Journal of Legal Science
Volume 41 / First Issue- 2026

مجلة العلوم القانونية
المجلد 41 / العدد الاول – 2026

The Role of Technology in Determining Liability for Damages Caused by the Use of Peaceful Nuclear Energy

Wafa A. H. Izzat
Princess Nourah Bint Abdulrahman University,
Wiabuhuwaij@pnu.edu.sa

Received Date: 1/5/2026. Accepted Date: 2/6/ 2026. Publication Date: 25/6/2026.

This work is licensed under a Creative Commons Attribution 4.0 International License

Abstract

Modern nuclear projects rely on digital systems, dense sensor networks, and data sharing tools. These tools can help show what happens when nuclear damage is claimed. They can also shape how the law assigns responsibility for that damage. Many nuclear liability systems already place strict liability on the operator and limit who can be sued. Even so, technology still matters because it affects proof, causation, and later recourse claims. Technology also matters when damage crosses borders and when cyber events play a role. This research explains how modern technology changes the way responsibility is found for nuclear damage from peaceful use. It reviews key liability treaties, state responsibility rules, and national examples. It then links those rules to radiation mapping, remote sensing, digital logs, and forensic methods. It also addresses cyber attribution and AI use in safety and operations. The research ends with practical steps that can improve fairness, speed, and trust in nuclear damage decisions.

Keywords: Nuclear Liability; Civil Liability Conventions; Operator Strict Liability; Nuclear Damage; Causation

دور التكنولوجيا في تحديد المسؤولية عن الأضرار الناجمة عن الاستخدام السلمي للطاقة النووية

وفاء عزت ابوحويج*
جامعة الأميرة نورة بنت عبد الرحمن
Wiabuhuwaij@pnu.edu.sa

تاريخ الاستلام: 5/1/ 2026. تاريخ القبول: 2 / 2026/6. تاريخ النشر: 2026/6/25.

المستخلص

تعتمد المشاريع النووية الحديثة على التكنولوجيا الرقمية، وأدوات مشاركة البيانات، بحيث يمكن لهذه الأدوات أن تساعد في تحديد الحوادث وأسبابها عند المطالبة عن الأضرار النووية وتحديد المسؤولية المدنية عن هذه الأضرار، وتفرض العديد من الأنظمة على المشغل المسؤولية بشكل مطلق، وتضع قيوداً على الجهات التي يمكن مقاضاتها، هنا تلعب التكنولوجيا دوراً كبيرا في الإثبات والسببية ودعاوى المطالبة، وتظهر أهميتها فضلاً عن ذالك عندما تتجاوز الأضرار الحدود الوطنية. يوضح هذا المقال كيف تغير التكنولوجيا الحديثة طريقة تحديد المسؤولية عن الأضرار النووية الناجمة عن الاستخدامات السلمية للطاقة النووية، ويتعرّض لقواعد المسؤولية والمعاهدات الدولية وأساليب الأدلة، ويتناول تحديد المسؤولية السيبرانية واستخدام الذكاء الاصطناعي في السلامة والعمليات، لينتهي بخطوات عملية يمكن أن تعزز العدالة والسرعة والثقة في إصدار القرارات المتعلقة بالأضرار النووية.

الكلمات المفتاحية: المسؤولية النووية؛ اتفاقيات المسؤولية المدنية؛ المسؤولية المطلقة للمشغل؛ الأضرار النووية؛ السببية.

---

[*] أستاذ مساعد دكتور

1.0 Introduction

The peaceful use of nuclear energy can create large benefits, yet it also carries rare but high-harm risks. When harm occurs, the law must decide who pays and on what basis. Nuclear damage claims can involve long time gaps, complex science, and cross-border effects. These features make proof hard even when liability rules are strict. Modern technology changes that proof setting. It can track plant status, record operator actions, map dose patterns, and preserve key records. It can also create new risk paths, such as cyber events and software faults. These changes raise a core legal issue. The issue is how technology affects decisions on responsibility for nuclear damage from peaceful use.

Many legal systems treat nuclear damage in a special way. They often channel liability to a single party, usually the operator. They also use strict liability rules, set liability caps, and require financial security. These choices aim to speed payment and avoid long fault disputes. Even under strict liability, technology still matters. Claims still need proof of nuclear damage and a link to an incident. States also need proof to meet treaty duties on notice, help, and cross-border cooperation. These tasks now depend on digital tools and data flows.

1.1 Problem Addressed

Responsibility for nuclear damage is not only a question of who operated a plant. It is also a question of what can be proven and how quickly it can be proven. Nuclear liability treaties and national laws often reduce fault debates by channeling strict liability to the operator. Still, several disputes remain. A claimant must show harm and a causal link to a nuclear incident. A court or claims body must also decide what evidence is reliable.

Modern technology creates two linked problems. First, it changes the evidence base. Digital control systems, sensors, drones, and remote sensing can create strong proof. They can also create large, messy data sets that are hard to verify. Second, it changes the risk profile. Digitalization can raise new failure modes tied to software, updates, human-machine interfaces, and cyber threats. These changes can affect liability allocation and the ability to pursue recourse claims beyond the operator. They can also affect state responsibility analysis when cyber attribution is disputed. These pressures require an updated legal account of how responsibility is determined in practice.

1.2 Research Questions

This research answers a set of connected questions.

The first question asks how core nuclear liability rules assign responsibility for nuclear damage. This includes strict liability, channeling, caps, and financial security. This also includes how these rules differ across key treaty models and national approaches (Paris Convention, 1960; Vienna Convention, 1963; Convention on Supplementary Compensation for Nuclear Damage, 1997).

The second question asks how technology affects proof of nuclear damage and causation. This includes radiation mapping, mobile detection, drone systems, and remote sensing tools. It also includes how these tools support dose and contamination findings that are used in legal settings (Marques et al., 2021; Corbacho et al., 2024; UNSCEAR, 2013).

The third question asks how technology affects secondary responsibility decisions. These include recourse claims, supplier disputes, and fault findings tied to digital systems and software. These also include how cyber events change attribution and proof standards for state responsibility claims (Office for Nuclear Regulation, 2024; Brunner, 2025; International Law Commission, 2001a).

