Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
http://ajee-journal.com

Research Article

AUTONOMOUS WEAPONS SYSTEMS AND EMERGING TECHNOLOGIES: LEGAL REGULATION CHALLENGES FOR NUCLEAR DISARMAMENT VERIFICATION

Alibek Bolat* and Sholpan Saimova

ABSTRACT

Background: *Autonomous weapons systems (AWS) and related emerging technologies are increasingly embedded in surveillance and decision-support architectures relevant to nuclear disarmament verification. This evolution intensifies concerns about accountability, human control and the reliability of evidentiary material generated by complex, opaque systems, including their downstream impact on fair-trial guarantees, evidentiary standards and the availability of effective remedies when such material is relied upon in judicial or quasi-judicial proceedings. The article asks whether existing international laws, especially nuclear disarmament treaties, international humanitarian law and general rules on state responsibility, adequately regulate the deployment of AWS-enabled capabilities in verification, or whether specific normative adaptations are required. By focusing on verification rather than battlefield use, the study highlights an underexplored dimension of the AWS debate and shows its significance for the credibility and sustainability of nuclear disarmament arrangements.*

DOI:
https://doi.org/10.33327/AJEE-18-9.1-a000182

Date of submission: 04 Dec 2025
Date of acceptance: 12 Jan 2026
Publication: 06 Feb 2026

Disclaimer:
The authors declare that opinion and views expressed in this manuscript are free of any impact of any organizations.

Methods: *The research relies on doctrinal and comparative legal analysis conducted by the authors, with artificial intelligence tools used solely for auxiliary tasks such as literature retrieval, material organisation, and preliminary screening of state practice, while all legal interpretations and normative assessments remain the independent work of the researcher. The study examines treaty regimes governing nuclear disarmament and non-proliferation, relevant soft-law instruments and the practice of international organisations involved in verification. It also compares policy documents and statements from multilateral forums concerning lethal AWS, verification technologies and the notion of meaningful human control to identify converging and diverging legal positions and emerging interpretive trends.*

Results and Conclusions: *Existing international law offers an essential but incomplete framework for regulating AWS-related verification. General principles of due diligence, precaution, proportionality, state responsibility and individual criminal liability apply, but they do not resolve challenges linked to high autonomy, algorithmic opacity and the delegation of legally significant judgments to machines. Future nuclear disarmament verification should therefore include explicit legal standards on meaningful human control, transparency, auditability and data governance for AI-enabled systems, with clear rules on attribution and review of machine-generated evidence. Developing concrete verification protocols, interpretive understandings, and institutional oversight to implement these standards would enhance legal certainty, scholarly and practical coherence, and confidence in verification, while preserving contestability, transparency and effective avenues of redress where autonomous outputs underpin allegations of non-compliance or individual responsibility.*

1 INTRODUCTION

Verification of nuclear disarmament is widely recognised as a necessary condition for any credible pathway towards a world without nuclear weapons. The existing non-proliferation and disarmament framework, centred on the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) and operationalised through the safeguards system of the International Atomic Energy Agency (IAEA) seeks to ensure that nuclear materials and activities remain exclusively peaceful.[1] At the same time, the strategic environment is being reshaped by a renewed nuclear arms race, the erosion of traditional arms-control instruments and the modernisation of both warheads and delivery systems by nearly all nuclear-armed states.[2]

1 IAEA, 'Safeguards and Verification' (*International Atomic Energy Agency (IAEA)*, 2025) <https://www.iaea.org/topics/safeguards-and-verification> accessed 3 December 2025; IAEA, 'Safeguards Overview: Comprehensive Safeguards Agreements and Additional Protocols' (*International Atomic Energy Agency (IAEA)*, 2025) <https://www.iaea.org/publications/factsheets/iaea-safeguards-overview> accessed 3 December 2025.

2 *SIPRI Yearbook 2025: Armaments, Disarmament and International Security* (56th edn, OUP 2025); SIPRI, 'Nuclear Risks Grow as New Arms Race Looms: New SIPRI Yearbook Out Now' (*Stockholm International Peace Research Institute (SIPRI)*, 16 June 2025) <https://www.sipri.org/media/press-release/2025/nuclear-risks-grow-new-arms-race-looms-new-sipri-yearbook-out-now> accessed

These dynamics have sharpened the long-standing concern that verification arrangements for future disarmament commitments must be both technically robust and politically legitimate. Initiatives such as the International Partnership for Nuclear Disarmament Verification (IPNDV), UNIDIR's work on verifying disarmament in the Treaty on the Prohibition of Nuclear Weapons (TPNW) and National Academies assessments of monitoring, verification and dismantlement capabilities illustrate an emerging ecosystem of research on innovative verification concepts, including the exploitation of big data, advanced sensors and remotely operated platforms.[3]

In parallel, rapid advances in artificial intelligence (AI), robotics and autonomy are transforming both military capabilities and verification technologies. On the verification side, the IAEA and research partners increasingly explore AI-enabled analysis of large heterogeneous datasets, as well as robotic and unmanned systems, including aerial drones, for tasks such as radiation mapping, container inspection and remote quasi-inspection of sensitive facilities.[4] This trend is also reflected in the IAEA's recent report to the General Conference, which highlights ongoing efforts to identify and assess emerging/innovative technologies to enhance the effectiveness and efficiency of the safeguards system.[5] On the military side, autonomous weapons systems (AWS) have become a central focus of legal and ethical controversy. The International Committee of the Red Cross (ICRC) defines AWS as systems which, once activated, select and apply force to targets without further human intervention and has called for new internationally agreed limits to preserve compliance with international humanitarian law (IHL) and ethical standards.[6] Within the framework of the Convention on Certain Conventional Weapons (CCW), the Group of Governmental Experts on lethal AWS has affirmed that IHL applies fully to all weapon systems and that human responsibility for decisions on the use of weapons must be retained, with appropriate

3 December 2025; Defence Industry Europe, 'SIPRI report highlights growing nuclear threat as modernization accelerates and arms control weakens' (*Defence Industry Europe*, 15 June 2025) <https://defence-industry.eu/sipri-report-highlights-growing-nuclear-threat-as-modernisation-accelerates-and-arms-control-weakens> accessed 3 December 2025.

3 IPNDV, 'Innovations in Nuclear Disarmament Verification: Research Poster Submissions from Experts around the World' (*International Partnership for Nuclear Disarmament Verification (IPNDV)*, 21 April 2020) <https://www.ipndv.org/news/innovations-in-nuclear-disarmament-verification-research-poster-submissions-from-experts-around-the-world/> accessed 3 December 2025.

4 Francisco F Parada Iturria and others, 'AI for Nuclear Safeguards Verification: ORNL Report' (*Oak Ridge National Laboratory*, November 2024) <https://www.ornl.gov/publication/ai-nuclear-safeguards-verification> accessed 3 December 2025.

5 IAEA, *Strengthening the Effectiveness and Efficiency of the Agency's Safeguards: Report of the Director General* (GC(68)/9, 12 August 2024) para 17 <https://www.iaea.org/sites/default/files/gc/gc65-16.pdf> accessed 3 December 2025.

6 ICRC, *ICRC Position on Autonomous Weapon Systems* (ICRC Position and Background Paper, May 2021) <https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems> accessed 3 December 2025.

human control exercised across the life-cycle of such systems.[7] Civil society and human rights organisations argue that AWS risks digital dehumanisation, structurally undermines accountability and should be subject to new legally binding prohibitions, especially where meaningful human control is absent.[8]

These debates intersect in complex ways with evolving nuclear delivery systems and the broader AI-nuclear nexus. Long-range missiles remain the most salient nuclear delivery platforms, but attention is increasingly directed towards advanced drones (unmanned aerial vehicles, UAVs) and other uncrewed systems. Arms-control instruments such as the Missile Technology Control Regime (MTCR) explicitly treat rockets and UAVs capable of delivering a 500 kg payload to a range of at least 300 km as potential carriers of weapons of mass destruction, while analytical work by the Nuclear Threat Initiative (NTI) and others classifies UAVs alongside aircraft, ballistic missiles and cruise missiles as nuclear-relevant delivery systems.[9] Recent scholarship emphasises that emerging technologies, especially unmanned systems and increasingly autonomous platforms, could reshape both nuclear delivery and nuclear disarmament verification.[10] In parallel, studies on military AI and nuclear risk highlight how autonomy, machine learning decision support and autonomous ISR can compress decision-making timelines and amplify the dangers of escalation in what some describe as the "third nuclear age".[11] Recent UNIDIR work reinforces these concerns, noting that a number of States explicitly prioritise risks associated with the possible integration of AI into nuclear command, control and communications (NC3), and warning that such integration may exacerbate strategic-stability pressures by further compressing decision timeframes and increasing the probability of misperception or inadvertent escalation.[12]

7 Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (CCW) (adopted 10 October 1980) <https://treaties.unoda.org/t/ccw> accessed 3 December 2025; CCW Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, 'Chairperson's Summary' (CCW/GGE.1/2020/WP.7, 19 April 2021) <https://docs.un.org/CCW/GGE.1/2020/WP.7> accessed 3 December 2025.

8 Human Rights Watch, *A Hazard to Human Rights: Autonomous Weapons Systems and Digital Decision-Making* (IHRC Harvard Law School 2025).

9 US Bureau of International Security and Nonproliferation, 'Missile Technology Control Regime (MTCR) Frequently Asked Questions' (*US Department of State*, 2025) <https://www.state.gov/bureau-of-international-security-and-nonproliferation/releases/2025/01/missile-technology-control-regime-mtcr-frequently-asked-questions> accessed 3 December 2025.

