questions the article tries to answer are how cyber attacks hurt international business agreements and why current laws are failing to stop these problems. The research focuses on how the growing use of digital technology in business affects how well legal systems can protect these deals. The study uses real examples to show these problems, like the 2016 DAO attack where hackers stole over $60 million using a vulnerability in a smart contract. More recently, in 2023, Euler Finance lost nearly $197 million in a flash loan attack, showing that these problems continue.

The research method involves studying actual cases rather than using numbers or statistics. The author examines legal cases and compares how different countries handle digital evidence. For example, the article discusses how in some arbitration cases, hacked emails were used as evidence even though they were obtained illegally. In one case between a Brazilian

company and Canadian partner, the court allowed hacked emails as evidence, focusing more on whether the evidence was relevant than how it was obtained.

This connects to principles we have learned in class, such as empiricism, which stresses that knowledge must come from observable and verifiable evidence. However, digital evidence like blockchain records or server logs can be easily altered or damaged, challenging its reliability in legal proceedings. The principle of skepticism reminds us to critically examine such evidence for potential tampering, especially since existing regulations lack clear standards for handling compromised digital data. We have also studied determinism in the context of state responsibility, where understanding the preceding events that lead to state-sponsored cyber attacks is complex, making attribution and proof particularly difficult.

While the article does not specifically focus on inequality, it does show how smaller businesses and investors from poorer countries are more vulnerable to cyber crimes. These groups often cannot afford strong cybersecurity protection or expensive lawyers. The article mentions that cryptocurrency investment fraud victims tend to be from developed countries while criminals operate from offshore locations. This means that when smaller businesses face cyber attacks, they have fewer options for getting justice.

The research helps society by pointing out these serious problems and suggesting practical solutions. The author recommends adding cybersecurity rules to international business treaties, requiring companies to report cyber attacks, and encouraging cyber insurance. These changes could help protect businesses and make the global economy more stable. Including cyber insurance requirements for high risk investments would help balance financial risk and make dealing with cyber incidents more about compensation than long legal battles.

In conclusion, this article does an excellent job explaining the complex challenges that cybercrime creates for international business. It shows that our current legal systems, designed before the digital age, are struggling to handle these new threats. The author's suggestions for updated laws and better international cooperation represent important steps forward. This research provides valuable information for anyone involved in or studying international business in our increasingly digital world.

Works Cited

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