elita.uz

№ 1 (4) 2026

THE CHALLENGE OF 'HARVEST NOW, DECRYPT LATER' (HNDL) TO THE INTERNATIONAL LAW OF STATE RESPONSIBILITY IN THE QUANTUM ERA

Islombek Abdikhakimov

islombekabduhakimov@gmail.com

Head of Artificial Intelligence and Legal Tech Laboratory,
Tashkent State University of Law

Abstract. The emergence of Cryptographically Relevant Quantum Computers (CRQCs) presents a profound challenge to the temporal and material thresholds of international law, specifically through the strategic practice known as "Harvest Now, Decrypt Later" (HNDL). This adversarial model, wherein state and non-state actors exfiltrate encrypted data with the intent of decrypting it once quantum capabilities mature, creates a legal grey zone that defies the traditional application of the International Law Commission's Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA). This article investigates the compatibility of ARSIWA's doctrines of attribution and breach with the delayed-impact nature of HNDL. Through a doctrinal legal analysis of recent scholarship and technical forecasts regarding Post-Quantum Cryptography (PQC), this study identifies a critical "attributional twilight" and a disconnect between the moment of data interception and the realization of injury. The results indicate that current legal frameworks treat HNDL largely as espionage—a practice often tolerated in international relations—thereby failing to account for the catastrophic, long-tail damage of retrospective decryption. The article concludes that the principle of due diligence must be radically reinterpreted to include a "crypto-agility mandate," obligating states to preemptively transition critical infrastructure to quantum-safe standards to fulfill their international responsibilities.

Kalit so‘zlar: Harvest Now Decrypt Later, HNDL, State Responsibility, Quantum Computing, ARSIWA, Due Diligence, Crypto-Agility, International Law, Cyber Attribution.

Introduction

The trajectory of quantum computing technology has shifted from theoretical physics to a tangible strategic imperative for national security and global finance. While the operational deployment of fault-tolerant quantum computers capable of breaking current encryption standards remains on the technological horizon, the threat they pose is immediate due to the "Harvest Now, Decrypt Later" (HNDL) strategy. Under this model, adversaries systematically collect encrypted data—ranging from government archives and military secrets to sensitive intellectual property—anticipating that future CRQCs will possess the computational power to break current public-key cryptographic schemes such as RSA and Elliptic Curve Cryptography (ECC) (Erol, 2025). This phenomenon fundamentally alters the temporal dynamics of cyber espionage and data theft, transforming a future technological capability into a present-day national security crisis (Jena, 2025).

The prevailing framework for addressing illicit state behavior in cyberspace is grounded in the law of state responsibility, primarily codified in the International Law Commission’s *Articles on Responsibility of States for Internationally Wrongful Acts* (ARSIWA). Under ARSIWA, state responsibility arises when conduct consisting of an action or omission is attributable to the state and constitutes a breach of an international obligation (Kastelic, 2019). However, the application of these principles to HNDL operations is fraught with doctrinal ambiguity. Traditional international law has struggled to regulate cyber operations that fall below the threshold of the use of force or armed attack, a category into which most data exfiltration campaigns fall (Payne, 2016).

The unique challenge of HNDL lies in its composite and temporally distributed nature. The initial act of interception may be legally ambiguous or technically unattributable at the time of occurrence, while the material injury—the decryption and exposure of sensitive information—occurs years or decades later. This temporal decoupling pressures the static definitions of "breach" and "injury"

within the law of state responsibility. It necessitates a rigorous re-examination of how international legal obligations apply to the long-term retention and future exploitation of encrypted data (Zafar, 2025).

Furthermore, the threat landscape is complicated by the inherent difficulties of attribution in the cyber domain. Legal attribution requires a high standard of proof to impute conduct to a state, often necessitating evidence of effective control over non-state actors or direct instruction by state organs (Chen et al., 2025). In the context of HNDL, the evidence of the initial intrusion may be degraded or lost by the time the data is decrypted and used, making it difficult for the injured state to satisfy the evidentiary burden required to invoke state responsibility.