10 Esra Serim, 'Drone Technology and the Future of Nuclear Weapons' (*The Loop*, 23 July 2025) <https://theloop.ecpr.eu/advancing-drone-technology-and-the-future-of-nuclear-weapons> accessed 3 December 2025.

11 Vincent Boulanin (ed), *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*, vol 1: Euro-Atlantic Perspectives (SIPRI 2019).

12 Yasmin Afina, *The Global Kaleidoscope of Military AI Governance: Decoding the 2024 Regional Consultations on Responsible AI in the Military Domain* (UNIDIR 2024); UNGA, 'Work of the Advisory Board on Disarmament Matters: Report of the Secretary-General' (A/80/240, 23 July 2025) para 27 <https://unidir.org/wp-content/uploads/2025/08/UNIDIR-2025-ABDM-Report.pdf> accessed 3 December 2025.

Despite this rapidly evolving landscape, the corresponding legal discourse remains fragmented. Legal analyses of AI in the nuclear field primarily address safety and regulatory issues in the civilian nuclear sector or the compatibility of AI-assisted NC3 architectures with international law and strategic stability concerns.[13] Work on verification focuses on institutional design and technical feasibility under the NPT and TPNW, with limited attention to how AI-enabled and autonomous tools, including drones used as verification platforms, affect evidentiary standards, due process and responsibility in disputes about compliance.[14] Conversely, core AWS debates concerning meaningful human control, foreseeability, accountability and the allocation of responsibility rarely consider settings in which autonomous or semi-autonomous systems generate, process or interpret verification-relevant data, or the specific problems posed when such systems may also be, or be closely related to, potential nuclear delivery platforms.[15] This lacuna is particularly problematic given broader concerns that emerging technologies could simultaneously lower barriers to the acquisition of nuclear-capable delivery systems, including certain categories of drones, and complicate the detection and attribution of treaty violations.[16]

Against this backdrop, the present article examines autonomous weapons systems and related emerging technologies as they pertain specifically to nuclear disarmament verification, with particular attention to autonomous and remotely operated drones both as potential carriers of nuclear weapons and as components of verification architectures. It asks whether, and to what extent, existing international law, including nuclear disarmament and non-proliferation treaties, IHL, international human rights law, and the law of state responsibility, adequately regulates AWS (and drone-enabled verification activities) or whether additional normative development is required. Building on doctrinal and comparative legal analysis of treaty provisions, soft-law instruments, state practice in CCW and nuclear disarmament fora, and policy guidance on AI in the nuclear domain, the article argues that current law provides an indispensable but incomplete framework. In outline, it concludes that legally robust and legitimate verification arrangements for future nuclear disarmament will require explicit and operational standards on meaningful human control, transparency, auditability and data governance for AI-, drone- and AWS-enabled verification systems, together with clear rules on attribution and evidentiary reliability where such systems may also be associated with nuclear delivery capabilities. By articulating these standards, the article seeks to bridge currently separate strands of scholarship on AWS, drones and nuclear verification, and to inform ongoing practical discussions on how to design trustworthy, legally sound verification mechanisms for future nuclear disarmament.[17]

13 IAEA, *Topical Issues in Nuclear Installation Safety: Strengthening the Safety of Evolutionary and Innovative Reactor Designs* (Proceedings Series, IAEA Publishing 2025).

14 Shirley Johnson and others, *IAEA Safeguards: Preparing for the Future* (NTI 2020)

15 SIPRI, *ICRC Position* (n 6).

16 *SIPRI Yearbook 2025* (n 2); SIPRI, 'Nuclear Risks Grow (n 2).

17 Vladislav Chernavskikh and Jules Palayer, 'Impact of Military Artificial Intelligence on Nuclear Escalation Risk' (2025) 6 SIPRI Insights on Peace and Security 1, doi:10.55163/FZIW8544

A small but significant body of case law—ranging from the International Court of Justice's jurisprudence on nuclear testing and disarmament to European human-rights decisions on radiological risk and access to information and domestic and constitutional litigation on armed drones—further illustrates how courts already grapple with technologically mediated risks and access-to-justice guarantees, including, in particular, the fair-trial and equality-of-arms requirements under Article 6 ECHR and the effective-remedy standard under Article 13 ECHR (and, where EU law applies, Article 47 of the EU Charter of Fundamental Rights) even though these strands are rarely discussed together with nuclear verification.[18]

At the same time, questions about autonomous verification are not merely institutional or strategic. Verification findings can feed into diplomatic disputes, sanctions regimes, criminal prosecutions and domestic litigation, where they influence decisions that affect the rights and obligations of States and individuals. If the underlying evidence is generated or processed by autonomous systems, issues of chain of custody, explainability and error become directly relevant to classic access-to-justice guarantees such as the right to a fair trial, equality of arms and the right to an effective remedy. The present article, therefore, approaches the regulation of AWS- and drone-enabled verification not only as a matter of arms-control design, but also as part of a broader access-to-justice agenda, with particular relevance for European and Eastern European legal orders.

Research objectives and questions. This article pursues four objectives: (1) to map how existing international legal regimes (arms control, IHL, human rights, data protection and State responsibility) apply to autonomy and AI-enabled technologies in nuclear-disarmament verification; (2) to identify the verification-relevant normative elements that recur across these regimes (e.g., accountability, due process, auditability and data integrity); (3) to assess the extent to which current treaty practice and safeguards frameworks can operationalize these elements for autonomous verification tools; and (4) to propose a legally grounded set of minimum requirements for the admissibility and contestability of machine-generated verification evidence.

Accordingly, the article is guided by the following research questions:

RQ1: Which existing international legal norms are most directly applicable to autonomous/AI-enabled verification technologies in nuclear disarmament?

RQ2: What normative elements are necessary to ensure that autonomous verification outputs can be treated as reliable and legally usable evidence?

RQ3: Where do current verification regimes (including safeguards practice) leave gaps regarding auditability, attribution and responsibility for machine-mediated findings?

18 Council of Europe, *European Convention on Human Rights* (Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols) (ECtHR 2013); Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.

RQ4: What minimum legal and procedural safeguards are required to ensure accountability and effective remedies when autonomous verification outputs affect compliance determinations?

2 METHODOLOGY

This article adopts a qualitative, doctrinal and comparative legal research design. The core of the analysis consists of a systematic interpretation of international legal instruments relevant to nuclear disarmament and the regulation of emerging military technologies, including autonomous weapons systems (AWS), drones and AI-enabled verification tools. The doctrinal component follows the general rule of interpretation under the Vienna Convention on the Law of Treaties, combining textual, teleological and systemic approaches to assess how existing norms on disarmament, international humanitarian law, international human rights law and state responsibility apply to AWS- and drone-enabled verification activities. Particular attention is given to the evidentiary and accountability dimensions of verification, to connect the argument with broader guarantees of access to justice and fair trial rights in both international and domestic fora.

The corpus of primary materials was defined *ex ante* and is replicable. It consists of: (a) universal treaties and related instruments on nuclear disarmament and non-proliferation (such as the NPT and TPNW), conventional arms-control regimes relevant to delivery systems (including those covering missiles and unmanned aerial vehicles), and core IHL and IHRL instruments; (b) institutional documents, reports and technical guidance produced by the IAEA, United Nations disarmament bodies, the Convention on Certain Conventional Weapons (CCW) and other relevant international organisations concerning AWS, drones, AI and verification; (c) soft-law standards and expert principles proposed by international and regional organisations, professional associations and civil society (for example on meaningful human control, AI governance and responsible military AI); and (d) case law from international courts and tribunals—including the International Court of Justice's jurisprudence on nuclear testing and disarmament and European Court of Human Rights decisions on radiological risk and access to information, as well as selected judgments of constitutional and supreme courts on technologically mediated evidence, armed-drone operations and military innovation where access-to-justice guarantees are at stake. Secondary materials include peer-reviewed scholarship and policy reports on AWS, drones as potential nuclear delivery systems, nuclear verification, and AI in the nuclear domain, identified through targeted keyword searches across major legal and interdisciplinary databases (including Scopus and Web of Science) and leading regional law journals. All searches were conducted in 2024–2025 using stable keyword combinations (e.g. "autonomous weapons AND verification", "drones AND nuclear delivery", "AI AND nuclear safeguards", "meaningful human control AND evidence"), which are reported in the supplementary materials so that other researchers can replicate and update the corpus.

The comparative element of the study has two layers. First, it compares the treatment of AWS, drones and AI-enabled verification across relevant treaty regimes and institutional practices, mapping convergences and divergences in how notions such as human control, foreseeability, proportionality and due process are articulated. Secondly, it selectively examines practice and doctrinal debates in Eastern European jurisdictions where questions of technologically mediated evidence, military use of AI and drones, or nuclear-related risks have prompted legislative or judicial responses. The analysis proceeds in three steps: 1) identification and classification of legal provisions and policy statements that bear on AWS- and drone-enabled verification; 2) reconstruction of their underlying normative assumptions, especially regarding human control, accountability and evidentiary reliability; and 3) evaluation of these assumptions against access-to-justice standards - in particular fair-trial and effective-remedy guarantees under international and regional human-rights instruments, leading to the normative proposals developed in the Results and Conclusions section. With a particular focus on the Council of Europe framework (ECHR Articles 6 and 13) and the EU standard of effective judicial protection (Charter Article 47), insofar as verification outputs may be used in proceedings or regulatory decisions within European jurisdictions. The tables and figures presented in the Results section, therefore, synthesise the material in a qualitative, interpretive manner rather than reporting a separate statistical dataset.