The fourth question asks what steps can improve fairness and trust. These steps focus on data governance, evidence preservation, transparency, and cross-border cooperation (NIST, 2022; Ismail & Ariffin, 2025; UNECE, 1991).

1.3 Study Purpose

The purpose of this study is to explain the role of modern technology in responsibility decisions for nuclear damage from peaceful use. The study focuses on how technology affects proof, process, and legal reasoning. It treats technology as more than a set of tools. It treats technology as a factor that can shift outcomes because it can change what can be known, what can be shown, and what can be challenged.

The study also aims to connect legal rules that are often discussed in isolation. Cyber law debates focus on attribution and evidence. These areas now overlap in real events. A modern nuclear incident can involve cross-border effects, digital evidence, and cyber concerns. The study's purpose is to offer one coherent account of that overlap and show how it affects responsibility decisions in practice.

1.4 Importance of the Study

This topic matters for several practical reasons. Nuclear harm can be high-cost and long-lasting. Victims need fast and fair payment systems. Operators need clear rules to price risk and secure insurance. States need stable cross-border rules to reduce conflict after an incident.

Radiation mapping can show where harm likely occurred. Digital logs can show which safety actions were taken. Remote sensing can help confirm patterns of dispersion and contamination. These tools can reduce guesswork and reduce false claims. These risks make evidence governance and preservation rules central to responsibility decisions. These issues are also tied to public legitimacy, since nuclear events often trigger public fear and political conflict. This makes the study important for legal design and for real dispute handling (WHO, 2013; Ismail & Ariffin, 2025).

1.5 Methodology

This study applies comparative and analytical methodologies alongside a doctrinal framework to evaluate transboundary nuclear liability, utilizing the Fukushima accident as a central case-based reference point for modern technical measurement and long-tail claims rather than as a narrow case note. While the doctrinal approach establishes international benchmarks via treaties and the International Law Commission (ILC) draft articles, the comparative method contrasts domestic legislative schemes across major nuclear states to expose regulatory gaps. Finally, the analytical method bridges these legal norms with data science, assessing how technical telemetry such as radiation mapping and drone data can satisfy strict cybersecurity and admissibility standards for digital evidence in international legal settings.

2.0 Nuclear Liability Frameworks and the Baseline Allocation of Responsibility

2.1 International Nuclear Liability Conventions

Most nuclear liability systems share a set of design features. Liability is often strict, meaning fault does not need to be proven. Liability is often channeled to the operator, meaning claims are directed to a single party. Liability is often limited in amount and time, and financial security is required. These choices aim to protect victims and stabilize the industry. They also aim to avoid long litigation against many actors after a large event (Paris Convention, 1960; Vienna Convention, 1963).

The Paris model applies in many European settings and is supported by a supplementary funding layer in the Brussels Supplementary Convention. The scheme reflects a policy choice that the operator should be the main liable party and that public funds may supplement compensation when needed (Paris Convention, 1960; Brussels Supplementary Convention, 1963). The Vienna model offers a parallel system with similar goals and was later updated through a protocol that expanded the concept of nuclear damage and increased the potential compensation scope (Vienna Convention, 1963; Vienna Convention, 1997).

The Convention on Supplementary Compensation aims to create a broader global approach. It supports national laws that follow key rules and adds an international supplementary fund structure. It also aims to reduce gaps across regions and support cross-border claims handling (Convention on Supplementary Compensation for Nuclear Damage, 1997).

These systems show an important starting point. Responsibility for nuclear damage is often not assigned by tracing every fault line. It is assigned by legal design, with the operator placed at the center. Technology does not remove that design. Instead, technology changes how the design works in practice. It affects which events are detected, how nuclear damage is defined in a claim, and how cross-border impacts are shown. It also affects whether recourse claims can later shift costs to suppliers or other actors under contract or product law.

2.2 National Approaches and the Ongoing Role of Proof

National systems often mirror treaty logic but can vary in key ways. Japan provides an important example because its compensation system after Fukushima relied on statutory rules and strong state involvement. Japan's Act on Compensation for Nuclear Damage sets a strict liability approach and links compensation to a system that can involve state support measures. The Act also supports dispute handling through a committee structure that can guide compensation practice (OECD NEA, 2020). Policy summaries of Japan's system show how the design aims to protect victims while keeping the system workable for the operator and the state (OECD NEA, 2012).

The United States uses the Price-Anderson Act model, which combines private insurance with an industry retrospective premium system and federal layers for certain settings. The system sets a structured approach to compensation and liability management for nuclear incidents.

Across these models, strict liability does not eliminate proof demands. Claimants still need to show that harm fits within the legal definition of nuclear damage. They also need to show a link to an incident or to exposure tied to a nuclear installation. Technology affects

2.3 Strict Liability and Channeling Principles

The two basic principles of allocation, which are incorporated into nuclear liability regimes and in the legal channels of responsibility following a nuclear accident, are strict liability and channeling. By pre-establishing liability to the operator regardless of fault, these institutional arrangements remove evidentiary burdens (no need to establish liability through an inquiry into whether the event was due to negligence), expedite claims, and provide speedy compensation. They are characteristic of the structure of international nuclear liability conventions and also reflect an attitude on the part of the national policy to administrative simplicity and predictability. OECD NEA (2015) points out that the motivation for such arrangements is when compensation for the victims is justified in the context of the financial security of the nuclear industry. They're concurrently reflective of the general international law rationale (International Law Commission 2001a). However, with the development of technologically advanced systems, that very justification is vulnerable. Even though the central liability system remains directed towards the operator, digital control and monitoring technologies will impact the evidentiary powers of responsibility attribution, as will be automated information-gathering procedures, across the operational system. Doctrinally sound but technologically challenging, strict liability and channeling are the two doctrines.

3.0 Technology and the Detection of Nuclear Damage

3.1 Radiation Detection and Monitoring Technologies

Modern measurement tools can improve the ability to detect contamination and dose patterns. These tools include fixed sensors, mobile detection systems, drone-based detectors, and lab methods. They also include modeling that links source terms to dispersion and exposure. These methods can help identify where harm likely occurred and can support decisions on compensation scope.