The highly anonymized nature of cyber operations, characterized by the use of proxies and obfuscation techniques, further complicates the establishment of a causal link between the state and the harvesting operation. As highlighted by recent scholarship, the technical complexity of these operations means that even if the "harvesting" is detected, attributing it to a specific state actor with the legal certainty required for countermeasures is often unfeasible (Chen et al., 2025). This attributional void invites states to engage in HNDL operations with a perception of impunity.

The "Harvest Now, Decrypt Later" threat model is not merely a theoretical risk but a concrete danger to national security, financial systems, and sensitive data stored today (Erol, 2025). Adversaries are actively targeting long-lived data, such as medical records, legal documents, and state secrets, which retain their sensitivity for decades. This reality highlights the urgency of the transition to post-quantum cryptography (PQC) and the implementation of crypto-agility strategies (Jena, 2025).

If international law fails to adapt to this new temporal reality, it risks obsolescence in the face of quantum advancements. The current legal silence on the status of encrypted data effectively incentivizes the stockpiling of information, creating a destabilizing arms race in the digital domain. This article posits that existing principles, particularly due diligence, must be stretched to cover the pre-decryption phase of HNDL attacks to maintain the rule of law in cyberspace.

Methodology

This article employs a qualitative doctrinal legal analysis to evaluate the compatibility of existing international legal frameworks with the emerging threat of HNDL. The primary legal text under analysis is the International Law Commission's *Articles on Responsibility of States for Internationally Wrongful Acts* (2001). Specifically, the study scrutinizes the provisions regarding attribution (Articles 4–11), the breach of an international obligation (Articles 12–15), and the content of international responsibility. This legal analysis is synthesized with a review of technical literature on quantum readiness and post-quantum cryptography to ground the legal arguments in technological reality.

The review encompasses peer-reviewed literature and grey literature, including technical reports on the timeline for CRQC development and the standardization of post-quantum algorithms. Key sources include reports on the National Institute of Standards and Technology (NIST) PQC standardization project and academic articles addressing the legal and regulatory aspects of quantum computing (Erol, 2025; Zafar, 2025). The selection of sources was guided by their relevance to the intersection of international law, cybersecurity, and quantum technology.

The study further integrates recent scholarship on the applicability of international law to cyber operations, drawing on the analysis of state practice and *opinio juris* regarding cyber attribution and due diligence obligations. This includes an examination of the "effective control" standard and the evidentiary challenges associated with attributing cyber operations to states (Chen et al., 2025). The analysis also considers the "rational choice theory" of compliance, which posits that states violate international law when the benefits of non-compliance outweigh the costs (Kastelic, 2019).

To ensure a comprehensive understanding of the HNDL threat, the methodology incorporates an interdisciplinary approach. It fuses doctrinal legal reasoning with insights from cryptographic science and financial systems analysis (Zafar, 2025). This approach allows for a nuanced assessment of the risks posed by quantum computing and the effectiveness of potential legal and regulatory responses.

The analysis is structured to identify specific gaps in the current legal framework. By contrasting the technical realities of HNDL with the static

requirements of ARSIWA, the study highlights areas where legal interpretation must evolve. This includes re-evaluating the temporal moment of breach and the scope of due diligence obligations in the context of long-term data security (Ollino, 2016).

Furthermore, the methodology examines the concept of "crypto-agility" not just as a technical specification but as a potential legal standard of care. By reviewing the "Crypto-Agility Mandate" proposed in recent computer science literature (Jena, 2025), the study assesses whether this technical requirement can be transposed into a binding obligation under the international law of state responsibility.

Limitations of this study include the speculative nature of the exact timeline for the arrival of fault-tolerant quantum computers. While the HNDL threat is current, the materialization of the injury depends on future technological breakthroughs (Mavroeidis et al., 2018). Consequently, the legal analysis relies on the assumption that CRQCs will eventually become operational, a consensus view held by the majority of the scientific community cited in the reviewed literature.