No separate empirical dataset involving human subjects, experimental measurements or proprietary computer code was generated for this research; instead, the study relies on doctrinal and policy analysis of publicly available legal and technical materials. All materials consist of publicly available legal and policy documents and published scholarship. Where access to materials depends on subscription-based databases or publisher paywalls, full citations are provided in the article so that readers with institutional access can consult the same sources. A consolidated list of all primary instruments and decisions, together with the keyword strings and inclusion/exclusion criteria used to construct the corpus, will be made available as supplementary material or via an open institutional repository, subject to the copyright and licensing conditions of the underlying documents. This enables other scholars to replicate the selection and to build upon the analytic framework proposed in this article.

Generative artificial intelligence (GenAI) was employed only as an auxiliary instrument in the research and writing process. Specifically, ChatGPT (OpenAI) was used to assist in: (a) preliminary mapping of existing literature and policy documents by suggesting additional search terms; (b) generating alternative formulations and structural options for certain sections; and (c) language refinement and consistency checks in the drafting stage. All legal interpretations, argumentation and conclusions were developed independently by the author, who reviewed, verified, and, where necessary, substantially rewrote any AI-assisted draft text. No AI tool was used to make legal or policy decisions, to generate original research findings, or to determine the normative positions advanced in the article.

The authors bear sole responsibility for the accuracy of citations, the selection and interpretation of sources, and all substantive claims contained in this work. The descriptive distributions and matrices in the Results section are based on this manual doctrinal and policy analysis and should be read as qualitative syntheses, not as the product of AI-driven document coding or statistical modelling.

3 RESULTS

The findings of this study can be organised into three interrelated clusters, which correspond to: 1) the extent to which existing international law regulates autonomous and AI-enabled technologies in nuclear disarmament verification; 2) the specific position of drones as both verification platforms and potential nuclear delivery systems; and 3) the emergence of a common set of normative standards that could guide the design and use of such technologies in legally robust verification architectures. Tables 1–4 and Figures 1–3 provide structured overviews of the doctrinal and policy-mapping results referred to below.

First, the cross-regime coding exercise shows that the bulk of relevant provisions in nuclear disarmament treaties, safeguards practice, international humanitarian law (IHL), human rights law and the law of state responsibility are formulated as obligations of control and due diligence, while a significantly smaller proportion directly addresses accountability and evidentiary reliability (Table 1).

***Table* 1. Cross-Regime Mapping of Relevant Legal Provisions**

Regime / Instrument Type	Example Instruments / Sources (generic)	Main Regulatory Focus for Verification Tech	Coded Category*
Nuclear disarmament and non-proliferation treaties	NPT, TPNW, bilateral reduction treaties	Prohibition of diversion, dismantlement obligations, verification mandates	Control & due diligence
Conventional arms control / delivery systems	Missile-related regimes, UAV export control rules	Limitations on delivery platforms, payload/range thresholds	Control & due diligence
International humanitarian law (IHL)	Geneva law and Hague law instruments	Conduct of hostilities, weapons reviews, targeting constraints	Control & due diligence
International human rights law (IHRL)	Core UN and regional human rights conventions	Right to life, fair trial, privacy, due process in evidence use	Accountability & evidentiary

Regime / Instrument Type	Example Instruments / Sources (generic)	Main Regulatory Focus for Verification Tech	Coded Category*
Law of state responsibility	Draft Articles on Responsibility of States for ILW	Attribution, breach, reparation, complicity	Accountability
International criminal law	Statutes of international tribunals	Individual criminal responsibility, command responsibility	Accountability
Institutional safeguards and verification practice	Safeguards agreements, verification handbooks	On-site inspections, remote monitoring, data-handling standards	Control & due diligence
Soft law and expert principles on AI/AWS	Principles on meaningful human control, AI ethics	Human control, transparency, auditability, safety requirements	Mixed (all three categories)

*Coded categories: **Control & due diligence**, **Accountability**, **Evidentiary reliability**

A qualitative review of these provisions indicates that most are framed as obligations of control and due diligence, with a smaller cluster concerned with accountability mechanisms and an even more limited subset explicitly addressing evidentiary reliability. Figure 1 offers a stylised representation of this pattern.

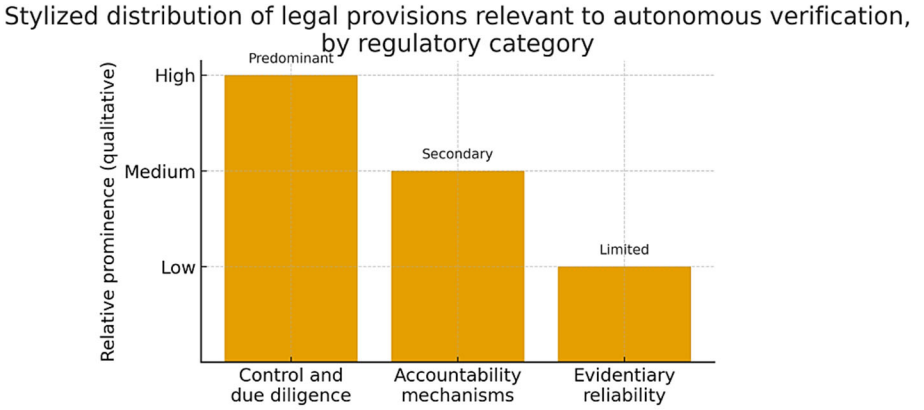


Figure 1. Stylised distribution of legal provisions relevant to autonomous verification, by regulatory category

This distribution confirms that existing regimes were not drafted with autonomous or AI-enabled verification tools in mind: they provide clear expectations that states must exercise adequate control over weapons and related technologies, but they offer little explicit guidance on how to treat data generated by autonomous systems, how to ensure its auditability, or how to allocate responsibility when such systems malfunction or embed bias. The gap is particularly evident when these general norms are read alongside contemporary debates on autonomous weapon systems (AWS), where the ICRC and others have called for new legally binding rules to address unpredictability, human control and responsibility in the use of autonomous force.[19] The findings therefore indicate that, while AWS debates already recognise the need for technologically specific limits, analogous questions arising in the context of nuclear disarmament verification remain only partially articulated in existing instruments.

Second, the technical and policy mapping demonstrates that drones occupy a particularly sensitive dual-use position. On the one hand, safeguards-oriented work by laboratories and international partners shows that unmanned aerial vehicles (UAVs) can greatly enhance verification by enabling remote visual inspection, environmental sampling and radiation mapping in inaccessible or hazardous locations.[20] On the other hand, both technical reports and recent analyses of nuclear safety and security highlight that many of the same UAV configurations—especially long-range systems with modular payload bays—possess characteristics comparable to delivery platforms for weapons of mass destruction or can be repurposed for hostile operations against nuclear facilities.[21]

A structured summary of technical characteristics relevant to verification is provided in Table 2, while Figure 2 visualises this overlap, showing that some archetypal verification drones fall within recognised missile-technology thresholds or could be modified to do so. The findings thus confirm that drones deployed in verification roles cannot be treated solely as benign technical aids; they must also be viewed as potential objects of regulation in their own right, raising proliferation, targeting, and escalation concerns that intersect with their verification functions. Related case law on armed-drone operations—such as the German Ramstein litigation, United States federal cases in the Al-Aulaqi line and criminal proceedings involving planned drone-delivered attacks—underscores that courts already treat certain categories of drones as inherently dangerous weapons and scrutinise the adequacy of legal frameworks governing their use, including in terms of extraterritorial obligations and access to effective remedies.

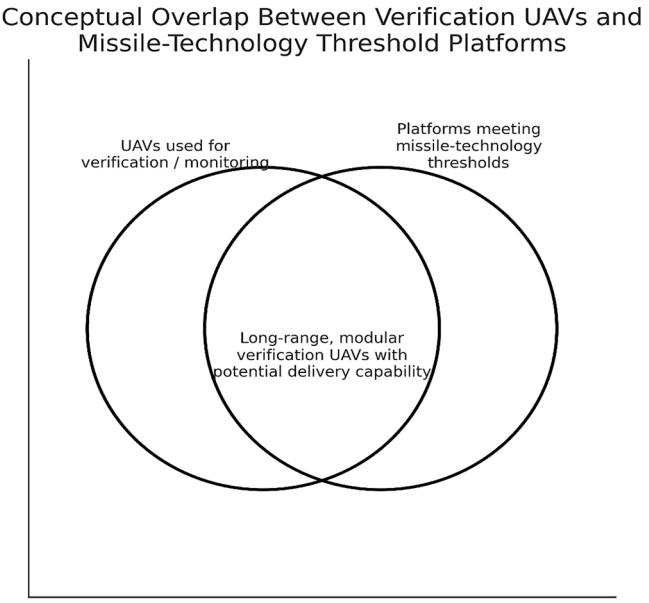
19 ICRC, *ICRC Position* (n 6).

20 John E Smart and others, *Nuclear Safeguards Applications Employing Unmanned Airborne Vehicles* (PNNL-25394, Pacific Northwest National Laboratory 2016).

21 Sven Dokter, 'The Role of Drones in Nuclear Safety and Security - An Overview of the Benefits and Risks of Using this Technology' (*European Technical Safety Organisations Network (ETSON)*, 11 September 2025) <https://www.etson.eu/node/429> accessed 3 December 2025.