Mobile radiation detection systems are now a major part of modern response and monitoring. A state-of-the-art review describes how mobile systems support location, identification, and mapping tasks. The review also explains how system limits, shielding, and calibration affect accuracy. These points matter in legal settings because a claimant's proof may depend on the reliability of mapping results (Marques et al., 2021).

3.2 Drone-Based Measurement Systems

Drone-based measurements are also growing. A study on a drone-based gamma-ray spectrometry system explains how airborne measurement can support accurate quantification and mapping. This can be critical when ground access is limited or risky. It can also support more complete coverage in large areas with uneven contamination (Corbacho et al., 2024).

These tools matter for responsibility because they shape the factual map used in claims. A nuclear damage claim often turns on where the exposure occurred and at what level. When exposure is uncertain, compensation systems can face delay and dispute. When exposure is shown with transparent methods, compensation can be faster and more defensible. Ultimately, technology serves as the only definitive means to prove the causal relationship between the nuclear damage and the fault; this remains vital because even under a framework of strict liability, the affected party is never exempt from the burden of proving that explicit causal link.

3.3 Technology, Modeling, and Causation

Causation is a recurring challenge in nuclear damage claims. Even when liability is strict, a link between harm and exposure is often required. For some harms, especially long-term health harms, the link is probabilistic and depends on dose estimates and risk models. Technology affects these estimates by improving measurement and improving model inputs.

UN scientific assessments show how dose and risk analysis evolves over time. Reports on Fukushima exposures explain how measurement data, food controls, and environmental processes shaped public doses. The analysis also shows how uncertainty and data gaps were handled. These points matter because courts and compensation bodies often rely on these scientific baselines when judging whether a harm claim is plausible (UNSCEAR, 2013; UNSCEAR, 2020/2021).

Public health assessments also show how early risk estimates can be conservative due to limited data. The WHO health risk assessment explains its approach and the basis for early risk projections. It also shows how early estimates can set the tone for public debates and later claims, even when later data refines the picture (WHO, 2013).

Technology can reduce uncertainty, but it can also create disputes about models. Parties can argue over sensor placement, calibration, data gaps, and method choice. For responsibility decisions, this means that the legal system needs rules for transparency and review. It also means that parties need access to methods, not only outputs.

3.4 Remote Sensing and Cross-Border Fact Building

Remote sensing tools add a further layer. Satellites and related tools can help confirm indicators linked to nuclear events. They can also support oversight when access is limited. Remote sensing is not a direct radiation detector in many cases. Still, it can provide proxy signals that support risk screening and early warning. This can affect responsibility decisions because early notice duties and early protective actions depend on timely information.

A conference paper on remote sensing proxies for radiation anomalies explains how remote sensing methods can be used to detect proxy signals that may align with abnormal events. The value here is not a final dose number. The value is the ability to support early scrutiny and guide where more direct measurement should occur. This can matter in cross-border settings where states seek early facts and may later rely on those facts in claims or diplomatic steps (Smith & Berthoud, 2024).

Remote sensing also links to treaty duties on early notice and assistance. These treaties aim to ensure the timely sharing of information and support during nuclear or radiological emergencies. Modern data tools can help meet these duties through faster detection, sharing, and coordination (Convention on Early Notification of a Nuclear Accident, 1986; Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency, 1986).

4.0 Digitalization and Cyber Risks in Nuclear Liability

4.1 Digitalization Inside Nuclear Operations

Digitalization in nuclear operations can create detailed logs of events and actions. These logs can support incident investigation and later claims. They can also shape the legal view of due care and compliance. If an operator can show that key safety actions were taken and that systems were maintained, that record can matter in disputes about recourse claims or regulatory enforcement. If logs show gaps, they can support findings of negligence or breach of duty, even when strict liability applies for third-party compensation.

Guidance on digitalization for nuclear work processes explains how digital tools can support consistency, quality assurance, and traceable records. The guidance also notes that digitalization requires governance choices on access, retention, and validation. These choices matter because responsibility disputes often turn on whether records can be trusted (Idaho National Laboratory, 2024).

4.2 Safety-Critical Software and Operational Logs

Digital systems also raise licensing and assurance questions. A common regulatory position on safety-critical software highlights the need for strong assurance practices for software that supports safety functions. The position reflects concern about hidden faults, updates, and complex supply chains. These points matter for responsibility as software faults can be a root cause, and software assurance practice can shape later findings on fault and recourse (Office for Nuclear Regulation, 2024), raising pivotal questions on how to determine liability and exactly who bears the responsibility: the operator, the programmer, or the supplier.

4.3 Cyber Risk, Attribution, and Responsibility

Cyber threats add a distinct challenge. A cyber event can disrupt operations, cause unsafe conditions, or hinder monitoring and response. Even if a cyber-event does not cause a release, it can cause loss and fear. If a release occurs, cyber involvement can complicate causation and responsibility.

A legal and policy report on cybersecurity of the civil nuclear sector explains the threat landscape and the limits of existing legal protections. It also highlights how governance gaps can raise systemic risk. This matters because responsibility decisions depend on whether systems were reasonably protected, and whether a state met due diligence duties in regulation and oversight (Chatham House, 2024).

Attribution is also central when cyber activity is linked to state conduct. Legal analysis of cyber attribution explains how political and technical factors shape attribution claims. It also explains how the legal rules on attribution interact with evidence standards. These issues matter if a state seeks to argue that another state bears responsibility for a harmful cyber operation tied to a nuclear event (Brunner, 2025).

State responsibility rules provide the legal framework for these arguments. The draft articles on state responsibility explain attribution, breach, and remedies concepts that can apply when a state's act or omission is linked to harm. These rules also show why attribution is a threshold issue in many disputes (International Law Commission, 2001a).

