Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Assessing Governance Adaptation Lag and Compound Strategic Vulnerability in the IAEA Nuclear Security Architecture

Nasser Ali AlHassani

nasser.alhassani.upnm@gmail.com

National Defence University of Malaysia

Mohd Mizan

National Defence University of Malaysia

Research Article

Keywords: Nuclear Security, IAEA Governance, Adaptive Governance, Cyber-Nuclear Interface, Drone Threat, Insider Threat, Compound Strategic Vulnerability, Policy Reform, Strategic Defence Studies

Posted Date: September 2nd, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10481698/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Abstract

The threat environment governed by the International Atomic Energy Agency-led nuclear security architecture has evolved substantially across the 2010-2025 period, yet the governance instruments through which the architecture operates have adapted at a measurably slower pace than the threat environment they are designed to address. This paper investigates the structural sources of this governance adaptation lag, integrates the institutional adaptability findings with the structural coherence and enforcement capacity dimensions developed in prior analysis, and develops five reform recommendations targeted at the most accessible governance leverage points. Drawing on systematic analysis of 112 documents (treaties, IAEA Nuclear Security Series guidance, NTI Index data, scholarly literature, 2004-2025) and five semi-structured expert interviews across four professional categories, the study applies adaptive governance theory (Folke et al., 2005), exploitation-exploration framework (March, 1991), and fragmented governance theory (Biermann et al., 2012). The empirical findings document adaptation lags ranging from three to eleven years across four threat categories: nuclear cybersecurity (eleven years from Stuxnet revelation to comprehensive guidance), illicit trafficking geographic shifts (six to eight years), remote digital insider threat (three years and ongoing), and the territorial exploitation acquisition model exemplified by the Islamic State (nine years and not addressed). The paper develops the "compound strategic vulnerability" concept to denote the system-level governance failure that emerges when structural coherence limitations, enforcement gaps, and adaptation lag interact through three self-reinforcing interaction effects. Five policy recommendations are proposed: a formal performance linkage between UN Security Council Resolution 1540 reporting and IAEA Nuclear Security Series conformance; a safeguards-security information sharing protocol within the IAEA; a graduated IPPAS accountability architecture; a Rapid Nuclear Security Guidance (RNSG) protocol enabling twelve-month guidance development for emerging threats; and a Joint Adaptation Workplan trilateral arrangement among the IAEA, INTERPOL, and the UN Office of Counter-Terrorism. The recommendations are sequenced by political feasibility rather than analytical priority, with each recommendation generating governance improvement in its own right while contributing to the cumulative interruption of the compound strategic vulnerability cycle.

1. Introduction

The rate at which the global nuclear security threat environment has evolved across the 2010-2025 period has no historical parallel. The Stuxnet revelation in June 2010 demonstrated for the first time that sophisticated cyber weapons specifically targeting nuclear facility control systems had moved from theoretical concern to operational reality. The Islamic State's seizure of nuclear material from Mosul University in 2014-2015 demonstrated a new acquisition modality territorial exploitation rather than theft and transport that the existing governance framework was not designed to address. The COVID-19-driven transition to remote digital access in nuclear facility operations, documented from 2020 onward, opened insider threat vectors that did not previously exist. Commercial drone capabilities have evolved on twelve-to-eighteen-month innovation cycles to reach operational sophistication that exceeds the threat parameters assumed in much of the existing physical protection guidance. The pace and breadth

of threat evolution have placed the governance architecture under adaptation pressure of a kind that the architecture's revision processes were not designed to manage.

This paper investigates the structural sources of the governance adaptation lag that has resulted, integrates the adaptation findings with the structural coherence and enforcement capacity dimensions developed in prior analysis, and develops policy-relevant reform recommendations. Two analytical questions guide the investigation. First, what is the empirically measurable adaptation lag between threat environment evolution and governance instrument revision in the IAEA-led nuclear security architecture, and what structural sources generate this lag? Second, how do the institutional adaptability dimension's limitations interact with the structural coherence and enforcement capacity dimensions to produce the system-level governance failure pattern? Both questions are addressed empirically through systematic analysis of the governance documentary corpus (112 documents) and analytically through application of adaptive governance theory and the integrated three-dimensional framework that this study develops.

