VOLUME 6 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

TRADE SECRETS AND CROSS-BORDER CYBER-ESPIONAGE: EVALUATING THE EFFECTIVENESS OF INTERNATIONAL LEGAL NORMS

- Manas Balayan[*]& Dr. Shireen Singh[*]

Abstract

Cross-border cyber-espionage targeting trade secrets is not an isolated phenomenon of opportunistic hacking, but rather a structural challenge reflecting fundamental tensions between national security imperatives, economic competitiveness, and inadequate international legal frameworks governing state-sponsored intellectual property theft in cyberspace. This paper provides a critical legal examination of how international norms including the TRIPS Agreement, WTO dispute settlement mechanisms, customary international law principles, and emerging cyber norms address or fail to address systematic trade secret misappropriation through digital means. Through doctrinal analysis of international treaties, state practice, and cyber incident case studies, this research argues that normative ambiguity operates as both a reflection of states' reluctance to constrain their own cyber-espionage capabilities and a structural enabler of economic espionage costing global businesses hundreds of billions annually. The lived realities of this normative vacuum include state-sponsored advanced persistent threat groups infiltrating corporate networks, industrial espionage campaigns targeting strategic sectors, and regulatory arbitrage where perpetrators exploit jurisdictional gaps and attribution difficulties inherent in cyberspace's architecture. The paper provides intensive discussion of enforcement mechanisms including WTO dispute settlement, domestic frameworks, and diplomatic responses, evaluating whether these mechanisms function as genuine deterrents or merely symbolic gestures perpetuating impunity for cyber-enabled economic espionage. Ultimately, recommendations emphasize constructing effective international frameworks through treaty development establishing cyber-espionage norms, attribution standards, state responsibility principles, and

[*]Student at Amity Law School, Noida, Amity University Uttar Pradesh
[*]Assistant Professor at Amity Law School, Noida

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com
https://www.ijalr.in/

multilateral cooperation mechanisms balancing trade secret protection with legitimate intelligence activities.

Keywords:*Trade secrets; cyber-espionage; international law; TRIPS Agreement; state responsibility; attribution; intellectual property; cybersecurity; economic espionage.*

INTRODUCTION: TRADE SECRETS IN THE CYBER AGE

Trade secrets constitute critical intellectual property assets for modern enterprises, encompassing confidential business information including technical data, manufacturing processes, research findings, and strategic plans providing competitive advantages when kept secret.[1] Unlike patents or trademarks requiring public registration, trade secrets derive value precisely from confidentiality, creating unique protection challenges when information exists in digital formats vulnerable to cyber-intrusion.[2]

The global digital transformation has fundamentally altered trade secret protection dynamics. Information previously requiring physical infiltration can now be exfiltrated remotely through sophisticated cyber-attacks penetrating corporate networks or exploiting software vulnerabilities. Advanced persistent threat groups, often state-sponsored, conduct sustained campaigns targeting specific industries with strategic economic value, combining technical sophistication with geopolitical motivations distinguishing them from common cybercrime.

International legal frameworks governing trade secret protection and cyber-espionage remain fragmented and inadequate. The TRIPS Agreement establishes minimum protection standards but provides limited enforcement mechanisms and does not specifically address cyber-enabled misappropriation or state-sponsored espionage. Customary international law principles including sovereignty and non-intervention require interpretation for cyberspace application, with ongoing debates about whether cyber-espionage constitutes internationally wrongful acts.

The regulatory vacuum creates multiple pathologies. Attribution difficulties enable perpetrators to operate with effective impunity, exploiting technical challenges linking cyber-attacks to specific actors.[3] Jurisdictional fragmentation allows espionage operations spanning multiple countries to evade coherent legal responses. Enforcement deficits plague international frameworks lacking mechanisms to compel compliance or impose meaningful

[1]World Intellectual Property Organization, *Understanding Industrial Property* 67–72 (2016).
[2]*Uniform Trade Secrets Act* § 1(4) (Unif. Law Comm'n 1985).
[3] Thomas Rid & Ben Buchanan, "Attributing Cyber Attacks," 38 *Journal of Strategic Studies* 4, 8–12 (2015).

consequences on state actors engaging in economic espionage.[4] Normative ambiguity regarding distinctions between legitimate intelligence gathering and prohibited economic espionage enables states to pursue aggressive campaigns while maintaining plausible deniability.