5.0 Digital Evidence Preservation and Admissibility

5.1 Digital Evidence Preservation

This rigorous demand for digital evidence preservation becomes particularly critical when evaluating transboundary nuclear liability arising from a malicious cyber breach. If a cyberattack compromises a nuclear facility's operational technology (OT) and triggers a radiological release, it creates a complex legal conflict regarding liability attribution. Under traditional nuclear liability regimes, liability is strictly channeled to the plant operator. However, a pivotal question arises: should the operator be held liable due to a failure to maintain adequate cyber defenses (negligence in protection), or does a catastrophic cyber operation constitute an intervening act of hostility that exonerates the operator? Unraveling this requires unalterable digital forensics capable of proving whether the operator met the expected technological standard of care in safeguarding its digital infrastructure.

Guidance on digital evidence preservation describes steps to preserve digital evidence in a way that supports integrity and later review. This kind of guidance is important when nuclear incidents create large data streams and many potential evidence sources. It can also support trust when parties dispute whether logs were changed after an event (NIST, 2022).

5.2 Admissibility of Digital Evidence

Court acceptance is another key step. Research on the admissibility of digital evidence from open-source forensic tools shows that courts often expect validated methods and clear standards. The study proposes a framework to support legal acceptance while recognizing resource limits. This is relevant for nuclear damage settings because public agencies, claimants, and local groups may rely on open tools to process data and images (Ismail & Ariffin, 2025).

These evidence issues also connect to fairness. If only operators and states can process data, claimants may distrust results. If data is shared without safeguards, privacy and security risks can rise.

Technology, therefore, creates a need for balanced data governance that supports both truth-finding and rights protection.

5.3 International Prevention Duties and Due Diligence

Even when nuclear liability is channeled to operators, international law can still matter. Cross-border harm can trigger disputes between states. International environmental law focuses on prevention and due diligence, not only on compensation after the fact.

The draft articles on prevention of transboundary harm describe a duty to take all appropriate measures to prevent significant harm when hazardous activities are involved. Nuclear energy fits the category of hazardous activity because it can cause serious cross-border harm in rare cases. Technology affects what counts as "appropriate measures" because modern monitoring and safety tools can raise the expected standard of care (International Law Commission, 2001b).

This principle is anchored in the jurisprudence of the International Court of Justice (ICJ), which recognizes environmental impact assessments and ongoing monitoring as mandatory due diligence requirements under general international law. Specifically, the Court's landmark *Pulp Mills* judgment established that when a project risks causing transboundary harm, the state must undertake continuous monitoring of its environmental impacts. This requirement directly underscores the relevance of modern technology to contemporary nuclear governance; as international law demands continuous oversight, modern nuclear projects must leverage advanced data streams and digital monitoring tools to effectively fulfill this evolving legal standard more than in prior decades, and those tools can affect the legal evaluation of due diligence (International Court of Justice, 2010).

The Espoo Convention also supports cross-border assessment duties for projects likely to cause a significant transboundary impact. Technology can improve these assessments through better modeling, better baseline data, and better public information tools. These improvements can affect later responsibility claims, because a weak assessment record can support arguments of breach (UNECE, 1991).

6.0 How Technology Shapes Responsibility Under Treaty-Based Nuclear Liability

6.1 Technology and Compensation Processes

Technology does not change the basic rule in many systems that the operator is the main liable party to victims. Still, technology shapes how that rule works. It shapes what counts as nuclear damage in practice, how many claims are filed, and how claims are processed. It can also shape the choice between court litigation and administrative compensation pathways.

Technology can also affect supplementary funding triggers and cross-border allocation under treaty systems. When damage spreads across borders, states, and insurers may dispute the scale and location of harm. Measurement tools can reduce these disputes, but only if methods are shared and trusted. When methods are not shared, technology can increase disputes because parties can produce competing models and maps.

Treaty texts also link to notice and cooperation. Early notice and assistance duties are built for cross-border events. Modern technology can support faster notice through automated alerts, satellite screening, and shared platforms. This can reduce harm and can also support later responsibility decisions by creating a clearer event timeline (Convention on Early.

6.2 Cross-Border Cooperation and Notification Duties

The cross-border cooperation and notification aspects are part and parcel of the nuclear governance under treaties because of the transboundary character of some nuclear accidents, which require prompt action and cooperation. The Convention on Early Notification of a Nuclear Accident provides a legal obligation for states to notify authorities that might be affected (Northern Ireland, Isle of Man, and/or the Channel Islands) and relevant international bodies of nuclear incidents. In this duty, they try to minimize the time of risk perception and to enable immediate implementation of protective measures, particularly if the radiation pathway is outside the boundaries. In a macro sense, the Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency requires timeliness among the interested parties and cooperation in sharing various forms of technical assistance in the event of a nuclear incident. The importance of the possibility for transboundary impact management through systematic procedures of cross-border communication is emphasized in UNECE (1991). In practice, advanced operational monitoring systems can significantly support the mechanics of treaty cooperation by providing timely, reliable, and complete delivery of information.

6.3 Limits and Risks of Technology in Responsibility Decisions

Modern technology can also create new limits. Data can be incomplete, biased, or hard to interpret. Models can embed assumptions that favor one party's view. Private control of data can reduce trust. Cyber threats can undermine records and measurement systems.

Another risk is overreliance on proxy tools. Remote sensing proxies can support early scrutiny, yet they do not replace ground measurements. Legal systems should treat such tools as one input, not as final proof. This is especially important when decisions can affect large compensation outcomes or state-to-state tensions (Smith & Berthoud, 2024).

A further risk is unequal access. Operators and states often control core plant data and key monitoring systems. Claimants may rely on limited public data. This gap can reduce perceived fairness even when the legal outcome is correct. Evidence rules and disclosure duties can help, but they must also balance security and privacy needs.

7.0 Findings

7.1 Evolution of the Liability Framework

The development of nuclear liability law reveals that new technology does not replace the traditional legal architecture based on operator-centered strict liability, but plays a major role in its operational nature. This finding supports the impact of treaty-based regimes (i.e., Paris Convention, Vienna Convention, and the Convention on Supplementary Compensation), which continue to have the liability remain with the operator. However, the way the liability is dealt with is important in terms of evidential mechanisms, and this is where technology takes a major role. The research shows that digital evidence and automation of recordkeeping, sensors, and monitoring systems create a basis to guide assessment of the liability in a technologically advanced regime. This is confirmed by OECD NEA (2015), which indicates a stable context for implementing the nuclear liability system and the changing context of implementation. It supports the position of the International Law Commission (2001a), which sustains "the notion that the responsibility of the operator remains central to nuclear liability, based on the principles of the international wrongful act".