Results

The analysis reveals that the HNDL threat model fundamentally disrupts the attribution frameworks of state responsibility. The primary obstacle identified is the legal characterization of the "harvesting" phase. While the eventual decryption of data by a quantum computer constitutes the realization of the threat, the initial act of data collection is often classified as cyber espionage. Contemporary legal scholarship indicates that cyber espionage is generally tolerated as a practice of statecraft, although it may breach sovereignty if it involves unauthorized intrusion into cyber infrastructure located within another state’s territory (Payne, 2016).

However, the HNDL strategy changes the nature of the injury associated with this intrusion. Unlike traditional espionage, where the intelligence value is immediate, HNDL targets "long-lived" data that retains its sensitivity for decades (Jena, 2025). Consequently, the injury to the victim state is latent, materializing only when the adversary achieves quantum advantage. This temporal lag complicates the establishment of an "internationally wrongful act" under ARSIWA, as the breach and the injury are separated by a significant period.

The results also indicate that the temporal gap between harvest and decryption creates significant hurdles for the doctrine of attribution. Legal attribution under ARSIWA requires a high standard of proof to impute conduct to a state. In the context of HNDL, the evidence of the initial intrusion may be degraded or lost by the time the data is decrypted, making it difficult for the injured state to satisfy the evidentiary burden required to invoke state responsibility (Chen et al., 2025).

Moreover, the highly anonymized nature of cyber operations complicates the establishment of a causal link between the state and the harvesting operation. The use of proxies and obfuscation techniques means that even if the "harvesting" is detected, attributing it to a specific state actor with the legal certainty required for countermeasures is often unfeasible (Chen et al., 2025). This difficulty is exacerbated by the involvement of non-state actors, whose actions are only attributable to the state if they act on its instructions or under its direction or control (Payne, 2016).

The study finds that the emerging standardization of Post-Quantum Cryptography (PQC) is creating new normative expectations for state behavior. The NIST standardization project has established a global benchmark for quantum resilience (Erol, 2025). This technical evolution suggests that the failure to transition to quantum-safe standards could increasingly be viewed as a failure of due diligence (Geremew & Mohammad, 2024).

While international law does not currently mandate specific cryptographic standards, the principle of due diligence obliges states to prevent their territory from being used for acts contrary to the rights of other states (Kastelic, 2019). The literature suggests that as PQC becomes the industry standard, the continued reliance on vulnerable encryption methods by critical infrastructure operators could be construed as a violation of international obligations regarding the protection of data integrity and privacy.

Furthermore, the results highlight the financial and systemic risks associated with HNDL. The failure to act pre-emptively may expose financial infrastructures to retrospective data breaches, regulatory incoherence, and cascading market instability (Zafar, 2025). This underscores the need for

anticipatory regulation that embeds enforceable standards and strategic collaboration across public and private stakeholders.

The analysis confirms that the "Harvest Now, Decrypt Later" strategy exploits the structural weaknesses of the current international legal regime. The difficulty of attributing the initial harvesting operation, combined with the delayed manifestation of harm, insulates perpetrators from immediate accountability. This creates a permissive environment for states to engage in data exfiltration with relative impunity, undermining the stability of the international order (Kastelic, 2019).

Additionally, the research indicates that HNDL challenges the traditional distinction between "peace" and "conflict" in cyberspace. The pre-positioning of decrypted intelligence for future strategic advantage creates a state of perpetual "grey zone" conflict (Harkavy, 2025). This constant low-level hostility erodes mutual trust and complicates diplomatic efforts to establish norms of responsible state behavior in cyberspace.

Finally, the results suggest that existing data protection frameworks, while robust for current threats, may be inadequate for the HNDL scenario without specific amendments addressing long-term encryption validity. The "state of the art" requirement in data protection laws is dynamic, and the advent of quantum computing is rapidly redefining what constitutes adequate security measures (Zafar, 2025).

Discussion

The implications of HNDL for the law of state responsibility suggest that a static interpretation of ARSIWA is insufficient to address the quantum threat. A critical area for legal development is the interpretation of the temporal moment of the breach. Article 14 of ARSIWA addresses the "extension in time of the breach of an international obligation," distinguishing between instantaneous acts and continuing wrongful acts (Kastelic, 2019). HNDL could theoretically be framed as a composite act or a continuing breach, where the retention of illicitly acquired data constitutes an ongoing violation of sovereignty or privacy rights that culminates in decryption.