This research evaluates whether existing international legal norms adequately address cross-border cyber-espionage targeting trade secrets, analyzing treaty frameworks, customary law principles, and enforcement mechanisms. The paper argues that normative development has lagged behind technological realities, creating governance gaps requiring systematic reform to protect innovation and international economic relations.

INTERNATIONAL LEGAL FRAMEWORK FOR TRADE SECRET PROTECTION

TRIPS Agreement and WTO Framework

The Agreement on Trade-Related Aspects of Intellectual Property Rights represents the primary international instrument establishing trade secret protection obligations. Article 39 requires WTO members to protect undisclosed information against disclosure or acquisition through means contrary to honest commercial practices, defining protected information as secret, commercially valuable, and subject to reasonable secrecy measures. This framework establishes baseline standards but leaves substantial implementation discretion to member states regarding specific protection mechanisms and enforcement procedures.

TRIPS Article 39 emerged from negotiations balancing developed countries' interests in strong intellectual property protection against developing countries' concerns about technology transfer barriers.[5] The compromise language requires protection against improper acquisition but does not mandate specific criminal penalties or damages frameworks, creating implementation variations that sophisticated actors exploit through regulatory arbitrage.

Enforcement mechanisms under TRIPS operate primarily through WTO dispute settlement enabling member states to challenge compliance with treaty obligations.[6] However, dispute settlement faces multiple limitations addressing cyber-espionage. Cases require state-to-state initiation, creating political barriers when governments hesitate to publicly accuse trading partners of espionage. Remedies are prospective, requiring violating states to achieve compliance without providing compensation for past harms. Attribution challenges

[4] Nicholas Tsagourias & Russell Buchan, *Research Handbook on International Law and Cyberspace* 234–39 (2015).
[5] Daniel Gervais, *The TRIPS Agreement: Drafting History and Analysis* 345–52 (4th ed. 2012).
[6] Dispute Settlement Understanding, arts. 3–7, Apr. 15, 1994, 1869 U.N.T.S. 401.

complicate establishing that states failed TRIPS obligations when espionage occurs through non-state actors or cannot be definitively linked to government involvement.

No WTO dispute has directly addressed state-sponsored cyber-espionage targeting trade secrets, reflecting political sensitivities and normative uncertainties about whether TRIPS obligations extend to preventing state intelligence agencies from conducting economic espionage.[7] This jurisprudential vacuum leaves critical questions unresolved regarding international obligations to prevent or remedy cyber-enabled trade secret theft.

Bilateral and Regional Agreements

Bilateral investment treaties and free trade agreements increasingly include intellectual property chapters establishing trade secret protection obligations exceeding TRIPS minimum standards. These agreements often require criminal penalties for misappropriation, specific remedies including injunctions, and enhanced enforcement mechanisms.[8]

Investment arbitration under bilateral treaties provides potential remedies when states expropriate foreign investors' trade secrets. However, successfully invoking investment protection faces multiple challenges. Establishing that cyber-espionage constitutes expropriation requires demonstrating state involvement and substantial investment value deprivation. Attribution difficulties proving state responsibility, even when national champions benefit, complicate causation analysis. Calculating damages for misappropriated secrets whose value derives from destroyed secrecy presents valuation challenges.[9]

Notable investment arbitration cases addressing intellectual property have involved physical seizures or regulatory measures rather than cyber-espionage, leaving precedential gaps regarding cyberspace-specific issues. The reluctance of arbitral tribunals to address intelligence activities traditionally considered sovereign prerogatives further limits investment arbitration's effectiveness.

CUSTOMARY INTERNATIONAL LAW AND CYBER-ESPIONAGE NORMS

[7] WTO Dispute Settlement Database (2023).
[8] Id. art. 20.70.
[9] Borzu Sabahi, *Compensation and Restitution in Investor-State Arbitration* 167–73 (2011).

Sovereignty and Non-Intervention Principles

Customary international law principles including territorial sovereignty and non-intervention potentially constrain cyber-espionage but face interpretive challenges regarding intelligence activities. The principle of sovereignty prohibits states from exercising authority on foreign territory without consent, yet cyber operations occur through cross-border data transmissions raising questions about whether information flows constitute territorial intrusions.[10]

The Tallinn Manual, an influential scholarly assessment of international law's cyberspace application, concludes that cyber-espionage not causing physical damage generally does not violate sovereignty principles, though minority positions argue any unauthorized cyber intrusion breaches territorial integrity.[11] This normative uncertainty reflects states' reluctance to establish clear rules potentially constraining their own intelligence capabilities.