Accordingly, the question is raised, and technology is expected to be an operational modifier, not a substitute for the structure and design of nuclear liability law.

7.2 Enhanced Fact-Finding Capabilities

Better fact-finding capability results in speed, reliability, and accuracy in the determination of the extent and damage caused by a nuclear incident. This result has validated the ability of radiation maps, mobile detection systems, and drone platforms to increase on-site/in-situ speed of contamination and dose identification. These enable much more rapid incident evaluation without undue uncertainty and thereby affect the accuracy of compensation and administrative reaction speed. Some of the data show that the improvement of detection parameters directly affects legal procedures concerning damages. This is proven by Marques et al. (2021), who provide convincing evidence of the successful application of mobile radiation detection units in the nuclear security context. Corbacho et al. (2024) also successfully demonstrated the importance and usefulness of gamma spectrometry using a drone for improving the spatial resolution of a contaminated environment, thus further contributing to a more reliable fact-based evidence niche in liability litigation.

7.3 Evolving Nature of Evidence

The nature of the nuclear evidence is dynamic; as time passes, all of the scientific models, exposure data, and environment measurements will need to be updated, but this finding shows a reduction in the scientific models. This suggests that the determination of causation in nuclear liability claims is not static, but dependent on the use of an updated scientific model. The effects of long-term exposure, particularly in cases of radiological harm, can require recalibration of dose estimates and risk models. This poses legal problems as findings of fact in the first instance need not have been adequate, and later are liable to be challenged in light of updated scientific knowledge. This finding is similar to that of the UNSCEAR (2013) report on Scientific response to radiation exposures after nuclear accidents, which observes changes in scientific knowledge of radiation exposure since the accidents. It is also backed by the WHO (2013), which reports that early scientific assessments of doses and early health effects after a nuclear accident often underestimate the doses and effects. The findings can be supported by these reports.

7.4 Cross-Border Fact Building

Presently, cross-border fact building is possible thanks to the remote sensing systems, which allow sources to have the first and uncontroversial facts in case of a nuclear accident across a border. This discovery is an example of how satellite images and other proxy radiation detection systems have been used to determine facts concerning the environmental effects on the border. The methods for conducting key factual findings by experts and competent authorities from operating states, even if access to the affected areas is restricted. It also establishes that capacity is relevant to invoking notification obligations and international response, as Smith and Berthoud (2014) have argued. Also backed by the Convention on Early Notification of a Nuclear Accident (1986). The debate demonstrated that these systems can contribute to resolving conflicting reports on the initial characterization of an event, to the ease with which facts can be established, and to the elimination of jurisdictional ambiguities in cross-border nuclear events.

7.5 Operational Digitalization and Recourse

In nuclear liability systems, operational digitalization generates abundant digital documentation, which is essential for access and compliance with regulations, as well as in recourse procedures.

This discovery demonstrates that evidence of the design of a pattern has been created in the digital log, that this evidence can be shared in an automated control process, and that this evidence can be shared as an observation of the operation of the nuclear facility as part of the operation of the automated process that is part of the obligation to perform safety functions. The discovery indicates that the issue of whether secondary liability/contractual recourse actions should be considered would be determined by the digital record in nuclear operations. This is evidenced by Idaho National Laboratory(2024) and OECD NEA(2020), which respectively depicted digitalization and operational framework as contributors to defining nuclear operation transparency, governance, and expectation. Digitalization, therefore, redefines liability after a nuclear incident, and findings reveal that the operational data has played a fundamental role in the accountability and recourse processes in the sense that it has become more evident in terms of intricacy.

7.6 Emergence of Cyber Paths to Liability

The cyber channels of liability show the integration of software systems in the nuclear operation. This demonstrates that cyber events can be a direct or indirect cause of nuclear safety failures. Novel causal chains for the purpose of liability attribution have been established. Given that software vulnerabilities, system intrusions, and digital manipulation can be the initiating event in scenarios of nuclear risk, Li and Filloy (2017) conclude that they render classical models of attribution in nuclear liability law more complex. This can be supported by an example from Chatham House (2024) highlighting the common theme of emerging risk in the civil nuclear industry, with cybersecurity deficiency as the most commonly identified emerging risk. The finding is also confirmed by Brunner (2025), who explains and places the unanswered attribution issue of cyber operations in the framework of international law. There are unanswered questions regarding responsibility between operators, suppliers, and other actors.

7.7 Centrality of Digital Evidence Admissibility

As courts and tribunals are increasingly taking into account more complex technological sources of information, the admissibility of digital evidence has become a major concern for nuclear liability adjudication. The discovery suggests that the evidence from sensors, drones, artificial intelligence, and open source information, as well as the rules of evidence that courts and tribunals are applying, are now relevant to the judgment. The finding demonstrates that whether the sources have been trusted or the method of analysis has been transparent could impact decisions, thus calling into question the fairness and predictability of the leakage of recognition and remedies in several compensation systems. This interpretation is supported by NIST (2022), which provides principles for the preservation of the fidelity of digital evidence. It's also established by Ismail and Ariffin (2025), who investigate judicial reaction to open source forensic tools. Evidentiary governance should be stressed to maintain institutional trust. This discovery accentuates the importance of admissibility in nuclear liability.

7.8 Elevated Standards of Due Diligence

The international legal instruments for due diligence have now been upgraded by the use of the new monitoring and predictive technology. This conclusion is that due diligence requirements are to be fulfilled using instruments available to the state or operator. In the absence of such tools, it might now be considered a violation of the preventative nature of state obligations, in a similar fashion to the notion of transboundary harm prevention and the state's obligation to maintain the environment. This is reinforced by the International Law Commission (2001b) establishing preventive obligations in regard to the introduction of new "environmental hazards" and the ICJ (2010) treating the obligation to engage in continuous monitoring as equivalent to the due diligence obligation. This is an example of the ways in which technology changes the content of standards of responsibility.