The paper proceeds as follows. Section 2 reviews the relevant theoretical literature on adaptive governance, the exploitation-exploration framework, and fragmented governance in international institutions. Section 3 specifies the research objectives. Section 4 describes the systematic methodology. Section 5 presents the findings on adaptation lag, the compound strategic vulnerability framework, and the five-recommendation reform architecture. Section 6 concludes with implications for international policymakers, the IAEA Secretariat, and future research directions.

2. Literature Review

2.1 Adaptive Governance and the Exploitation-Exploration Distinction

Folke et al. (2005) developed the adaptive governance framework to address governance challenges in complex systems where the environment being governed evolves at rates that exceed the traditional governance revision cycle. Their framework identifies four adaptive governance characteristics capacity for surprise; learning from disturbance; combining different knowledge systems; and creating opportunity for self-organisation that distinguish adaptive from non-adaptive governance regimes. The framework was developed primarily in environmental and ecological governance contexts, but has been increasingly applied to international security governance domains where threat environments evolve more rapidly than governance instruments.

March (1991) provides the complementary exploitation-exploration framework that distinguishes governance approaches that elaborate existing instruments to address marginally new challenges (exploitation) from governance approaches that develop genuinely new analytical frameworks and instruments to address fundamentally new challenges (exploration). The framework predicts that institutions facing rapid environmental change will exhibit a characteristic adaptation pattern: initial reliance on exploitation as the lower-cost response, followed by the eventual recognition that exploration is required when exploitation has been demonstrated insufficient. The transition from exploitation to

exploration is the most costly governance moment, requiring institutional resources, conceptual renovation, and political consensus that are rarely available simultaneously.

Biermann et al. (2012) extend the adaptive governance framework to fragmented international governance domains characterised by multiple parallel institutional authorities operating without integration mechanisms. Their framework predicts three pathologies in fragmented governance domains: adaptation incoherence (parallel institutions adapting independently and producing inconsistent governance approaches to common challenges); adaptation underprovision (institutions deferring adaptation responsibility to other institutions in the regime complex, with no institution accepting primary responsibility); and adaptation inertia (the political costs of cross-institutional consensus required for major adaptation slow the adaptation pace below the threshold needed to maintain governance currency).

2.2 The Cyber-Nuclear Governance Literature

The literature on cyber threats to nuclear facilities and the governance response has expanded substantially since the Stuxnet revelation. Futter (2023) provides the most comprehensive analytical assessment, documenting the governance lag pattern in international security institutions more broadly and showing that the cyber-nuclear governance interface exhibits the lag pattern in particularly acute form. The technical complexity of cyber governance (which requires both information security and operational technology expertise that few institutions possess in integrated form) and the political sensitivity of the nuclear domain (which constrains transparency about specific cyber vulnerabilities) compound to generate longer adaptation lags than would be expected for either dimension alone. The first IAEA Nuclear Security Series guidance specifically addressing computer security at nuclear facilities NSS No. 17-T was published in 2011, eleven years before the comprehensive cyber security guidance suite was completed with NSS No. 42-G in 2021.

Holloway and Ledeneva (2022) document the COVID-19-driven expansion of insider threat vectors associated with the transition to remote digital access in nuclear facility operations. Their analysis identifies a specific governance gap: the existing IAEA insider threat guidance (NSS No. 8-G) was developed when remote digital access to nuclear facility systems was either non-existent or strictly limited, and the post-2020 normalisation of remote access in many operational dimensions has not yet generated corresponding guidance updates. The institutional adaptability gap for this specific dimension is at minimum three to four years and ongoing.

2.3 The Drone Threat and Physical Protection Adaptation

Commercial drone capabilities have evolved at innovation cycles substantially faster than the IAEA Nuclear Security Series revision cycle. The drone threat to nuclear facilities including reconnaissance, payload delivery, and swarming attack modalities has been documented in scholarly and practitioner literature since approximately 2014. The first IAEA technical document specifically addressing drone-related physical protection considerations was published in 2018 (a Technical Report rather than an NSS

guidance document), with comprehensive guidance on drone intrusion governance still in development as of 2024. The five-to-eight-year adaptation lag for drone-specific physical protection guidance falls within the range documented across other threat categories but represents particularly acute governance currency loss given that commercial drone capabilities have continued to evolve during the lag period.