Non-intervention principles prohibit states from coercively interfering in other states' internal affairs.[12] However, applying non-intervention to cyber-espionage requires determining whether information theft constitutes coercive interference. State practice demonstrates widespread intelligence collection targeting foreign governments and businesses without generating consistent claims of international law violations, suggesting limited customary prohibition of espionage activities.[13]

State Responsibility for Non-State Actor Conduct

International law holds states responsible for internationally wrongful acts committed by state organs or individuals exercising governmental authority.[14] However, attributing cyber-espionage to states faces technical and legal challenges. Technical attribution requires linking malicious activities to specific actors through forensic analysis often deliberately obscured through sophisticated tradecraft.

Legal attribution determining state responsibility involves assessing whether cyber actors constitute state organs, operate under state direction, or receive state acknowledgment of their conduct. Advanced persistent threat groups may receive state funding or protection while

[10] Schmitt, *supra* note 10, at 16–21.

[11] Id. at 169–71.

[12] *Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.)*, 1986 I.C.J. 14, ¶ 205 (June 27).

[13] Simon Chesterman, "The Spy Who Came in from the Cold War," 27 *Michigan Journal of International Law* 1071, 1089–94 (2006).

[14] International Law Commission, *supra* note 6, arts. 4–8.

maintaining plausible deniability through ostensibly private structures.[15] Determining when states bear responsibility for non-state actors' cyber-espionage requires fact-intensive analysis often frustrated by limited public evidence.

Due diligence obligations potentially require states to prevent their territory from being used for internationally wrongful acts, though controversy persists regarding whether this extends to cyber-espionage. If states must prevent non-state actors from conducting trade secret theft from their territory, substantial enforcement obligations could arise. However, state practice does not demonstrate consistent compliance with such duties regarding economic espionage.

ENFORCEMENT CHALLENGES AND ATTRIBUTION PROBLEMS

Technical Attribution Difficulties

Attributing cyber-espionage operations to specific actors requires sophisticated technical analysis correlating malware characteristics, infrastructure, operational patterns, and targeting choices often deliberately obscured. False flag operations plant indicators suggesting different perpetrators, creating misattribution risks. Proxy operations route attacks through compromised systems in third countries, concealing actual origin and complicating legal responsibility determination.[16]

Private sector cybersecurity firms conduct attribution analysis based on proprietary intelligence, creating transparency challenges when governments rely on confidential methodologies. Different analytical standards produce conflicting attributions, with some firms requiring high confidence while others publicize preliminary assessments. This analytical fragmentation undermines legal processes requiring reliable attribution evidence meeting evidentiary standards for state responsibility.

Evidentiary Standards and Intelligence Sensitivities

Legal proceedings addressing cyber-espionage face tension between evidentiary requirements and intelligence sensitivities. Criminal prosecutions require proof beyond reasonable doubt, presenting challenges when attribution depends on classified intelligence sources that

[15] U.S. Department of Justice, *Chinese Military Personnel Charged with Computer Fraud* (May 19, 2014).
[16] Jason Healey, *Beyond Attribution* 8–12 (Atlantic Council 2012).

disclosure would compromise.[17] Governments may prioritize operational security over prosecution, declining cases requiring sensitive evidence disclosure.

Investment arbitration and WTO dispute settlement employ lower evidentiary standards but still require substantial proof linking conduct to respondent states. Attribution evidence often derives from signals intelligence or technical collection capabilities that states resist revealing publicly. Victims lack access to government intelligence, creating information asymmetries disadvantaging private parties pursuing remedies.[18]

Public attribution by governments declaring specific actors responsible provides political responses but faces credibility challenges without supporting evidence disclosure. The United States and European Union have publicly attributed major cyber-espionage campaigns to specific countries, yet attributions' legal significance remains uncertain absent follow-through with formal accountability mechanisms.[19]