***Table* 2. Technical archetypes of AWS and drone-enabled systems considered in the verification analysis**

System Type / Archetype	Primary Verification Function	Autonomy Level (low–high)	Typical Payload / Capability	Sensor Suite (examples)	Auditability (log / traceability features)	Dual-Use Assessment (delivery risk)
Autonomous inspection UAV (short-range)	Perimeter monitoring, radiation mapping	Medium	Lightweight detectors, cameras	EO/IR cameras, basic radiation sensors	Flight logs, sensor logs, basic anomaly reports	Low–medium (limited payload, range)
Long-range UAV with modular bay	Area surveillance, remote observation of facilities	Medium–high	Modular bay up to several hundred kg	EO/IR, SAR, SIGINT payloads	Detailed mission logs, payload usage logs	High (meets missile-type MTCR thresholds)
Fixed autonomous ground sensor network	Continuous local monitoring (radiation, movement)	Medium	Fixed, non-mobile	Radiation detectors, motion sensors	Continuous data logging, local tamper-evident storage	Low (no delivery capability)
AI-based anomaly-detection platform	Off-site analysis of multimodal verification data	High (algorithmic)	Non-physical, software-based	Input: satellite imagery, sensor streams	Versioned models, change logs, decision logs	Indirect (supports targeting/ intelligence)
Autonomous surface/underwater vehicle	Monitoring of maritime nuclear sites	Medium–high	Sensors, possible heavy payload	Sonar, radiation detectors, navigation aids	Mission logs, route tracking, sensor data logs	Medium–high (potential for delivery modification)



Note. Venn diagram **Circle A (left):** UAVs deployed or proposed for verification/monitoring tasks (Characteristics: long loiter time, high-resolution sensors, secure comms.); **Circle B (right):** Platforms meeting missile-related payload/range thresholds for WMD delivery (Characteristics: payload ≥ 500 kg and range ≥ 300 km, or equivalent criteria). **Intersection: -** Class of long-range drones used for surveillance that also meet or could easily be modified to meet delivery thresholds; - Systems with modular bays, autonomous navigation, and secure guidance.

***Figure* 2. Conceptual overlap between UAVs used for nuclear verification and UAVs meeting recognised missile-technology thresholds**

Third, the analysis of state submissions to the Convention on Certain Conventional Weapons (CCW) Group of Governmental Experts on lethal AWS, ICRC guidance, NGO advocacy and specialist safeguards literature reveals a converging set of normative elements that could serve as building blocks for regulating autonomous and AI-enabled verification systems. These elements include requirements for meaningful human control over critical functions, limitations on unpredictability, transparency and explainability of system behaviour, robust data integrity and cybersecurity safeguards, and pre-deployment technical-legal reviews.[22] The frequency distribution of these elements is displayed in **Figure 3, while** a consolidated matrix of recurring normative themes is presented in **Table 3.**

22 Cristina Siserman-Gray and others, 'Regulatory Challenges Related to the Use of Artificial Intelligence for IAEA Safeguards Verification' (*Institute of Nuclear Materials Management (INMM)*, 2023) <https://resources.inmm.org/annual-meeting-proceedings/regulatory-challenges-related-use-artificial-intelligence-iaea> accessed 4 December 2025.

***Table* 3. Recurring normative elements in discourses on AWS, drones and AI-enabled verification**

Normative Element / Principle	State Submissions (frequency)	Institutional Reports (frequency)	Expert / NGO Principles (frequency)	Typical Formulation (generic)
Meaningful human control	High	Medium	High	Human officials must retain effective authority and practical ability to 1) authorize and constrain verification missions, 2) supervise and intervene/override autonomous behaviour, and 3) validate and sign-off autonomous outputs before they generate legal effects (evidence, compliance findings, or enforcement triggers)
Transparency and explainability	Medium	High	High	System behaviour and decision paths must be understandable.
Data integrity and cybersecurity	Medium	High	Medium	Verification data must be protected against tampering and intrusion.
Pre-deployment review and certification	Low–medium	Medium	High	Systems must undergo technical–legal review before use.
Proportionality and risk assessment	Medium	Medium	Medium	Use must be preceded by context-sensitive risk analysis.
Remedies, accountability, redress	Low–medium	Low–medium	Medium	Mechanisms for responsibility and redress must be specified.

Note: Entries "high", "medium" and "low" reflect the author's qualitative assessment of the prominence of each element in the sampled materials rather than the output of a formal quantitative coding exercise.

Meaningful Human Control in verification. For the purposes of nuclear disarmament verification, meaningful human control (MHC) should be understood as the continuous and effective involvement of designated human officials in the critical verification functions that can produce legal consequences. Unlike the use-of-force context, where MHC primarily concerns human control over target selection and the application of force, in the verification context, MHC concerns human control over evidence generation and compliance assessment. At minimum, MHC requires: 1) human authorisation of mission objectives, geographic scope and rules of operation; 2) practical ability to supervise operations and intervene/override or abort autonomous behaviour; and 3) human validation and formal sign-off of any machine-generated compliance-relevant assessment before it is treated as evidence or triggers enforcement measures. MHC, therefore, depends on auditable logs, explainability sufficient for review, and an institutional review pathway that can correct or contest autonomous outputs.[23]

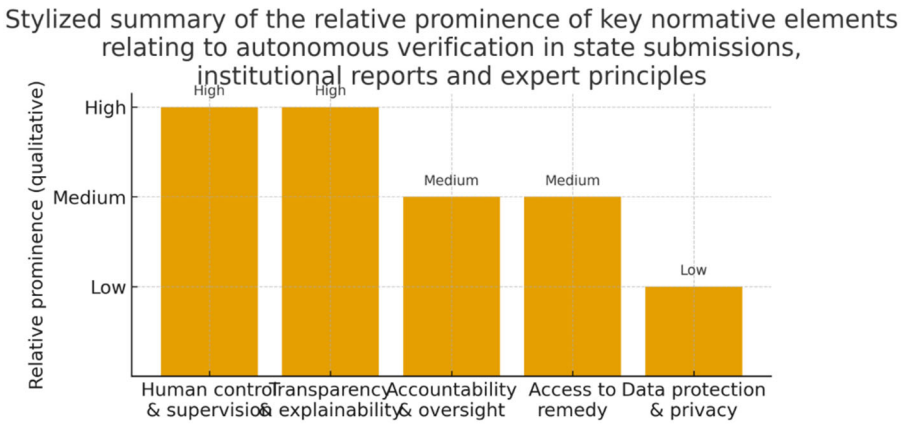


Figure 3. Stylised summary of the relative prominence of key normative elements relating to autonomous verification in state submissions, institutional reports and expert principles

At the same time, studies on AI in nuclear safeguards underline that AI-based tools are already being explored for anomaly detection, pattern recognition and the fusion of geospatial and operational data, while stressing that these developments must be aligned with evolving AI regulatory frameworks and safeguards-specific legal constraints.[24] The findings of this study systematise these strands by showing that, across the examined

23 UNIDIR Security and Technology Programme, *The Weaponization of Increasingly Autonomous Technologies: Considering How Meaningful Human Control Might Move the Discussion Forward* (UNIDIR 2014) 4.

24 Ahmed Abdelrahman Ibrahim and Hak-Kyu Lim, 'A Deterministic Assurance Framework for Licensable Explainable AI Grid-Interactive Nuclear Control' (2025) *18*(23) *Energies* 6268, doi:10.3390/en18236268.

discourse, there is implicit agreement on a core normative grammar-human control, transparency, auditability, data protection, but that explicit, verification-specific operationalisation of these principles is still largely absent.

Finally, the jurisprudential survey summarised in Table 4 shows that courts and quasi-judicial bodies have begun to engage with technologically generated evidence and with disputes arising from nuclear-related risks and armed drone operations. One cluster of decisions, exemplified by *Prosecutor v Ahmad Al Faqi Al Mahdi (ICC)*, *Big Brother Watch and Others v the United Kingdom* (ECtHR), *City of Sioux City v Jacobsma* and *State v Loomis*, addresses satellite imagery, bulk interception, automated enforcement and algorithmic risk scoring, and thus illustrates how judges assess the admissibility, probative value and contestability of machine-generated evidence.

A second cluster, including the ICJ's Nuclear Tests, Nuclear Weapons and Marshall Islands cases, ECtHR judgments such as McGinley and Egan, LCB and Roche, and domestic and constitutional litigation on armed drones in Germany (Ramstein) and the United States (the Al-Aulaqi line of cases), concerns the evidentiary and remedial dimensions of nuclear testing, radiological exposure and lethal drone strikes.

Taken together, these strands reveal both a willingness to admit technologically mediated evidence and a persistent concern with issues such as chain of custody, access to underlying data, the burdens of proof and the effective availability of remedies.

While none of the decisions examined directly addresses autonomous nuclear disarmament verification, they illustrate the types of procedural safeguards that will be necessary if autonomous or AI-enabled verification outputs are used to support allegations of non-compliance or to justify sanctions and other coercive measures, and they show how courts link technologically mediated risk to fair-trial guarantees, equality of arms and the right to an effective remedy. Against the background of broader analyses of AI, strategic stability, and nuclear risk—which emphasise compressed decision-making timelines, new escalation pathways and uncertainties in human-machine interaction—the study concludes that integrating autonomous and AI-enabled systems into nuclear disarmament verification without explicit evidentiary and accountability standards would risk exacerbating, rather than reducing, doubts about compliance and fairness.[25]

Taken together, the findings support three core conclusions: 1) existing law forms a necessary but incomplete basis for regulating autonomous verification technologies; 2) drones used for verification must be governed with full awareness of their dual-use potential as nuclear-relevant delivery systems; and 3) future nuclear disarmament arrangements will need to codify verification-specific standards on human control,

25 Olivia Le Poidevin, 'Nations Meet at UN for «Killer Robot» Talks as Regulation Lags' (*Reuters*, 12 May 2025) <https://www.reuters.com/sustainability/society-equity/nations-meet-un-killer-robot-talks-regulation-lags-2025-05-12> accessed 4 December 2025.

transparency, data governance and evidentiary treatment if they are to maintain both technical effectiveness and legal legitimacy.