2.4 The Territorial Exploitation Acquisition Model

The acquisition modalities employed by terrorist organisations have evolved in ways that the existing governance framework has not yet addressed. The al-Qaeda nuclear acquisition programme (1993-2001) exemplified the centralised, well-resourced acquisition model in which terrorist organisations sought to acquire nuclear material through transactional exchanges with criminal networks or rogue state actors. The Islamic State's seizure of nuclear material from Mosul University in 2014-2015 exemplified a fundamentally different model: opportunistic territorial exploitation in which terrorist organisations exploit the breakdown of regulatory governance in conflict zones to access nuclear material directly without requiring transactional exchanges. As Stern and Berger (2015) document, the territorial exploitation model is governance-distinct from the theft-and-transport model in that it operates through the breakdown of state regulatory authority rather than through circumvention of intact regulatory authority. The IAEA's nuclear security guidance framework continues to be optimised primarily for the theft-and-transport model and does not yet specifically address governance responses to the territorial exploitation model.

2.5 Fragmented Adaptation: The Cross-Institutional Coordination Gap

The institutional architecture for nuclear security adaptation comprises multiple parallel institutions the IAEA, the UN Security Council 1540 Committee, INTERPOL, the United Nations Office of Counter-Terrorism, and (until its dormancy after 2017) the Global Initiative to Combat Nuclear Terrorism operating without an integrating coordination mechanism. The fragmented adaptation pattern that this architecture generates has been documented across the cyber-nuclear interface (where IAEA cybersecurity, 1540 Committee cybersecurity, and INTERPOL cybercrime functions adapt independently) and across the emerging-threat domain more broadly. Squassoni (2023) confirms that the consensus formation required for meaningful adaptation of binding nuclear security instruments is structurally constrained by contemporary geopolitical fragmentation, particularly the post-2022 deterioration in major-power cooperative security mechanisms.

3. Objectives

The objectives of this study were to:

i. Empirically measure the governance adaptation lag in the IAEA-led nuclear security architecture across four threat categories (cyber-nuclear interface, illicit trafficking geographic shifts, remote digital insider threat, and the territorial exploitation acquisition model);

ii. Apply adaptive governance theory (Folke et al., 2005), the exploitation-exploration framework (March, 1991), and fragmented governance theory (Biermann et al., 2012) to assess the structural sources of the documented adaptation lag;

iii. Develop the integrated three-dimensional governance assessment framework combining structural coherence, enforcement capacity, and institutional adaptability and document the system-level governance failure pattern that emerges when the three dimensions interact;

iv. Specify the three interaction effects through which the dimensions' limitations reinforce each other (compound strategic vulnerability), with quantified empirical confirmation drawn from the governance evidence base; and

v. Develop and sequence five policy recommendations targeted at the most accessible governance leverage points, with each recommendation specified for implementing authority, political feasibility, and implementation timeline.

4. Methodology

This study employed the same systematic mixed-methods qualitative research design described in the companion paper, combining structured documentary analysis of 112 governance documents (PRISMA-compliant selection, 947 to 804 to 231 to 112) with five semi-structured expert interviews across four professional categories. The methodological design followed PRISMA (Page et al., 2021) protocols for the documentary component and established expert interview standards (Tansey, 2007; Harvey, 2011) for the qualitative component.

4.1 Adaptation Lag Measurement Methodology

The institutional adaptability findings reported in this paper apply a specific methodology for measuring governance adaptation lag. For each threat category, three temporal markers are identified: first credible identification (the earliest scholarly or operational documentation of the specific threat in published or institutional sources); IAEA acknowledgement (the first institutional recognition of the threat in IAEA documents, including non-guidance documents such as Director General reports); and IAEA Nuclear Security Series guidance publication (the first NSS document specifically addressing the threat with operational guidance). The adaptation lag is calculated as the interval between first credible identification and NSS guidance publication. For threats where comprehensive guidance has not yet been published, the lag is calculated as ongoing from the first credible identification to the present.

4.2 Inter-Rater Reliability and Member Checking

The 112-document corpus was coded against a deductive coding framework comprising fourteen codes organised in three analytical dimensions, with the institutional adaptability dimension specifically comprising five codes (IA-01 through IA-05) covering threat assessment timeliness, governance revision timelines, illicit trafficking adaptation, insider threat adaptation, and emerging threat adaptation. Inter-

rater reliability for the institutional adaptability codes ranged from Cohen's kappa = 0.78 to 0.82, all within Landis and Koch's (1977) "substantial agreement" range. All five expert interview participants reviewed both their interview transcripts and the analytical findings derived from them through member checking (Birt et al., 2016).