If the "harvesting" is viewed merely as the preparatory phase of a composite act that is only completed upon decryption, the statute of limitations and

the evidentiary requirements for attribution would shift. This interpretation would potentially allow states to invoke responsibility decades after the initial intrusion. However, this approach challenges the principle of legal certainty and raises complex questions about inter-temporal law—specifically, whether the legality of the decryption should be judged by the laws in force at the time of harvest or at the time of decryption.

The doctrine of due diligence offers the most viable pathway for addressing the responsibility gaps created by HNDL. The principle of due diligence in cyberspace requires states to take all reasonable measures to terminate unlawful cyber operations emanating from their territory (Kastelic, 2019). As the "harvest now" component of the threat relies on present-day vulnerabilities in classical cryptography, the standard of "reasonable measures" must evolve to include "crypto-agility"—the ability to rapidly switch to quantum-safe algorithms (Jena, 2025).

The failure of a state to implement PQC standards in its critical infrastructure, despite knowledge of the HNDL threat, could expose it to claims of non-diligent behavior. If such negligence facilitates the exfiltration of third-party data or allows domestic actors to launch HNDL attacks, the state could be held responsible. This "crypto-agility mandate" essentially reframes the obligation from a negative duty (refraining from espionage) to a positive duty (ensuring the quantum resilience of digital infrastructure to prevent future harm) (Jena, 2025).

Furthermore, the passive collection of data under HNDL challenges the "harm" requirement often associated with countermeasures. For a state to lawfully employ countermeasures, it must be an "injured state" affected by an internationally wrongful act (Kastelic, 2019). If the injury (decryption) has not yet occurred, the victim state may be precluded from taking proportional countermeasures to recover the stolen data or deter the adversary.

This creates a dangerous strategic imbalance where the aggressor accumulates potential power without facing immediate legal consequences. To restore the balance of rights and obligations, legal scholars and policymakers must consider whether the mere possession of vast troves of encrypted foreign data with the intent to decrypt constitutes a present injury to the "informational sovereignty"

of the victim state. Such a recognition would trigger the right to reparation or cessation (Kastelic, 2019).

The discussion also necessitates an analysis of whether computer data qualifies as a protected "object" under international law. Recent scholarship suggests that data is increasingly viewed as an object capable of being targeted or damaged, a definition that is crucial for establishing a violation of International Humanitarian Law or sovereignty in the context of cyber operations (Pomson, 2023). If harvested data is considered a protected object, the act of harvesting itself could be elevated from espionage to a violation of property rights or sovereignty.

The "rational choice theory" of compliance further elucidates the behavior of states regarding HNDL. States choose to disregard their international legal obligations and resort to unlawful cyber operations when the benefits of non-compliance outweigh the associated costs (Kastelic, 2019). HNDL operations offer high potential rewards—access to sensitive future intelligence—with currently low risks of attribution or retaliation.

To alter this calculus, the international community must increase the costs of HNDL operations. This could be achieved by strengthening the attribution capabilities of states and international organizations, thereby reducing the anonymity that facilitates these operations (Chen et al., 2025). Additionally, the widespread adoption of PQC would devalue the harvested data, making the "harvest" phase less strategically attractive.

Finally, the discussion underscores the importance of public-private partnerships in building quantum resilience. Financial institutions and other critical infrastructure operators must work closely with government regulators to implement quantum-safe standards (Zafar, 2025). This collaborative approach is essential for ensuring that the legal and technical responses to HNDL are coordinated and effective.

Conclusion

The "Harvest Now, Decrypt Later" strategy represents a profound challenge to the international law of state responsibility, exploiting the temporal fissures between the act of data theft and the realization of its strategic value. Current legal frameworks, predicated on kinetic thresholds and immediate injury, are ill-equipped to deter adversaries who operate on decadal timelines. The difficulty

of attributing the initial harvesting operation, combined with the delayed manifestation of harm, insulates perpetrators from immediate accountability under the ARSIWA regime (Chen et al., 2025).