***Table* 4. Selected judicial decisions on technology-generated evidence and their implications for autonomous verification and access to justice**

Case	Forum / Jurisdiction	Technology involved	Core procedural issue	Admissibility outcome (simplified)	Relevance for autonomous verification and access to justice
Prosecutor v. Ahmad Al Faqi Al Mahdi No. ICC-01/12-01/15, 27 September 2016[26]	International Criminal Court	Satellite and aerial imagery, remote sensing, digital reconstructions	Reliability, authentication and corroboration of imagery-based evidence	Evidence admitted as part of a broader evidentiary mosaic, with explicit discussion of corroboration and expert validation	Illustrates conditions under which high-tech imagery can satisfy evidentiary standards and be subjected to adversarial challenge when used to support legally significant findings.
Big Brother Watch and Others v. the United Kingdom Apps Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021[27]	European Court of Human Rights (Grand Chamber)	Bulk interception, communications-data collection and algorithmic selectors	Right to privacy and freedom of expression versus national-security surveillance; adequacy of safeguards and ex post remedies	Violations found due to insufficient safeguards and oversight; emphasis on foreseeability and effective remedies	Sets out requirements for legal frameworks governing large-scale, automated data collection and for ensuring effective remedies where such systems are used.
City of Sioux City v. Jacobsma No. 13–1502, 20 February 2015[28]	National supreme court (United States, Iowa)	Automated speed-enforcement cameras	Burden of proof, presumption of innocence and due process where liability is based on machine-generated data	Automated-enforcement scheme upheld under a model of rebuttable presumption and with opportunities to contest machine-generated evidence	Illustrates judicial approaches to the probative value of automated sensor data and the need to preserve contestability for affected parties.

26 *Prosecutor v Ahmad Al Faqi Al Mahdi* no ICC-01/12-01/15-171 (ICC, Trial Chamber VIII, 27 September 2016) <https://www.icc-cpi.int/court-record/icc-01/12-01/15-171> accessed 6 December 2025.

27 *Big Brother Watch and Others v the United Kingdom* App nos 58170/13, 62322/14 and 24960/15 (ECtHR [GC], 25 May 2021) <https://hudoc.echr.coe.int/eng?i=001-210077> accessed 6 December 2025.

28 *City of Sioux City v Jacobsma* no 13–1502 (Iowa Sup Ct, 20 February 2015) <https://law.justia.com/cases/iowa/supreme-court/2015/131502.html> accessed 6 December 2025.

Case	Forum / Jurisdiction	Technology involved	Core procedural issue	Admissibility outcome (simplified)	Relevance for autonomous verification and access to justice
State v. Loomis No. 2015AP157-CR, 13 July 2016[29]	National supreme court (United States, Wisconsin)	Proprietary algorithmic risk-assessment tool (COMPAS)	Opacity of algorithm, fair-trial guarantees and due process in sentencing decisions	Use of risk scores permitted only as one factor among others, with warnings about limitations and safeguards to preserve judicial discretion	Demonstrates judicial concern with explainability, transparency and the ability of defendants to challenge algorithmic assessments.
Nuclear Tests (Australia v. France), 20 December 1974[30]	International Court of Justice (ICJ)	French atmospheric nuclear tests in the South Pacific and their monitoring (air and sea measurements, remote sensing)	Admissibility of a claim following France's unilateral announcements to cease atmospheric testing; sufficiency of the state's public statements as evidence of a change in the legal situation and fulfillment of an obligation	The Court found that France's public statements about the cessation of atmospheric testing created legally binding unilateral obligations, and as a result the dispute lost its subject matter; the case was dismissed.	Demonstrates that official declarations and observational data can serve as elements of a "verification regime" even without a formal treaty. It demonstrates how the Court assesses the reliability and sufficiency of evidence of the cessation of nuclear activity-an important precedent for discussing the credibility of autonomous and remote verification systems. It is important for access to justice that the Court uses a standard that allows applicant states to rely on publicly available evidence (declarations and technical data), and not just internal documentation.

29 *State v Loomis* no 2015AP157-CR (Wis Sup Ct, 13 July 2016) <https://law.justia.com/cases/wisconsin/supreme-court/2016/2015ap000157-cr.html> accessed 6 December 2025.

30 *Nuclear Tests (Australia v France)* (ICJ, 20 December 1974) <https://www.icj-cij.org/case/58> accessed 6 December 2025.

Case	Forum / Jurisdiction	Technology involved	Core procedural issue	Admissibility outcome (simplified)	Relevance for autonomous verification and access to justice
Legality of the Threat or Use of Nuclear Weapons, 8 July 1996[31]	International Court of Justice, advisory opinion at the request of the UN General Assembly.	Nuclear weapons as a specific type of weapon; assessment of their compatibility with the UN Charter and IHL; emphasis on the obligation to conduct disarmament negotiations "under strict and effective international control."	The Court's competence to give an opinion; the limits of its advisory function in the sensitive field of security and disarmament.	The Court found the request admissible and issued an advisory opinion. It stated that, in general, the threat or use of nuclear weapons is incompatible with IHL, but was unable to definitively resolve the issue in the "extreme case of self-defense, when the very existence of a State is at stake". It affirmed the obligation to negotiate nuclear disarmament and pursue it to a conclusion.	Normative foundation: the rationale that any autonomous verification mechanisms serve the purpose of implementing nuclear disarmament obligations. The formula of "strict and effective international control" logically leads to the development of technical and algorithmic means of verifying treaty compliance. For access to justice, this establishes a framework within which courts and quasi-judicial bodies evaluate evidence of compliance/violation of disarmament obligations, including data obtained through autonomous systems.
Obligations concerning Negotiations relating to Cessation of the Nuclear Arms Race and to Nuclear Disarmament (Marshall Islands v. United Kingdom),	International Court of Justice	Obligations under Article VI of the NPT and customary law on nuclear disarmament negotiations; the question of whether nuclear powers are conducting genuine negotiations	The existence of a "dispute" between the Marshall Islands and the defendants at the time of the application; the standard of proof of the dispute and the jurisdiction of the Court	The court, by a majority, found that there was no proven dispute and declined jurisdiction without proceeding to the merits.	The high threshold for proving the existence of a dispute is indicative – important for all cases where the applicant relies on open sources, technical data, and automated analysis of state behavior. From an access to justice perspective,

31 *Legality of the Threat or Use of Nuclear Weapons* (ICJ, 8 July 1996) <https://www.icj-cij.org/case/95> accessed 6 December 2025.

Case	Forum / Jurisdiction	Technology involved	Core procedural issue	Admissibility outcome (simplified)	Relevance for autonomous verification and access to justice
5 October 2016[32]					the case demonstrates how insufficient empirical evidence (including monitoring data) can lead to a case being denied admission to trial.
Aerial Drone Deployment on 4 October 2010 in Mir Ali/Pakistan, 3 BJs 7/12-4, 20 June 2013[33]	The Federal Attorney General at the Federal Court of Justice of Germany (Bundesgerichtshof) has decided not to initiate criminal proceedings against a complaint regarding the targeted use of a combat drone.	The attack by a combat drone on a building in Mir Ali, Pakistan; the launch of a missile from a drone against suspected members of an armed group is a classic example	Can the use of a drone to launch a missile at a building be classified as a use of armed force in a non-international armed conflict and/or a war crime? Is a German agency obligated to investigate possible war crimes if part of the operation involves foreign territory and foreign services?	The Federal Prosecutor declined to prosecute based on his assessment of the facts and applicable law; in effect, it was recognized that under the circumstances there were insufficient grounds for criminal prosecution.	Shows how the fact-finding body relies on a limited body of information about a drone strike (military secrecy, intelligence). Highlights the problem: without transparent mechanisms for registering and monitoring drone operations (which autonomous verification systems could potentially provide), victims are virtually deprived of effective access to justice.
Ramstein – Deployment of Drones, *2 BvR 508/21*, *15 July 2025*[34]	German administrative courts and the Federal Constitutional Court – Yemeni complaints against	The use of American attack drones in Yemen, relying on the infrastructure of Ramstein Air Base (signal	What is the scope of Germany's obligation to protect the right to life of individuals outside its territory if German territory or	The Supreme Administrative Court (OVG Münster) initially recognized Germany's	These decisions are critical to your topic: they demonstrate that a state hosting the infrastructure (Ramstein) may

32 *Obligations concerning Negotiations relating to Cessation of the Nuclear Arms Race and to Nuclear Disarmament (Marshall Islands v United Kingdom)* (ICJ, 5 October 2016) <https://www.icj-cij.org/case/160> accessed 6 December 2025.

33 *Aerial Drone Deployment on 4 October 2010 in Mir Ali/Pakistan (Targeted Killing in Pakistan Case)* 3 BJs 7/12-4 (BVerfG Public Prosecutor General, 20 June 2013) <https://casebook.icrc.org/case-study/germany-aerial-drone-attack-mir-alipakistan> accessed 6 December 2025.

34 *Ramstein – Deployment of Drones* 2 BvR 508/21 (BVerfG, 15 July 2025) <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2025/07/rs20250715_2bvr050821en.html> accessed 6 December 2025.