4.3 Ethical Considerations

The study was conducted under the institutional research ethics framework of the National Defence University of Malaysia, with informed consent secured from all interview participants and confidentiality protections specifying institutional category-level identification. Ethical compliance statement: this study was conducted in accordance with the institutional research ethics guidelines of the National Defence University of Malaysia (Universiti Pertahanan Nasional Malaysia, UPNM). Under those institutional guidelines, formal ethics committee approval was not required for this non-interventional, minimal-risk study involving semi-structured interviews with professional experts speaking in their professional capacity, and the need for formal ethics committee approval was accordingly waived; no protocol number is therefore applicable. This waiver under UPNM research ethics policy was confirmed by the candidate’s main doctoral supervisor, Dr. Azrul Azlan, Faculty of Defence Studies and Management, UPNM. Freely given informed consent was obtained from all participants prior to their engagement.

5. Results and Discussion

5.1 The Governance Adaptation Lag: Empirical Findings Across Four Threat Categories

The first principal finding documents the empirically measurable governance adaptation lag across four threat categories. For the cyber-nuclear interface, the Stuxnet revelation in June 2010 established the governance need with unambiguous evidence that sophisticated state-sponsored cyber weapons specifically targeting nuclear facility control systems had been developed and deployed. The IAEA's first dedicated cyber security guidance NSS No. 17-T was published in 2011, providing initial guidance one year after the establishing event. The full NSS computer security guidance suite, including the comprehensive NSS No. 42-G, was completed in 2021 eleven years after Stuxnet. The cyber-nuclear adaptation lag was therefore one year for initial guidance and eleven years for comprehensive guidance.

For illicit trafficking, the documented geographic shift in trafficking routes toward South Asian and West African corridors was first identified in scholarly literature in approximately 2010-2012 (Zaitseva, 2021). Dedicated IAEA guidance on detection and response capabilities specifically addressing the new geographic risk distribution first appeared in the 2018-2025 Nuclear Security Plan period, generating an adaptation lag of approximately six to eight years.

For remote digital insider threats, the COVID-19-driven expansion of remote digital access in nuclear facility operations was documented from 2020-2021 onward (Holloway and Ledeneva, 2022). As of 2024, dedicated IAEA Nuclear Security Series guidance specifically addressing remote digital access

insider threats had not yet been published, though the issue is included in the current NSS revision workplan. The adaptation lag for this dimension is at minimum three to four years and ongoing.

For the territorial exploitation acquisition model, the Islamic State's seizure of nuclear material at Mosul University was documented in scholarly literature beginning in 2015 (Stern and Berger, 2015). As of 2024, the IAEA's nuclear security guidance framework does not specifically address governance responses to the territorial exploitation model distinct from the theft-and-transport acquisition model. The adaptation lag for this dimension is approximately nine years and ongoing, with no published timetable for guidance development.

The expert interview evidence reinforced the analytical significance of these adaptation lags. A Category D participant (technical policy expert with cybersecurity expertise) observed that "cyber capabilities provide new dimensions of risk because adversaries can ignore physical barriers entirely and still attack the target. With cyber intrusions, attackers can manipulate monitoring systems, disrupt operations, and exploit weaknesses in digital infrastructure without being physically present. That changes the threat surface fundamentally, and the governance framework has been slow to recognise it." A Category B participant (senior military strategist) reinforced the operational dimension: "Pre-positioned cyber access can disable security before any physical move is made adversaries can install malware or backdoors into facility networks long before an attack happens. By integrating pre-staged cyber access with secondary physical action, this hybrid modality dramatically increases the threat envelope."

5.2 The Structural Sources of the Adaptation Lag

The adaptation lag findings are not random across threat categories. Three structural sources generate the pattern. First, the IAEA Nuclear Security Series revision cycle is structurally slow: the consultation, drafting, member state review, and consensus formation process typically requires five to seven years from the identification of a guidance need to the publication of a finalised document. This pace mismatch with twelve-to-eighteen-month commercial technology innovation cycles (drones, AI, cyber tooling) is the operational source of the governance currency loss.

Second, the architecture's fragmentation across multiple parallel institutions (IAEA, 1540 Committee, INTERPOL, UNOCT) generates adaptation underprovision: when no institution holds primary responsibility for adaptation in an emerging threat domain, the adaptation gap persists because each institution defers to the others. The cyber-nuclear interface exhibits this pattern in particularly acute form, with three parallel cybersecurity governance streams (IAEA cybersecurity, 1540 Committee cybersecurity, GICNT digital detection) developing independently and producing boundary inconsistencies that compound the original governance gap.