Jurisdictional Gaps and Enforcement Limitations

Even when attribution succeeds, jurisdictional limitations frustrate enforcement. Criminal jurisdiction requires either territorial presence of perpetrators or effects within prosecuting states. Cyber-espionage operators typically remain in home jurisdictions declining extradition, particularly when state-sponsored. Prosecuting in absentia produces symbolic victories without practical accountability.[20]

Civil remedies face similar jurisdictional challenges plus difficulties enforcing judgments against foreign defendants claiming sovereign immunity. Victims obtaining favorable judgments against perpetrators in non-cooperative jurisdictions rarely collect damages, undermining deterrent effects. Asset seizure mechanisms developed for money laundering have limited application to trade secret theft not generating traceable financial flows.[21]

Mutual legal assistance treaties facilitate cross-border evidence gathering but operate slowly through diplomatic channels requiring cooperation from states that may protect perpetrators serving national interests. Requests implicating intelligence activities often receive non-responses providing insufficient evidence for legal proceedings.

[17] U.S. Department of Justice, *Best Practices for Victim Response* 34–38 (2015).
[18] Dolzer&Schreuer, *supra* note 21, at 278–83.
[19] U.S. Department of Justice, *Seven International Cyber Defendants Charged* (Sept. 16, 2020).
[20] Id. § 432.
[21] Financial Action Task Force, *Virtual Assets: Red Flag Indicators* 34–39 (2020).

EMERGING NORMS AND REFORM PROPOSALS

United Nations Processes

The UN has convened multiple processes developing norms for responsible state behavior in cyberspace. The Group of Governmental Experts produced consensus reports affirming that international law applies to cyberspace and identifying voluntary norms including refraining from allowing territory to be used for internationally wrongful cyber acts. However, the process stalled over disagreements about whether existing international law adequately addresses cyber operations.

The Open-Ended Working Group established broader participation, producing a 2021 report endorsing previous recommendations while identifying areas requiring normative development. Neither process specifically addressed cyber-espionage targeting trade secrets, focusing instead on critical infrastructure protection and confidence-building measures.

Bilateral Agreements and Regional Initiatives

The United States has pursued bilateral agreements addressing cyber-espionage, notably the 2015 U.S.-China agreement where both countries committed to refrain from cyber-enabled intellectual property theft for commercial advantage. While initial compliance appeared positive, subsequent analyses documented continued Chinese operations, raising questions about agreement effectiveness.

The European Union has developed frameworks for cyber sanctions targeting individuals responsible for cyber-attacks including economic espionage. These measures impose travel bans and asset freezes but face effectiveness limitations when targets lack EU assets. The EU promotes binding cyber norms through diplomatic initiatives with like-minded countries.

Proposals for Treaty Development

Scholars have proposed comprehensive treaties establishing substantive prohibitions, enforcement mechanisms, and dispute resolution for cyber operations including economic espionage. Proposed elements include substantive prohibitions distinguishing legitimate intelligence from prohibited economic espionage based on beneficiary distinctions, with theft

benefiting private commercial entities prohibited while governmental intelligence potentially permissible.[22]

Attribution protocols establishing standards for determining responsibility could include independent investigative bodies, evidence sharing requirements, and burden-shifting rules addressing attribution uncertainties. Creating credible attribution mechanisms requires balancing transparency with intelligence protection.

Enforcement mechanisms ranging from WTO-style dispute settlement to international courts adjudicating state responsibility with compensatory remedies could provide accountability. Countermeasure frameworks authorizing proportionate responses including sanctions or defensive cyber operations, with procedural safeguards preventing escalation, could deter violations.

FINDINGS AND RECOMMENDATIONS

Critical Findings

Several findings emerge from this analysis of international legal norms addressing cross-border cyber-espionage targeting trade secrets. First, existing frameworks including TRIPS, customary international law, and bilateral agreements provide fragmented and inadequate protection European Commission, EU Cybersecurity Strategy 8–12 (2020). state-sponsored economic espionage. Normative gaps, enforcement deficits, and political obstacles prevent systematic accountability.

Second, technical attribution challenges and legal evidentiary standards create structural barriers to establishing state responsibility even when substantial circumstantial evidence suggests government involvement. Intelligence sensitivities prevent disclosure of definitive attribution evidence, creating information asymmetries defendants exploit.

Third, the distinction between legitimate intelligence gathering and prohibited economic espionage remains contested, reflecting states' reluctance to constrain their own capabilities through clear frameworks. Without consensus regarding definitional issues, developing effective enforcement mechanisms proves extraordinarily difficult.