Case	Forum / Jurisdiction	Technology involved	Core procedural issue	Admissibility outcome (simplified)	Relevance for autonomous verification and access to justice
	Germany's participation in the US drone strike program via the Ramstein air base	relay, flight control, satellite channels)	infrastructure is used for drone strikes? Should Germany conduct more stringent legal assessments and oversight of US drone operations' compliance with international law?	obligation to actively review the legality of drone strikes. The Federal Administrative Court and then the Federal Constitutional Court limited this obligation: the complaints were rejected, emphasizing the government's broad discretion in the area of foreign and defense policy; the constitutional complaint was found to be unfounded.	have positive obligations to "control" the use of drones. Autonomous/algorithmic verification systems can be considered as a tool that a state must implement to fulfill this obligation of control (log collection, automatic mission registration, algorithmic auditing of compliance with IHL). From an access to justice perspective, the decisions highlight how difficult it is for victims of drone strikes to document the facts and obtain judicial redress in the absence of transparent technical verification mechanisms.
Al-Aulaqi et al v. Panetta et al, No. 1:2012cv01192, 4 April 2014[35]	United States District Court for the District of Columbia	Targeted killings using attack drones in Yemen, including US citizens (Anwar and Abdulrahman Al-Awlaki); inclusion on a "kill list" and subsequent use of drones.	Is a preliminary judicial review of a person's inclusion on a secret target-killing list possible (political question doctrine?)? The procedural standing of relatives of the deceased and the admissibility of considering claims for violation of constitutional rights	In both cases, the court dismissed the merits on the grounds of lack of standing and political question; in effect, it was established that judicial review of	These cases vividly illustrate how the secrecy and lack of transparent procedures governing drone operations deprive victims and their families of effective legal redress. Your article contrasts this with

35 *Al-Aulaqi et al v Panetta et al* no 1:2012cv01192 (US D DC, 4 April 2014) <https://dockets.justia.com/docket/district-of-columbia/dcdce/1:2012cv01192/155312> accessed 6 December 2025.

Case	Forum / Jurisdiction	Technology involved	Core procedural issue	Admissibility outcome (simplified)	Relevance for autonomous verification and access to justice
			related to drone strikes.	decisions on the use of attack drones is extremely limited.	the idea of autonomous verification: algorithmic accounting and independent auditing can reduce reliance on political discretion and strengthen procedural guarantees of fair trials.
United States v. Rezwan Ferdaus, No. 1:11-cr-10331-RGS, 1 November 2012[36]	United States District Court for the District of Massachusetts	Planning attacks on the Pentagon and the Capitol using small, remote-controlled aircraft/drones loaded with explosives and providing detonators to individuals the defendant believed to be terrorists.	Classification of the use of drones as weapons of mass destruction/dangerous weapons under anti-terrorism legislation; the scope of liability for the preparation and attempted attack using explosives delivered by drones	The defendant pleaded guilty to several charges (terrorism, attempted use of weapons of mass destruction, material support for terrorism); the court sentenced him to a lengthy prison term.	The case demonstrates that national legal systems already explicitly consider drones as explosive devices and potential weapons of mass destruction, which strengthens the argument for the need for strict control and reporting regimes for their use. For your article, it is useful as a bridge between the military and civilian dimensions: autonomous verification mechanisms can be applied not only in interstate disarmament agreements but also in the context of law enforcement to prevent the use of drones to attack critical infrastructure.

36 *United States v Rezwan Ferdaus* no 1:11-cr-10331-RGS (US D Mass, 1 November 2012) <https://www.investigativeproject.org/case/595/us-v-ferdaus-pentagon-us-capitol-plot> accessed 6 December 2025.

As explained in the Methodology section, the corpus combines treaty provisions, institutional reports, technical specifications, expert statements and case law, and the Results section draws on this mixed set of sources for cross-regime comparison.

4 DISCUSSION

The findings of this study broadly confirm the initial hypothesis that existing international law offers a necessary but incomplete framework for governing autonomous and AI-enabled technologies in nuclear disarmament verification. At the level of principle, norms on state responsibility, due diligence, weapons reviews and IHL rules on the conduct of hostilities already impose robust expectations of human control, predictability and accountability in the use of weapons systems.[37] However, when these norms are applied to verification tools such as autonomous data-collection platforms, AI-driven anomaly detection, and drone-based inspection systems, significant gaps emerge regarding evidentiary standards, the auditability of algorithmic outputs, and the allocation of responsibility for technically mediated non-compliance assessments. This result complements the ICRC's call for new legally binding rules on autonomous weapon systems and meaningful human control, while extending the analysis beyond the battlefield to the verification infrastructures that underpin nuclear disarmament regimes.[38]

Cyber resilience, spoofing, and legal responsibility. Autonomous verification drones rely on geolocation and time-stamping to link observations to treaty-relevant coordinates. Coordinate manipulation (e.g., GNSS spoofing) can produce technically "plausible" outputs while attaching them to the wrong location and/or mission context, thereby compromising the chain-of-custody and the reliability of compliance-relevant evidence. This creates a compounded attribution problem: it becomes difficult to distinguish an actual violation from a corrupted verification record, and the technical attribution of the interference itself is also complicated. From a legal perspective, this strengthens the case for 1) explicit integrity and cyber-resilience obligations in verification arrangements (tamper-evident logging, authenticated telemetry, redundancy/corroboration, incident disclosure and forensic access) and 2) procedural safeguards before autonomous outputs can trigger legal effects, including a structured opportunity to challenge both the data and the integrity of the collection process.

From the standpoint of access to justice, these gaps create uncertainty about how parties can meaningfully contest machine-generated verification findings, demand disclosure of

37 Neil Davison, 'A Legal Perspective: Autonomous Weapon Systems Under International Humanitarian Law' (2017) 30 UNODA Occasional Papers 5.

38 ICRC, 'International Committee of the Red Cross (ICRC) Position on Autonomous Weapon Systems: ICRC Position and Background Paper' (2021) 102 *International Review of the Red Cross 1335, doi:10.1017/S1816383121000564.*

underlying models and data, and obtain effective remedies when autonomous systems contribute to erroneous or discriminatory outcomes.

The case law surveyed in this article confirms that these concerns are not hypothetical. In the nuclear field, ICJ and ECtHR decisions on atmospheric testing, radiological exposure and access to information (Nuclear Tests, Nuclear Weapons, McGinley and Egan, LCB, Roche) show how evidentiary uncertainty, secrecy and limited access to technical data can shape the justiciability of claims and the availability of remedies. In parallel, constitutional and administrative litigation on armed-drone operations in Germany (Ramstein) and the United States (the Al-Aulaqi cases) illustrates both the potential and the limits of judicial review where lethal force is exercised through remote or semi-autonomous platforms and key operational information remains classified. From an access-to-justice perspective, these strands reinforce the need for verification architectures that generate auditable records, allow affected parties and courts to reconstruct critical decision points, and provide sufficiently transparent explanations of how autonomous and AI-enabled systems contributed to compliance assessments.

In comparative perspective, these findings resonate with, but also refine, earlier work on AI, autonomy and strategic stability. The SIPRI series on artificial intelligence and nuclear risk has shown that AI-enabled systems may compress decision-making timelines, introduce new escalation pathways, and complicate crisis management, especially in nuclear command, control, and communications and on advanced delivery platforms.[39] By contrast, the present study concentrates on the upstream moment in which compliance with disarmament or non-proliferation obligations is assessed, documented and, ultimately, contested. It suggests that many of the destabilising features identified in the AI/strategic-stability literature – opacity of complex models, difficulty of validating performance across contexts, and the risk of automation bias-also arise when autonomous or AI-enabled systems are embedded in verification architectures. If verification outcomes are increasingly shaped by systems whose functioning is not transparent to inspectors, diplomats or courts, the credibility of assurances and the perceived fairness of compliance procedures may be undermined even in the absence of any material breach.

The dual-use role of drones is a central illustration of this tension. Technical work by Pacific Northwest National Laboratory has demonstrated that unmanned aerial vehicles (UAVs) can significantly enhance IAEA-type safeguards through remote imaging, environmental sampling and access to hazardous or otherwise unreachable locations.[40] At the same time, policy analyses on the future of IAEA safeguards underline the importance of preserving confidence in verification conclusions and managing perceptions of politicisation or technological overreach. Parallel arms-control discussions point out that many UAV configurations have characteristics comparable to recognised delivery systems and therefore

39 Vincent Boulanin and others, *Artificial Intelligence, Strategic Stability and Nuclear Risk* (SIPRI 2020).
40 Smart and others (n 20).

raise questions about their regulation in zones free of weapons of mass destruction and their delivery vehicles.[41] Recent commentary on drone technology and the future of nuclear weapons further emphasises that AI-enabled drones may blur the line between strategic delivery platforms and ostensibly defensive or verification-oriented systems.[42] Taken together, these strands reinforce the study's conclusion that drones deployed in verification roles cannot be treated as neutral technical enablers; they must be governed as potential vectors of nuclear risk in their own right, with appropriate limits on range, payload, autonomy and data-handling functions.

The emerging normative template identified in the findings also aligns with broader civil-society and expert discourse on autonomous weapon systems. ICRC instruments, UN disarmament debates, and NGO advocacy repeatedly call for meaningful human control, limits on unpredictability, and robust legal review of new weapons, while emphasising that accountability cannot be transferred to machines. Human Rights Watch's recent report on autonomous weapons and digital decision-making adds a human rights perspective, arguing that delegating life-and-death decisions to opaque systems jeopardises rights to life, non-discrimination, and an effective remedy, and therefore warrants a legally binding instrument.[43] The present study suggests that the same normative elements-human control, transparency, predictability and access to remedy- should be systematically transposed into the design, deployment and legal assessment of autonomous or AI-enabled verification systems, including those based on drones. For courts and compliance bodies, particularly in Eastern European jurisdictions where ECHR standards (Articles 6 and 13 ECHR) structure domestic procedure, these elements translate into concrete doctrinal requirements that evidence derived from autonomous verification chains remains intelligible, contestable and accompanied by clear avenues of appeal. Doing so would help ensure that technologically sophisticated verification does not erode, but rather reinforces, the rule-of-law foundations of disarmament processes.