Third, the geopolitical environment for international consensus on binding governance instruments has deteriorated substantially across the study period. The post-2022 collapse of major-power cooperative security mechanisms has constrained the consensus formation required for major adaptation of binding instruments to a degree that the 2010-2021 period did not exhibit. Squassoni (2023) confirms that this

geopolitical constraint is structural rather than cyclical: meaningful adaptation of binding nuclear security instruments requires consensus that contemporary great-power competition systematically prevents.

5.3 The Compound Strategic Vulnerability Framework

The integration of the institutional adaptability findings with the structural coherence and enforcement capacity findings developed in companion analysis produces what this study terms the compound strategic vulnerability (CSV) framework. The CSV framework specifies that the IAEA-led nuclear security architecture's governance failure operates not as the additive sum of three separate dimensional weaknesses but as the multiplicative interaction of three dimensions whose limitations amplify rather than compensate for each other.

Three interaction effects constitute the CSV. Interaction Effect 1 Structural Coherence Undermining Enforcement Capacity: the compliance facade problem (the gap between formal legal compliance and substantive performance) creates an environment in which IAEA technical assistance can be directed toward formal compliance improvement rather than substantive performance improvement, because the structural coherence gap allows the former to substitute for the latter. The empirical measurement of this effect is the 12-percentage-point gap between CPPNM Amendment ratification rate (80 per cent of relevant states) and IPPAS hosting rate (68 per cent of relevant states): the most accessible accountability mechanism is satisfied at substantially higher rates than the most demanding accountability mechanism.

Interaction Effect 2 Enforcement Capacity Limitations Reducing Adaptation Incentives: the absence of operational consequences for persistent governance gaps removes the primary incentive for state engagement with governance adaptation processes. States facing no meaningful accountability for maintaining outdated physical protection systems have reduced incentive to participate in NSS revision processes, host follow-up IPPAS missions, or invest in regulatory capacity development. The empirical measurement of this effect is the 42-percentage-point gap between initial IPPAS mission completion and follow-up mission completion: states that engage IPPAS at the most visible stage do not follow through to the stage that requires demonstrating adaptation implementation.

Interaction Effect 3 Fragmented Adaptation Creating New Coherence Problems: the three parallel digital security governance streams independently adapt to the digital security challenge in ways that produce boundary gaps at their institutional interfaces gaps that correspond precisely to the normative inconsistency patterns documented in the structural coherence assessment. This dynamic creates a self-reinforcing coherence degradation cycle: existing structural incoherence reduces governance effectiveness, which weakens enforcement incentives for adaptation, which generates fragmented adaptation when it occurs, which creates new structural incoherence.

The system-level governance diagnosis that the three confirmed interaction effects generate is specific: the IAEA nuclear security governance framework's underperformance is not primarily a function of

inadequate technical standards (the NSS is technically comprehensive), inadequate assistance capacity (the IAEA's nuclear security programme is well-resourced), or inadequate state capability in technically capable states (IAEA assistance is effective for capacity-limited non-compliance). It is primarily a function of the structural interdependencies among governance dimensions that generate a self-reinforcing weakness cycle. The governance system is not in stable equilibrium at a suboptimal performance level; it is in a deteriorating trajectory unless a systemic intervention interrupts the degradation cycle.

5.4 Five Policy Recommendations

The five reform recommendations developed in this study are not five separate ideas; they are a coordinated package designed to interrupt the equilibrium trap at multiple points simultaneously, with each recommendation targeting one or more of the three confirmed interaction effects.

Recommendation 1: Create a Formal NSS-1540 Performance Linkage. The 1540 Committee should develop supplementary implementation guidance specifying that comprehensive national implementation reports include as a standard reporting element reference to the state's most recent IPPAS mission findings and its status of implementation of IPPAS recommendations. The element would not be mandatory in the formal legal sense, but its inclusion as a standard reporting element would create a soft accountability norm: states that have not hosted IPPAS missions would be expected to explain what alternative mechanisms they have used to assess their nuclear security framework against IAEA NSS standards. The reform addresses Interaction Effect 1 by closing the structural coherence gap between formal legal compliance and substantive governance performance. Political feasibility is moderate; implementation timeline is medium-term (three to five years).