7.9 Role of Customary International Law

In the field of nuclear liability and technologies, the major contribution of customary international law is that it is a major point of reference and that, in many respects, it is interpreted in the light of technological innovation. As can be seen from the rulings, the principles of state responsibility, preventive obligation, and measures and duty to assess the environmental impact remain as the guiding principles, but technologies employed for monitoring and analytic purposes have a significant influence on how they are applied. The thesis also builds a solid argument for the evidentiary obligations associated with breaches of international commitments and how technological capabilities support those obligations. This is corroborated by the International Law Commission (2001a), which sets out rules on state responsibility for internationally wrongful acts. The result is supported by UNECE (1991), which highlights the significance of environmental impact assessment, particularly in transboundary impact. This relationship is a testament to the fact that customary principles are still significant in technologically advanced contexts.

7.10 Simplification of Breach and Causation

High technology data systems allow for simulation and radiological mapping, leading to a better case for breach and causation in nuclear damage. It demonstrates the real capacity of scientific technology to explain the cause-and-effect pattern, and to evaluate the burden of causation with a high degree of certainty and evidence.9 In particular, technological advances in data analysis, exposure, and environmental pattern mapping have shed light on the reconstruction of causation. An improved reconstruction of causation leads to better allocation of obligations and compensation in court. UNSCEAR (2020/2021) is a scientific and thorough analysis of the emission and impact of radiation, which supports this. It is further strengthened by WHO (2013), which elaborates on the structured risk assessment of causation. It provides options for judicial application of causal reasoning in complex radiological causes of injury, and therefore justifies the increased evidentiary clarity.

7.11 New Challenges to Trust

The technological reliance on institutional and public trust in the nuclear liability scheme can be interpreted as new epistemic and systemic challenges as a result of data governance and interpretive complexity. This finding reveals that reliance on institutions on proprietary software, framing through competing models of interpretation, and cyber risks pose epistemic risks to confidence in the factual conclusions of the liability scheme. Disputes might be over data rights, methodological openness, and the trustworthiness of cyber systems. The finding highlights the potential for such challenges in both domestic (civil law) and international (third-party dispute settlement) contexts. This is proved by Chatham House (2024), which emphasizes the growing importance of cybersecurity and governance of the nuclear sector. In addition, this is exemplified by OECD NEA (2015) on the need for transparency and confidence in a nuclear governance framework. This finding is evidence of the epistemo-systemic risks that have occurred as a result of technological optimism. The finding also demonstrates that, today, there is no consensus regarding technology, which is now the main weakness of technology-dependent liability schemes.

8.0 Recommendations

8.1 Strengthen Digital Evidence Governance

It is recommended that nuclear operators take strong action to establish digital evidence governance to ensure the evidence is sufficiently reliable for the purposes of nuclear liability determinations, where digital systems have been increasingly used in factual reconstruction and attribution. The conclusion is based on the implications of Findings 7.7 and 7.11, which indicate that specific concerns exist within technology-based system liability regimes in terms of the reliability and admissibility of digital evidence. For example, nuclear operators should implement 'cryptographic verification', secure data acquisition and audit trail systems, and develop redundant digital record systems that keep digitally-generated operating and environmental data. Preservation should be long-term, for the effect of radiation, to allow digital evidence to be tendered for future claims and court action. The governance practices are consistent with the NIST (2022) statement that: 'The need for structured preservation protocols and reference systems is clear in any preservation effort to maintain the integrity of digital evidence.' They also follow the OECD NEA (2015) conclusion that: 'a nuclear governance framework for digital evidence systems must include ... exhaustive, standard methods of managing available, preserving digital evidence.

8.2 Expand Verification Capacity

Independent verification networks are additionally required to get away from the dependency on public verification data curated and managed by operators, specifically if the threat of an accident is high, bringing the image of objectivity into public decisionmaking into question. This recommendation strengthens the results of Findings 7.2 and 7.11 in pointing to the manner in which technology enhances the fact-finding process, but also creates a trust imbalance with the control of data. Indeed, IAOIs should put pressure on the development of independent networks of drones, mobile types of radiation detectors, and remote sensing devices that determine the level of contamination and of radiation exposure, other than the contested decisions of operators, in order to facilitate benefit transfer from Insurance to Compensation. The evidence presented by Marques et al. shows that mobile radiation detectors are suitable for screening environmental contamination, and the evidence presented by Corbacho et al. validates the use of drone-enabled gamma spectrometry for spatial mapping.

8.3 Embed Cybersecurity into Nuclear Legal Standards of Care

As part of the operator's duty of care, cybersecurity needs to be formally codified as incorporated into the law of nuclear liability. This is because the software and digital infrastructure for safety systems in nuclear plants are increasingly becoming an integral part of nuclear plant operations, and cybersecurity is a component of the duty of care. This recommendation is directly related to Finding 7.6 and Finding 7.5, which used a physical path as a means of causality, but have become a digital pathway to causality with mechanisms that can be exploited and liability assigned. All safety-critical systems must require a real-time Vulnerability Assessment, ongoing monitoring of the supply chain risk, and software assurance verification performed by operators. The regulators should put in place clear technical requirements to replace the standards of negligence perception to ensure cyber resilience. This is also indicated by Chatham House (2024), which lists systemic cyber-GIS risks to knowledge governance in civil nuclear power, and is further supported by the Office for Nuclear Regulation (2024), which states that software assurance is an important consideration for the nuclear regulator.

8.4 Enhance Cross-Border Data Sharing

The cross-border governance should be strengthened by creating digital platforms and systems to share real-time data, which could help to facilitate the orderly flow of information and therefore the coordination of emergency response. The suggestion is drawn from the Report 7.4 and 7.8, which address the importance of the use of remote sensing tools in transboundary nuclear risk management and the process of increased due care of the affected states. States need to establish a mode of transmitting encrypted radiation data to each other along existing international notification and assistance channels. To facilitate the conveyance of information without subjectivity, data reported in a universal format of the environmental media should be presented. The above-cited international legal instruments, the Convention on Early Notification of a Nuclear Accident (1986) and the UNECE (1991) Liaison between the neighboring heads of state to the United Nations, could support such innovative international solutions.