In practical terms, the findings indicate that future nuclear disarmament and non-proliferation arrangements should incorporate verification-specific obligations on data governance, algorithmic transparency and evidentiary treatment. Work on AI for nuclear safeguards verification by Oak Ridge National Laboratory already highlights both the promise and the risks of introducing machine-learning tools into safeguards practice, stressing the need for careful integration with existing legal and institutional standards.[44] Building on this and on NTI-sponsored analyses of the future of IAEA safeguards, states and international organizations could, for example, require: 1) pre-deployment legal-technical reviews of verification algorithms and autonomous

41 Christian Weidlich and others, 'Unmanned Aerial Vehicles: A Challenge to a WMD/DVs Free Zone in the Middle East' (2012) 8 Policy Briefs for the Middle East Conference on a WMD/DVs Free Zone 1.

42 Serim (n 10).

43 Human Rights Watch (n 8).

44 Parada Iturria and others (n 4).

platforms; 2) auditable logging of system behavior and data transformations throughout the verification chain; 3) clear rules on when and how machine-generated evidence may be used to support non-compliance findings; and 4) mechanisms for independent expert challenge and review of contested technical assessments.[45] For drones specifically, verification mandates might include explicit constraints on operational envelopes and payload configurations, integration of cybersecurity and data-protection standards, and measures to separate verification UAV fleets from systems designed or perceived as potential nuclear delivery platforms.

At the same time, several limitations of the present study must be acknowledged. First, the analysis is primarily doctrinal and policy-oriented: it relies on open-source legal instruments, technical reports, policy papers, and expert commentary, and thus cannot capture classified or state practice materials that may significantly shape how autonomous and AI-enabled systems are actually being integrated into nuclear infrastructures. Second, the coding of legal and policy documents, particularly the identification of core normative elements, necessarily involves a degree of interpretive judgement, even though it was guided by existing syntheses on AI, AWS and strategic stability.[46] Third, the study is technology-sensitive but does not undertake independent technical validation of specific algorithms, platforms or deployment concepts; its conclusions about risk and responsibility are therefore conditional on the current state of public technical knowledge, which is itself rapidly evolving. Finally, while the discussion incorporates global perspectives, it inevitably reflects the biases of the English-language literature and of debates taking place in UN and Euro-Atlantic forums.

These limitations point directly to future research needs. One priority is empirical, interdisciplinary work that brings together lawyers, computer scientists and verification practitioners to model concrete verification scenarios involving autonomous systems and drones, including stress-testing proposed standards for human control, transparency and auditability. Another is region-specific analysis of how autonomous verification tools might be perceived and regulated in different strategic environments, for example, within prospective WMD-free zones in the Middle East or in regions highlighted in SIPRI's East Asian and South Asian volumes on AI and nuclear risk.[47] Region-specific perspectives are particularly important. For example, UNIDIR's recent regional analysis of AI-driven threat perceptions in the Middle East WMD-Free Zone context illustrates how the same enabling technologies can be interpreted either as drivers of arms-racing dynamics or as potential

45 John Carlson, Vladimir Kuchinov and Thomas Shea, *The IAEA's Safeguards System as the Non-Proliferation Treaty's Verification Mechanism* (NTI Paper, Nuclear Threat Initiative 2020).

46 Boulanin (n 11); SIPRI, 'Artificial intelligence, strategic stability and nuclear risk: Euro-Atlantic perspectives – new SIPRI volume now available' *(Stockholm International Peace Research Institute (SIPRI)*, 6 May 2019) <https://www.sipri.org/news/2019/artificial-intelligence-strategic-stability-and-nuclear-risk-euro-atlantic-perspectives-new-sipri> accessed 4 December 2025.

47 Lora Saalman (ed), *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk, vol 2: East Asian Perspectives* (Policy Paper, SIPRI 2019).

facilitators of risk-reduction and verification arrangements, depending on regional security conditions and negotiating priorities.[48] A third direction is to explore how evidentiary doctrines in international and domestic courts can adapt to machine-generated verification outputs without sacrificing principles of adversarial challenge, due process and public reason-giving. Finally, as both AI and drone technologies continue to develop, longitudinal studies will be needed to track whether the integration of autonomous systems into verification practices actually enhances confidence in compliance or instead generates new forms of contestation and mistrust. The present study offers an initial legal framework for this inquiry, but sustained engagement by states, international organizations and scholars will be required to translate its proposals into operational, treaty-ready norms.

5 CONCLUSIONS

This article set out to answer a straightforward but largely neglected question: how do autonomous weapons systems, drones and other AI-enabled technologies fit into the legal framework of nuclear disarmament verification? To address it, the study used doctrinal and comparative legal methods. It systematically examined treaty law on disarmament and non-proliferation, international humanitarian and human rights law, the law of state responsibility, soft-law standards on autonomous systems and AI, state practice in multilateral forums, and selected case law on technology-generated evidence. Rather than proposing entirely new concepts, the method was to read these existing sources together and to test how far they can be stretched to govern autonomous and semi-autonomous verification tools, including drones that are technically capable of acting as nuclear delivery platforms.

The main results can be summarised quite concretely. First, current international law does reach autonomous and AI-enabled verification systems, but only in a general and fragmented way. It speaks clearly about state control, due diligence and responsibility, yet remains largely silent on how to treat machine-generated verification data as legal evidence, how to ensure its auditability, and how to allocate responsibility when automated systems influence compliance assessments. Second, drones emerge as a genuinely dual-use technology: the same classes of unmanned aerial vehicles that can greatly improve verification by extending the reach of inspections also share key technical parameters with platforms that raise proliferation and deterrence concerns. Third, across ICRC guidance, CCW debates, safeguards practice and AI-governance discussions, a fairly stable cluster of normative building blocks can be identified-meaningful human control, limits on unpredictability, transparency and explainability, data-integrity and cyber-security

48 Nasser bin Nasser, *The Impact of Artificial Intelligence on Regional Security, Threat Perceptions and the Middle East WMD-Free Zone* (UNIDIR 2025); Wenting He, *Enabling Technologies and International Security: A Compendium* (UNIDIR 2024) 5-7.

safeguards, and pre-deployment legal-technical review–even though these elements are rarely translated into detailed, verification-specific standards.

On this basis, the article's central claim can be confirmed. Existing law provides a necessary foundation, but it is not sufficient on its own to guarantee that autonomous and AI-enabled verification will be both effective and legitimate. The contribution to legal scholarship lies in three clarifications. First, it shows that the AWS debate cannot remain confined to battlefield uses: many of its core concepts, especially meaningful human control and accountability, must be carried over into the design and legal evaluation of verification chains. Second, it reframes drones used for monitoring not only as instruments of verification but also as objects that require careful legal classification due to their proximity to recognised nuclear delivery systems. Third, it organises dispersed principles from disarmament law, AI governance, and human rights practice into an integrated set of criteria that can guide future regulation of autonomous verification technologies. In this way, the study slightly shifts the state of knowledge: the problem is no longer whether law applies to such systems, but rather what additional, verification-specific standards are needed for evidence, responsibility, and the management of dual-use platforms.

The practical and forward-looking implications follow directly from this. In terms of implementation, the analysis suggests that future nuclear disarmament agreements and safeguards arrangements should move beyond technology-neutral formulations and incorporate explicit clauses on: (i) minimum requirements for human control over critical verification functions; (ii) transparency and logging of algorithmic processes that shape verification conclusions; (iii) secure and traceable handling of data produced by autonomous sensors and platforms; and (iv) the special treatment of drones whose technical characteristics bring them close to delivery systems regulated in other arms-control regimes. These elements can be developed through interpretative understandings, verification protocols, institutional review procedures and model guidelines for the design and certification of autonomous verification tools.

At the same time, the work points to clear avenues for further research and gradual implementation. Interdisciplinary projects can test proposed standards in simulated verification scenarios, helping to translate broad legal principles into technical specifications and test procedures. Regional case studies can explore how different security environments-particularly those where nuclear risks and unmanned systems are already closely intertwined- might adapt and refine these standards. Courts and compliance bodies, in turn, will need to experiment with evidentiary rules that allow for the use of machine-generated verification outputs while preserving due process and meaningful avenues for challenge. The jurisprudence reviewed in this article— from ICJ and ECtHR cases on nuclear risk and radiological exposure to domestic litigation on armed drones and algorithmic decision-support—already sketches the contours of such rules, even if it has not yet been systematically connected to the design of nuclear disarmament verification regimes. Taken together, these steps outline a realistic path for

integrating autonomous systems, drones, and AI into nuclear disarmament verification that strengthens, rather than weakens, both legal certainty and trust between states. At the same time, by embedding access-to-justice safeguards—fair-trial guarantees, robust evidentiary standards and effective remedies—into the regulation of autonomous verification, these measures can help ensure that technologically sophisticated compliance mechanisms reinforce, rather than erode, the ability of individuals and States to obtain justice in disputes over nuclear disarmament obligations.