Recommendation 2: Establish a Formal IAEA Safeguards-Security Information Sharing Protocol. The IAEA Director General should establish a formal cross-functional information sharing protocol between the safeguards function (which has independent verification authority) and the nuclear security function (which lacks it). The protocol would enable security-relevant information generated through safeguards inspection to inform security governance assessment, while protecting the independence of the safeguards function from security governance pressures that could compromise its non-proliferation mandate. The reform addresses the SC-03 internal IAEA boundary condition and supports reduction of Interaction Effect 1. Political feasibility is high (within DG existing authority); implementation timeline is near-term (one to two years).

Recommendation 3: Develop a Graduated IPPAS Accountability Architecture. The IAEA Board of Governors should establish a three-tier IPPAS framework differentiated by accountability intensity. Tier 1 (current standard IPPAS) would remain available for states seeking technical engagement without accountability commitments. Tier 2 would add follow-up mission requirements with specified implementation timelines for accepted recommendations. Tier 3 would add public reporting of follow-up mission findings. States would self-select their tier of engagement, with progressive accountability for states whose engagement remains at Tier 1 despite extended programme participation. The reform

addresses Interaction Effect 2 by introducing oversight functionality without requiring the litigation mechanism Member States have resisted. Political feasibility is medium (Board precedent supports incremental reform); implementation timeline is near-term (two to three years).

Recommendation 4: Establish a Rapid Nuclear Security Guidance (RNSG) Protocol. The IAEA Director General's Office should establish an expedited twelve-month guidance development track for emerging threats requiring rapid governance response. The RNSG track would operate within existing NSS authority but with abbreviated consultation requirements, designated rapid-response drafting teams, and an explicit understanding that RNSG documents represent provisional guidance subject to subsequent comprehensive revision. The reform addresses Interaction Effect 3 by closing the adaptation lag at its operational source the structural slowness of the standard NSS revision cycle. Political feasibility is high (administrative reform within DG authority); implementation timeline is near-term (one to two years).

Recommendation 5: Establish a Joint Nuclear Security Governance Adaptation Workplan (JAWP). The IAEA, INTERPOL, and the UN Office of Counter-Terrorism should establish a trilateral coordinating mechanism the Joint Adaptation Workplan to address fragmented adaptation across the three institutions' overlapping mandates. The JAWP would not require formal institutional restructuring; it would establish a coordinating committee with secretariat support, a shared emerging-threat monitoring capacity, and a coordinated guidance development planning process. The reform addresses Interaction Effect 3 by addressing fragmented adaptation at the cross-institutional level. Political feasibility is low (requires P5 consensus on geopolitical cooperation); implementation timeline is long-term (five-plus years).

5.5 Recommendation Sequencing and Implementation Architecture

The five recommendations are sequenced by political feasibility rather than analytical priority. Recommendations 2 and 4 both within the IAEA Director General's existing authority are the most immediately achievable and would generate measurable governance improvement on shorter timescales. Recommendation 3 falls within the IAEA Board of Governors' standard reform authority. Recommendation 1 requires UN Security Council 1540 Committee action and is feasible in soft-norm form but requires P5 consensus for binding form. Recommendation 5 is the most ambitious and depends on broader geopolitical conditions for cross-institutional cooperation. The package is designed so that partial implementation of the lower-feasibility recommendations does not undermine the governance value of the more achievable recommendations: each recommendation generates governance improvement in its own right while contributing to the cumulative compound strategic vulnerability interruption that complete implementation would achieve.

6. Conclusion

This paper has documented the governance adaptation lag in the IAEA-led nuclear security architecture across four threat categories (cyber-nuclear interface: eleven years; trafficking route shifts: six to eight years; remote digital insider threat: three years and ongoing; territorial exploitation acquisition model:

nine years and ongoing), identified three structural sources of the lag (revision cycle slowness, fragmented adaptation, geopolitical consensus constraints), and developed the compound strategic vulnerability framework as the system-level diagnosis of the IAEA nuclear security architecture's governance failure pattern. Five policy recommendations have been developed targeting the most accessible reform leverage points, sequenced by political feasibility, and designed as a coordinated package that interrupts the compound strategic vulnerability cycle at multiple points simultaneously.