8.5 Modernize Judicial and Evidentiary Frameworks for Digital Proof

Judicial procedures need to evolve evidentiary standards to respond to the increasing reliance on technology-driven evidence in nuclear liability cases. This proposal was developed based on Findings 7.7 and 7.10, both of which found that the admissibility of this evidence and the scientific models used were relevant to causation and breach, respectively. It is also recommended that judicial training programs be conducted to build institutional capacity to evaluate scientific uncertainty and cyber-technical evidence. The analysis is based on the results of (i)Ismail and Ariffin (2025), which shows the need for institutionalized legal standards for open source forensic credibility, and (ii)Smith and Berthoud (2024), which shows the importance of the law of remote sensing for environmental and anomaly detection.

8.6 Enhance Technology-Enabled Due Diligence

Due diligence obligation has expanded in international nuclear and environmental law through monitoring and forecasting technologies. This tip is derived from Findings 7.8 and 7.9, which state that technological capability has a significant impact on preventive duties and customary international law, as well as the remainder of this recommendation, which calls on States to integrate continuous monitoring, predictive risk modeling, and real-time knowledge of environmental changes into nuclear governance, as part of the due diligence requirement. Technological developments for Nepal and other alleged States should be included in the due diligence listed below, to prevent transboundary harm. The due diligence obligation codified in the International Law Commission (2001b) for preventing substantial transboundary environmental harm is supported by the International Court of Justice (2010) affirmation of the due diligence standard with respect to transboundary environmental monitoring.

9.0 Conclusion

This paper explored the use of modern technology in the context of the existing treaty-based regimes of liability for peaceful nuclear energy use in the event of nuclear damage. The investigation revolved around several questions: how much technology influences nuclear damage liability; to what extent technology influences proof of causation, cross-border fact-finding, cyber forensics, and the reliability of the evidence used in nuclear damage claim cases? The legal framework of nuclear damage liability (e.g., strict liability, the channeling of liability to operators) itself has been left untouched, but its operation has been drastically changed by technological systems. Even if responsibility under the law remains with the nuclear operators, proof of damage and causality is shifted from being based on tangible evidence to being based on digital, scientific, and administrative evidence. This confirms that technology cannot displace nuclear damage law, but it can reshape the latter.

The evidence of improved fact-finding and developing evidence directly backs this, showing that new technology (including radiation mapping, unmanned drone systems, and remote sensing) can speed up and improve identification of the nuclear event and mode of exposure. However, new and emerging technology may also create challenges for fact-finding in terms of interpretation, disagreement, and uncertainty between methods, particularly in the field of long-term exposure. This directly answers the causality question as it shows that proof is of a higher standard, but technologically more difficult. The fact-finding exercise also shows that the nuclear event is not confined to a state border in terms of the evidentiary fact-finding and necessitates joint technical effort in establishing a shared set of facts. It demonstrates that new technology is a contributing factor to the facts, but it can also be a great source of verification challenges.

Responsibility structures are not developing the same way they have in the past, responding to physical causes. A vast amount of traces of "how and why" certain digital events occurred is generated, processed, and stored in the operational digital systems. This evidence is becoming increasingly relevant in regulatory compliance investigations and, of course, also in potential recourse claims, making digital traceability a key part of the liability inquiry. Nonetheless, the advent of cyber-borne threats has created novel causal trajectories complicating attribution and prompting difficult dilemmas as to whether liability should fall on the operators, the software developers, or the hackers. The first aspect offers a solid answer to the research question of 'who should be held responsible in the cyber context' by noting that nuclear liability law is not only evolving in recognition of novel vectors of risk, abstract causes of damage, but also non-physical, intangible, and digital. It also provides an example of the importance of the ability to establish evidentiary integrity and system security in making legal decisions.

The concept of due diligence and other international law principles also support this, as both of these trends point to a blurring of the lines of responsibility in the context of technological change and a focus on what is reasonable for state and business or other operators to do in relation to risk reduction. The developments are apparent when it comes to compliance and breach, in how the prevention commitments in transnational contexts get interpreted in specific rather than abstract terms of technological means. Similarly, the capacity to cooperate better between States and to set up notification systems shows that nuclear jurisdiction is becoming a more empirical and less conceptual concept.

From the increased reliance on digital modalities in nuclear governance, upgrade of data quality & governance, provision of better independent monitoring mechanisms, enhancement of cyber-security resilience, modernization of cross-border cooperation mechanisms & regulation of the functioning of evidentiary provisions. The purpose of these instrumentations is to eliminate 'the provisional and probabilistic character of the calculation and the arising underestimation threat' and to make the

instrumentations more transparent, but also to control informational asymmetry and insidiousness aspects, and not to endanger the fairness of the liability apportioning due to the technological complexity. Finally, this study finds that the legal structure of nuclear liability remains sound, but with a new functionality, where the process of evidence collection, analysis, and validation is abduced by technology.

References

International Treaties and Conventions

I. Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency (1986). *United Nations Treaty Collection*. https://treaties.un.org/doc/Publication/UNTS/Volume%201455/volume-1455-I-24645-English.pdf

II. Convention on Early Notification of a Nuclear Accident (1986). *United Nations Treaty Collection*. https://treaties.un.org/doc/Publication/UNTS/Volume%201438/volume-1438-I-24516-English.pdf

III. Convention on Supplementary Compensation for Nuclear Damage (1997). *Treaty Doc. 107-21*. Congress.gov. https://www.congress.gov/treaty-document/107th-congress/21/document

IV. Convention on Third-Party Liability in the Field of Nuclear Energy (Paris Convention). *OECD Legal Instruments*. https://legalinstruments.oecd.org/public/doc/307/307.en.pdf

V. Brussels Supplementary Convention (1963). *Convention supplementary to the Paris Convention of 29 July 1960 on Third Party Liability in the Field of Nuclear Energy*. United Nations Treaty Collection. https://treaties.un.org/doc/Publication/UNTS/Volume%201041/volume-1041-I-15974-English.pdf