REFERENCES

1. Abdelrahman Ibrahim A and Lim HK, 'A Deterministic Assurance Framework for Licensable Explainable AI Grid-Interactive Nuclear Control' (2025) *18*(23) *Energies* 6268, doi:10.3390/en18236268
2. Afina Y, *The Global Kaleidoscope of Military AI Governance: Decoding the 2024 Regional Consultations on Responsible AI in the Military Domain* (UNIDIR 2024)
3. Boulanin V (ed), *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*, vol 1: Euro-Atlantic Perspectives (SIPRI 2019)
4. Boulanin V and others, *Artificial Intelligence, Strategic Stability and Nuclear Risk* (SIPRI 2020)
5. Carlson J, Kuchinov V and Shea T, *The IAEA's Safeguards System as the Non-Proliferation Treaty's Verification Mechanism* (NTI Paper, Nuclear Threat Initiative 2020)
6. Chernavskikh V and Palayer J, 'Impact of Military Artificial Intelligence on Nuclear Escalation Risk' (2025) 6 SIPRI Insights on Peace and Security 1, doi:10.55163/FZIW8544
7. Davison N, 'A Legal Perspective: Autonomous Weapon Systems Under International Humanitarian Law' (2017) 30 UNODA Occasional Papers 5
8. Dokter S, 'The Role of Drones in Nuclear Safety and Security: An Overview of the Benefits and Risks of Using this Technology' (*European Technical Safety Organisations Network (ETSON)*, 11 September 2025) <https://www.etson.eu/node/429> accessed 3 December 2025
9. He W, *Enabling Technologies and International Security: A Compendium* (UNIDIR 2024)
10. Johnson S and others, *IAEA Safeguards: Preparing for the Future* (NTI 2020)
11. Le Poidevin O, 'Nations Meet at UN for Killer Robot Talks as Regulation Lags' (*Reuters*, 12 May 2025) <https://www.reuters.com/sustainability/society-equity/nations-meet-un-killer-robot-talks-regulation-lags-2025-05-12> accessed 4 December 2025
12. Nasser N, *The Impact of Artificial Intelligence on Regional Security, Threat Perceptions and the Middle East WMD-Free Zone* (UNIDIR 2025)

13. Parada Iturria FF and others, 'AI for Nuclear Safeguards Verification: ORNL Report' (*Oak Ridge National Laboratory*, November 2024) <https://www.ornl.gov/publication/ai-nuclear-safeguards-verification> accessed 3 December 2025
14. Saalman L (ed), *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk, vol 2: East Asian Perspectives* (Policy Paper, SIPRI 2019)
15. Serim E, 'Drone Technology and the Future of Nuclear Weapons' (*The Loop*, 23 July 2025) <https://theloop.ecpr.eu/advancing-drone-technology-and-the-future-of-nuclear-weapons> accessed 3 December 2025
16. Siserman-Gray C and others, 'Regulatory Challenges Related to the Use of Artificial Intelligence for IAEA Safeguards Verification' (*Institute of Nuclear Materials Management (INMM)*, 2023) <https://resources.inmm.org/annual-meeting-proceedings/regulatory-challenges-related-use-artificial-intelligence-iaea> accessed 4 December 2025
17. Smart JE and others, *Nuclear Safeguards Applications Employing Unmanned Airborne Vehicles* (PNNL-25394, Pacific Northwest National Laboratory 2016)
18. Weidlich C and others, 'Unmanned Aerial Vehicles: A Challenge to a WMD/DVs Free Zone in the Middle East' (2012) 8 Policy Briefs for the Middle East Conference on a WMD/DVs Free Zone 1

AUTHORS INFORMATION

Alibek Bolat*
Master of juridical sciences, Faculty of law and economics, Zhetysu University named after Ilyas Zhansugurov, Taldykorgan, Kazakhstan
a.bolat@zu.edu
https://orcid.org/0000-0002-7098-1305
Corresponding author, responsible for conceptualization, writing – original draft, data curation, software, supervision and writing – review & editing.

Sholpan Saimova
Ph.D. (Law), Associate Professor, Faculty of Law, Astana International University, Astana, Kazakhstan
Saimova@umto.kz
https://orcid.org/0000-0002-9000-6136
Co-author, responsible for conceptualization, methodology, resources, investigation and formal analysis and writing – review & editing.

Competing interests: No competing interests were disclosed.

Disclaimer: The authors declare that opinion and views expressed in this manuscript are free of any impact of any organizations.

RIGHTS AND PERMISSIONS

EDITORS

Assistant editor – Mag. Viktoriia Ivanova. **English Editor** – Julie Bold.
Ukrainian language Editor – Liliia Hartman.

ABOUT THIS ARTICLE

Cite this article
Bolat A and Saimova S, 'Autonomous Weapons Systems and Emerging Technologies: Legal Regulation Challenges for Nuclear Disarmament Verification' (2026) 9(1) Access to Justice in Eastern Europe 329-61 <https://doi.org/10.33327/AJEE-18-9.1-a000182>

DOI: https://doi.org/10.33327/AJEE-18-9.1-a000182

Keywords: *autonomous weapons systems, nuclear disarmament verification, emerging technologies, AI-enabled verification, meaningful human control, international legal regulation.*

DETAILS FOR PUBLICATION

Date of submission: 04 Dec 2025
Date of acceptance: 12 Jan 2026
Publication: 06 Feb 2026
Whether the manuscript was fast tracked? - No
Number of reviewer report submitted in first round: 2 reports
Number of revision rounds: 1 round with major revisions

Technical tools were used in the editorial process

Plagiarism checks - Turnitin from iThenticate
https://www.turnitin.com/products/ithenticate/
Scholastica for Peer Review
https://scholasticahq.com/law-reviews

FUNDING

This research is funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan, grant number AP 26100031

AI DISCLOSURE STATEMENT

Generative AI (ChatGPT) was utilized solely as an auxiliary tool for literature mapping, structural suggestions, and language refinement. All legal interpretations, argumentation, and conclusions were developed independently by the authors, who maintain full responsibility for the accuracy and substantive claims of the work. AI was not used to generate original findings, make policy decisions, or perform data coding; all qualitative matrices are the result of manual doctrinal analysis.

АНОТАЦІЯ УКРАЇНСЬКОЮ МОВОЮ

Дослідницька стаття

АВТОНОМНІ СИСТЕМИ ОЗБРОЄННЯ ТА НОВІТНІ ТЕХНОЛОГІЇ: ВИКЛИКИ ПРАВОВОГО РЕГУЛЮВАННЯ ПЕРЕВІРКИ ЯДЕРНОГО РОЗЗБРОЄННЯ

Алібек Болат та Шолпан Саймова

АНОТАЦІЯ

Вступ. *Автономні системи озброєння (АСО) та пов'язані з ними новітні технології дедалі частіше інтегруються в архітектуру спостереження та підтримки прийняття рішень, що мають значення для перевірки ядерного роззброєння. Ця тенденція посилює занепокоєння щодо підзвітності, людського контролю та надійності доказів, відтворених складними і непрозорими системами. Зокрема, це стосується їхнього подальшого впливу на гарантії справедливого судового розгляду, стандарти доказування та наявність ефективних засобів правового захисту, коли такі докази використовуються у судових або квазісудових провадженнях. У статті ставиться питання про те, чи чинне міжнародне право — зокрема договори про ядерне роззброєння, міжнародне гуманітарне право та загальні правила відповідальності держав — належним чином регулює процеси розгортання спроможностей на основі АСО під час перевірки, чи необхідні специфічне нормативне регулювання. Фокусуючись на процесі перевірки, а не на застосуванні на полі бою, в дослідженні висвітлюється малодосліджений аспект дискусії щодо АСО та демонструється його значення для забезпечення надійності та стійкості домовленостей про ядерне роззброєння.*

Методи: *Дослідження ґрунтується на доктринальному та порівняльно-правовому аналізі, проведеному авторами; інструменти штучного інтелекту використовувалися виключно для допоміжних завдань, таких як пошук літератури, організація матеріалів та попередній скринінг державної практики, тоді як усі правові інтерпретації та нормативні оцінки залишаються незалежною роботою дослідників. У дослідженні аналізуються договірні режими, що регулюють ядерне роззброєння та нерозповсюдження, відповідні інструменти «м'якого права» та практика міжнародних організацій, залучених до перевірки. Також порівнюються програмні документи та заяви на багатосторонніх форумах щодо летальних АСО, технологій перевірки та концепції «значущого людського контролю» з метою виявлення спільних і відмінних правових позицій та нових інтерпретаційних тенденцій.*

Результати та висновки: *Чинне міжнародне право надає необхідну, але неповну базу для регулювання перевірки за допомогою АСО. Застосовуються загальні принципи належної обачності (due diligence), застережності, пропорційності, відповідальності держав та індивідуальної кримінальної відповідальності, проте це не вирішує проблем, пов'язаних із високим рівнем автономії, алгоритмічною непрозорістю та делегуванням машинам юридично значущих рішень. Тому майбутня перевірка ядерного роззброєння повинна включати чіткі правові стандарти щодо значущого людського контролю, прозорості, можливості аудиту та управління даними для систем на основі ШІ, з чіткими правилами атрибуції та перегляду доказів, згенерованих машинами. Розробка конкретних протоколів перевірки, інтерпретаційних домовленостей та інституційного нагляду для впровадження цих стандартів посилить правову визначеність, наукову та практичну узгодженість, а також довіру до процесу перевірки. Водночас це дозволить зберегти можливість оскарження, прозорість та ефективні шляхи відшкодування у випадках, коли автономні результати стають основою для звинувачень у недотриманні зобов'язань або індивідуальній відповідальності.*

Ключові слова: *автономні системи озброєння, перевірка ядерного роззброєння, новітні технології, верифікація на основі ШІ, значущий людський контроль, міжнародно-правове регулювання.*