Fourth, enforcement mechanisms including WTO dispute settlement, investment arbitration, and criminal prosecution face jurisdictional, procedural, and remedial limitations preventing

[22] Schmitt, *supra* note 10, at 173–76.

effective deterrence.[23] The combination of attribution difficulties and remedy enforcement challenges creates effective impunity for sophisticated state-sponsored actors.

Normative and Institutional Recommendations

Addressing cyber-espionage targeting trade secrets requires comprehensive reforms spanning treaty development and institutional capacity building. Treaty development should establish clear substantive prohibitions distinguishing permissible intelligence activities from prohibited economic espionage based on beneficiary analysis.[24] States should prevent cyber-enabled theft benefiting commercial entities while potentially permitting government intelligence collection for legitimate security purposes.

Attribution standards and evidentiary protocols should balance technical realities with legal requirements through graduated frameworks.[25] High-confidence technical attribution combined with circumstantial evidence of state involvement could establish presumptive responsibility, shifting burdens to accused states. Independent technical investigation capabilities through international organizations could provide credible attribution reducing reliance on national intelligence claims.

State responsibility principles should explicitly address cyber contexts, clarifying when states bear responsibility for non-state actor conduct including private companies or criminal organizations operating from their territory with government knowledge or support.[26] Due diligence obligations requiring reasonable measures to prevent cyber-espionage could establish baseline standards.

Enforcement mechanisms should combine diplomatic, economic, and legal tools creating meaningful consequences. Strengthened WTO dispute settlement could include remedies beyond compliance including compensatory trade concessions. Countermeasure frameworks should authorize proportionate responses with procedural safeguards preventing escalation while maintaining deterrent credibility.[27]

Institutional capacity building through WIPO, WTO, or specialized cyber organizations could provide technical expertise and dispute resolution forums addressing cyber-specific

[23] Shackelford, *supra* note 8, at 267–73.
[24] Schmitt, *supra* note 10, at 176–79.
[25] Healey, *supra* note 35, at 18–23.
[26] International Law Commission, *supra* note 6, commentary to art. 8.
[27] International Law Commission, *supra* note 6, arts. 49–54.

challenges.[28] Public-private partnerships leveraging private sector technical expertise while maintaining governmental enforcement authority could enhance collective defense.

CONCLUSION

Cross-border cyber-espionage targeting trade secrets represents a fundamental challenge to international economic order and innovation incentives. The systematic theft of confidential business information costs global businesses hundreds of billions annually while undermining legal frameworks premised on protecting intellectual property rights.

Existing international legal norms provide inadequate responses. The TRIPS Agreement establishes baseline protection obligations but lacks enforcement mechanisms addressing state-sponsored espionage. Customary international law's application remains contested, with fundamental disagreements about whether intelligence activities violate sovereignty principles. Bilateral agreements produce limited compliance absent credible enforcement, while dispute settlement faces attribution and remedial limitations.

The normative vacuum reflects fundamental political resistance to constraining states' intelligence capabilities through international obligations. Governments conduct and benefit from cyber-espionage while condemning foreign operations, creating hypocrisy frustrating norm development. Attribution challenges and intelligence sensitivities provide convenient justifications for inaction, enabling sophisticated actors to operate with effective impunity.

Effective reform requires confronting these political obstacles through graduated frameworks balancing legitimate intelligence activities with economic espionage prohibitions, establishing attribution standards suited to cyber contexts, clarifying state responsibility for non-state actor conduct, and building institutional capacity for investigation and adjudication.

The analysis demonstrates that technological capabilities have outpaced normative development, creating governance deficits requiring systematic multilateral cooperation. Trade secret protection in the cyber age demands international consensus regarding acceptable state behavior, credible enforcement mechanisms, and institutional capacity managing cyberspace's technical and jurisdictional complexities.

Ultimately, protecting innovation and international economic relations from destabilizing cyber-espionage campaigns represents a collective challenge requiring collective responses. Only through strengthened international legal frameworks establishing clear norms, credible

[28] Shackelford, *supra* note 8, at 312–18.

attribution mechanisms, and effective enforcement can the international community prevent cyber-espionage from fundamentally undermining the intellectual property regime that innovation economies depend upon.