VI. Vienna Convention on Civil Liability for Nuclear Damage (1963). *United Nations Treaty Collection*. https://treaties.un.org/doc/Publication/UNTS/Volume%201063/volume-1063-I-15497-English.pdf

VII. Vienna Convention on Civil Liability for Nuclear Damage (1997 Consolidated Text). *Nuclear Pool Documentation*.

https://nuclearpool.by/wp-content/uploads/2020/09/the-vienna-convention-on-civil-liability-for-nuclear-damage-1963.pdf

VIII. UNECE (1991). *Convention on Environmental Impact Assessment in a Transboundary Context (Espoo Convention)*. https://unece.org/fileadmin/DAM/env/eia/documents/legaltexts/Espoo_Convention_authentic_ENG.pdf

International Law Instruments and Case Law

IX. International Court of Justice (2010). *Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment*. https://www.icj-cij.org/case/135

X. International Law Commission (2001a). *Draft Articles on Responsibility of States for Internationally Wrongful Acts*. United Nations. https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

XI. International Law Commission (2001b). *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities*. United Nations. https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_7_2001.pdf

Journal Articles and Conference Papers

XII. Brunner, I. (2025). Attributing cyber operations under international law: Political and legal aspects. *QIL-Questions of International Law*. https://www.qil-qdi.org/wp-content/uploads/2025/06/03_Regulating-Activities_BRUNNER_FIN.pdf

XIII. Corbacho, J. A., García-Talavera, M., & others (2024). Use of a drone-based gamma-ray spectrometry system to quantify contamination and dose rate. *Radioprotection*. https://www.radioprotection.org/articles/radiopro/full_html/2024/02/radiopro230060/radiopro230060.html

XIV. Ismail, I., & Ariffin, K. A. Z. (2025). The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. *PLOS ONE, 20*(9), e0331683. https://doi.org/10.1371/journal.pone.0331683

XV. Klebanov, L. R., & Lizikova, M. S. (2025). Artificial intelligence in nuclear energy: Legal challenges and international cooperation in regulation. *RUDN Journal of Law*. https://journals.rudn.ru/law/article/view/44990/24989/en_US

XVI. Marques, L., Cardoso, R., & others (2021). State-of-the-art mobile radiation detection systems for nuclear security applications. *Sensors, 21*(4), 1051. https://www.mdpi.com/1424-8220/21/4/1051

XVII. Smith, R., & Berthoud, L. (2024). Remote sensing techniques for detecting proxies of radiation anomalies at nuclear facilities. *IEEE Aerospace Conference Proceedings*. https://www.researchgate.net/publication/379893920

XVIII. Xu, R. (2023). Application of drones in nuclear contaminated sites. *E3S Web of Conferences, 424*, 03004. https://www.e3s-conferences.org/articles/e3sconf/pdf/2023/61/e3sconf_icree2023_03004.pdf

Institutional Reports and Policy Documents

XIX. Chatham House (2024). *Cybersecurity of the Civil Nuclear Sector: Threat Landscape and International Legal Protections*. https://www.chathamhouse.org/sites/default/files/2024-11/2024-11-18-cybersecurity-civil-nuclear.pdf

XX. Congressional Research Service (2025). *Price-Anderson Act: Nuclear Power Industry Liability Limits and Compensation to the Public After Radioactive Releases (IF10821)*. Congress.gov.

https://www.congress.gov/crs_external_products/IF/PDF/IF10821/IF10821.6.pdf

XXI. Idaho National Laboratory (2024). *Digitalization Guiding Principles and Method for Nuclear Industry Work Processes*. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_232168.pdf

XXII. NIST (2022). *Digital Evidence Preservation (NISTIR 8387)*. https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf

XXIII. OECD Nuclear Energy Agency (NEA) (2012). *Japan's Compensation System for Nuclear Damage*. https://www.oecd-nea.org/upload/docs/application/pdf/2021-02/japans_compensation_system.pdf

XXIV. OECD NEA (2013). *Radiological Characterization (NEA/RWM/WPDD(2013)2)*. https://www.oecd-nea.org/upload/docs/application/pdf/2020-01/rwm-wpdd2013-2.pdf

XXV. OECD NEA (2015). *Nuclear Law Bulletin No. 95*. https://www.oecd-nea.org/upload/docs/application/pdf/2020-11/nlb95.pdf

XXVI. OECD NEA (2020). *Japan: Act on Compensation for Nuclear Damage (Act No. 147 of 1961, as amended)*. https://www.oecd-nea.org/upload/docs/application/pdf/2020-03/act_on_compensation_for_nuclear_damage_.pdf

XXVII. OECD NEA (2021). *Nuclear Law Bulletin, Volume 2020 Issue 2*. https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/05/nuclear-law-bulletin-volume-2020-issue-2_964d124e/27b9c2df-en.pdf

XXVIII. Office for Nuclear Regulation (2024). *Licensing of Safety-Critical Software for Nuclear Reactors: Common Position*

(Revision 1). https://www.onr.org.uk/documents/2024/common-position-safety-critical-software-rev1.pdf

XXIX. U.S. Department of Energy (2023). *Price-Anderson Act Report to Congress (January 2023).* https://www.energy.gov/sites/default/files/2023-02/PAA%20Report%20January%202023_0.pdf

XXX. WHO (2013). *Health Risk Assessment from the Nuclear Accident after the 2011 Great East Japan Earthquake and Tsunami.* https://eeae.gr/docs/files/_WHO%20health%20risk%20assessment_report.pdf

XXXI. UNSCEAR (2013). *UNSCEAR 2013 Report, Volume I: Scientific Annex A.* https://www.unscear.org/docs/publications/2013/UNSCEAR_2013_Report_Vol.I.pdf

XXXII. UNSCEAR (2020/2021). *UNSCEAR 2020/2021 Report, Volume II: Scientific Annex B.* https://www.unscear.org/docs/publications/2021/UNSCEAR_2020_21_Report_Vol.II.pdf