To maintain the relevance of international law in the quantum era, the interpretation of due diligence must expand to encompass a positive obligation of quantum readiness. States must not only refrain from HNDL operations but also actively harden their digital infrastructure against them through the adoption of post-quantum cryptography (Jena, 2025). This evolution requires a shift from reactive legal measures to proactive regulatory frameworks that anticipate future technological capabilities.

The "crypto-agility mandate" emerges as a crucial component of this new legal landscape. By requiring organizations to adopt architectural strategies that allow for the rapid updating of cryptographic algorithms, states can mitigate the long-term risks of retroactive decryption (Jena, 2025). This proactive approach aligns with the broader goals of international law to maintain peace and security in the digital domain.

Ultimately, the true deadline for legal and technical migration is not when quantum computers arrive, but now (Jena, 2025). The data currently being harvested will be vulnerable to future decryption, meaning that the window for protecting sensitive information is closing. Legal scholars, policymakers, and technical experts must collaborate to close the gaps in the international legal framework and ensure that the transition to the quantum era is secure and orderly.

Without such an evolution in legal interpretation and technical implementation, the international community risks entering a period of strategic instability. The retroactive decryption of sensitive data could undermine the foundations of diplomatic trust and national security, creating new sources of conflict in an already volatile global environment (Zafar, 2025). The time to act is now, before the quantum threat becomes a quantum reality.

REFERENCES

Chen, H., Coco, A., Rotondo, A., & Ying, Y. (2025). *The Attribution of Cyber Operations to States in International Law*. Geneva Centre for Security Policy (GCSP).

Cohen, J. E., de Witte, B., & Purnhagen, K. (2016). Bridging the transatlantic divide? The United States, the European Union, and the protection of privacy across borders. *International Journal of Constitutional Law*, 14(1), 220–229.

Erol, V. (2025). The Strategic Imperative of Quantum Readiness: A Comprehensive Review of Post-Quantum Cryptography. *Preprints.org*.

Geremew, A., & Mohammad, A. (2024). Preparing Critical Infrastructure for Post-Quantum Cryptography: Strategies for Transitioning Ahead of Cryptanalytically Relevant Quantum Computing. *International Journal on Engineering, Science, and Technology*, 6(4), 338-365.

Harkavy, R. (2025). The quantum reckoning: law's next frontier. *International Comparative Legal Guides*.

Jang-Jaccard, J. (2025). Practical Challenges in Executing Shor's Algorithm on Existing Quantum Platforms. *arXiv*.

Jena, J. (2025). The Quantum Security Deadline: Building Crypto-Agility Against 'Harvest Now, Decrypt Later' Threats. *European Journal of Computer Science and Information Technology*, 13(52), 35-52.

Kastelic, A. (2019). *Inducing compliance with international law in cyberspace – State responsibility, countermeasures and the obligations of due diligence*. White Rose eTheses Online.

Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. *International Journal on Advanced Science, Engineering and Information Technology*, 8(3), 991-998.

Ollino, A. (2016). *Due Diligence Under International Law: Reappraising its Scope, Functions and Limits* (Doctoral dissertation). Università degli Studi di Milano-Bicocca.

Payne, T. (2016). Teaching Old Law New Tricks: Applying and Adapting State Responsibility to Cyber Operations. *Lewis & Clark Law Review*, 20(2), 683-715.

Pomson, O. (2023). 'Objects'? The Legal Status of Computer Data under International Humanitarian Law. *Journal of Conflict and Security Law*, 28(2).

Rajagopalan, R. P. (Ed.). (2022). *Future Warfare and Technology: Issues and Strategies*. Observer Research Foundation and Global Policy Journal.

Sharma, M., & Vedashree, R. (Eds.). (2022). *Gearing up for Digital ++*. Mastercard and Observer Research Foundation.

Zafar, A. (2025). Quantum Computing in Finance: Regulatory Readiness, Legal Gaps, and the Future of Secure Tech Innovation. *European Journal of Risk Regulation*, 1–20.