The findings have direct implications for international policymakers. The compound strategic vulnerability is not a permanent feature of international nuclear security governance; it is the result of specific institutional design choices and specific gaps in mechanism deployment, both of which can be addressed within the scope of existing institutional authorities. Recommendations 2 and 4 in particular the safeguards-security information sharing protocol and the Rapid Nuclear Security Guidance protocol are achievable within the IAEA Director General's existing authority and would generate measurable governance improvement within near-term implementation timelines. Their implementation does not require Member State consensus, treaty renegotiation, or Security Council action, and would establish institutional precedent for the more politically demanding reforms that the compound strategic vulnerability ultimately requires for full interruption.

Future research should investigate three priorities: first, the comparative assessment of governance adaptation patterns in adjacent international security domains (the Chemical Weapons Convention's rapid revision response to the Syria chemical weapons crisis; the World Health Organization's pandemic preparedness governance evolution post-COVID-19) to identify transferable design features; second, the development of measurement frameworks for the compound strategic vulnerability that enable empirical assessment of governance reform effectiveness; and third, the political economy of nuclear security reform in conditions of contemporary great-power competition, including the conditions under which Member States have accepted incremental governance accountability strengthening despite broader geopolitical resistance to multilateral cooperation.

Declarations

Funding: The authors declare that no funding was received for conducting this study.

Clinical trial number: not applicable.

Data availability

The datasets generated and/or analysed during the current study are not publicly available due to the confidentiality protections applying to expert interview transcripts but are available from the corresponding author on reasonable request. The documentary corpus analysed in this study consists of publicly available treaty texts, IAEA publications, and published scholarly literature, all of which are cited in the reference list.

Ethical Approval and accordance

In accordance with the institutional guidelines of the National Defence University of Malaysia (UPNM), formal ethics committee approval was not required for this study, which involved non-interventional, minimal-risk semi-structured interviews with professional experts speaking in their professional capacity. The research was carried out in accordance with those institutional guidelines, and freely given informed consent was obtained from all participants prior to their engagement.

Consent to participate

Freely given, informed consent to participate in the study was obtained from all interview participants prior to their engagement. All participants were adults and professional experts participating in their professional capacity.

Consent to publish

Informed consent to publish was obtained from all interview participants. No identifying personal information is included in this manuscript; all interview material is presented in anonymised form.

References

1. Biermann, F., Pattberg, P., & van Asselt, H. (2012). The fragmentation of global governance architectures. *Global Environmental Politics*, 9(4), 14-40.
2. Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research*, 26(13), 1802-1811.
3. Bunn, M. (2006). Securing the bomb 2006. Project on Managing the Atom, Belfer Center for Science and International Affairs.
4. Folke, C., Hahn, T., Olsson, P., & Norberg, J. (2005). Adaptive governance of social-ecological systems. *Annual Review of Environment and Resources*, 30, 441-473.
5. Futter, A. (2023). *Hacking the bomb: Cyber threats and nuclear weapons*. Georgetown University Press.
6. Harvey, W. S. (2011). Strategies for conducting elite interviews. *Qualitative Research*, 11(4), 431-441.
7. Holloway, D., & Ledeneva, A. (2022). Insider threats in nuclear security: Lessons from the COVID-19 transition. *Nonproliferation Review*, 29(3), 215-238.
8. International Atomic Energy Agency. (2021). *Computer security at nuclear facilities (NSS No. 17-T)*. IAEA.
9. International Atomic Energy Agency. (2025). *Nuclear security report 2025*. IAEA.
10. Kroenig, M., & Volpe, T. (2015). 3-D printing the bomb? The nuclear non-proliferation challenge. *The Washington Quarterly*, 38(3), 7-19.

11. Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, 33(1), 159-174.
12. March, J. G. (1991). Exploration and exploitation in organizational learning. *Organization Science*, 2(1), 71-87.
13. Nuclear Threat Initiative. (2023). *NTI nuclear security index: Building a framework for assurance, accountability, and action*. NTI.
14. Page, M. J., McKenzie, J. E., Bossuyt, P. M., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71.
15. Squassoni, S. (2023). Geopolitical fragmentation and nuclear security governance: The post-2022 collapse of major-power cooperative security mechanisms. *Bulletin of the Atomic Scientists*, 79(4), 232-245.
16. Stern, J., & Berger, J. M. (2015). *ISIS: The state of terror*. HarperCollins.
17. Tansey, O. (2007). Process tracing and elite interviewing: A case for non-probability sampling. *PS: Political Science & Politics*, 40(4), 765-772.
18. Zaitseva, L. (2021). Illicit trafficking of nuclear and radioactive materials: Patterns, networks, and governance responses. *Nonproliferation Review*, 28(2), 173-193.