

WHITE PAPER

Nuclear Piracy

Weaponization of Nuclear Facilities

Ali Alkis

2025 NUCLEAR FUTURES FELLOW

Junior Affiliated Fellow, NATO Defense College

PhD Candidate, Hacettepe University

Ali Alkis is a nuclear security professional and PhD candidate based in Türkiye. He is a Junior Associate Fellow at the NATO Defense College, one of NTI's Emerging Nuclear Security Leaders, Secretary General of BSWN, and a member of Harvard's Ukraine Nuclear Security Working Group. His research focuses on nuclear policy, nonproliferation, nuclear piracy, and Türkiye's security landscape. In August 2026, he received the Institute of Nuclear Materials Management (INMM) Early Career Award in recognition of his early contributions to the field of nuclear security and nonproliferation. This paper serves as the capstone project of his Ploughshares–Horizon 2045 Nuclear Futures Fellowship and builds on his wider research and public outreach on nuclear security.

Acknowledgements

The author gratefully acknowledges BSWN, the host institution, for supporting his participation in the fellowship. He extends his sincere appreciation to the experts interviewed for this paper, listed alphabetically by first name: Aybars Gürpınar, Dmitry Kovchegin, Elena Sokova, Geoff McCabe, George Foster, Jasmine Auda, Laura Holgate, Mariana Budjeryn, Robert Budnitz, Scott Roecker, Stephen Herzog, Tatsujiro Suzuki, Trevor Findlay, and Vitaly Fedchenko. Their time, expertise, candid insights, and professional exchanges substantially enriched the analysis. The author is especially grateful to Anne Harrington, Jasmine Auda, Jennie Gromoll, and Trevor Findlay for their thoughtful peer review, careful reading, and constructive recommendations, which strengthened the paper's arguments and clarity. He also thanks Erika Gregory and Habib Bako for their encouragement, guidance, and steadfast support throughout the fellowship. Special thanks are due to Alex Hall for her exceptional guidance throughout the project. Her strategic perspective, intellectual generosity, meticulous attention to detail, and consistently thoughtful feedback helped sharpen the paper's arguments, improve its clarity, and connect the research more effectively to the fellowship's wider mission and policy priorities.

Any errors or omissions remain the author's own. The views expressed are those of the author alone.

Table of Contents

Acknowledgements	2
Table of Contents	0
Executive Summary	1
1. Introduction.....	2
2. Tactical Realities and Disruptive Technologies	7
I. Military Occupation Beyond the Design Basis Threat (DBT)	7
II. The Proxy Threat and the “Wagner Loophole”	8
III. Asymmetric Drone Warfare and Grid Vulnerability	9
IV. Implementing the “Disruptive Technology” Lever	11
3. Strategic Impacts, Insider Threats, and the “Uninsurable” Atom.....	11
I. The Staffing Trap and Accelerated Degradation Under Duress	11
II. Military Occupation Beyond the Traditional Insider-Threat Model	12
III. The Uninsurable Atom and Macroeconomic Fallout.....	13
4. The Governance Void and Eroding Legal Norms	14
I. The Statutory Gap in Relation to Nuclear Security.....	14
II. Improvisational Diplomacy: The ISAMZ Precedent	15
III. Board Paralysis and Global South Positions	16
IV. Institutional Paralysis and Broader Normative Decay.....	17
V. The Strategic Necessity of Legal Evolution	18
5. Opportunities for Action: The 2045 Horizon	19
I. Policy Recommendation 1: Regional Non-Attack Treaties (Legal Lever)	22
II. Policy Recommendation 2: Economic “Security-by-Design” (Technology Lever)	24
III. Policy Recommendation 3: Reframing Nuclear Piracy (Conceptual Model Lever).....	26
Conclusion	27

Executive Summary

This paper analyzes a consequential shift in the global nuclear security environment: civilian nuclear infrastructure is no longer only at risk of becoming collateral damage in armed conflict, but may also be exploited as an instrument of state-level coercion. The phenomenon described here as “**nuclear piracy**” captures the strategic risk that arises when an adversary state occupies a civilian nuclear power plant and uses the facility as a radiological shield or source of coercive leverage. Although attacks on nuclear facilities are not unprecedented, damage to an operating reactor or its essential support systems could cause a severe radiological release with transboundary human, environmental, and economic consequences, while their occupation and weaponization expose a critical gap in a security framework designed primarily around non-state threats.

This mismatch between contemporary security realities and existing response mechanisms has become increasingly consequential. Recent state-to-state armed conflicts have exposed, in concrete operational terms, how a framework designed primarily to counter non-state threats is ill-equipped to address the deliberate targeting, occupation, weaponization, and exploitation of civilian nuclear infrastructure by states. Protecting nuclear facilities during armed conflict is therefore no longer a hypothetical concern, but an urgent policy and security challenge that the international community must address.

The paper argues that the absence of credible state-level deterrents could increase the risk that nuclear piracy becomes incorporated into military doctrine. Such a possibility would have strong negative implications for the post-World War II nuclear order and further entrench “War 3.0,”¹ characterized by hybrid operations, infrastructure coercion, and attacks on critical civilian systems.

Key takeaways:

- **Strategic aims, not terrorism:** Unlike acts of nuclear terrorism, such as the theft of materials or sabotage by non-state actors, nuclear piracy refers to the occupation and coercive control of nuclear facilities to serve strategic aims in state-to-state conflict.

¹ According to the Horizon 2045 Foresight Radar, the “War 3.0” driver describes a future where the scale and scope of conflicts are shifting, making it difficult to differentiate between proxy and hybrid (digital/physical) conflicts. This new era of warfare is characterized by the rise of disinformation, drone swarms, attacks on critical infrastructure, autonomous weapons systems, and an overall increase in military budgets.

- **The hybrid readiness gap:** Russia’s occupation of the Zaporizhzhia Nuclear Power Plant (ZNPP) exposed a hybrid operational model in which invading forces secured the site and specialized *Rosgvardia* units later assumed control. Whether this reflected prior planning or opportunistic adaptation, the case revealed how a civilian nuclear facility can be folded into military coercion.
- **Operational and human degradation:** Technical safety measures are not designed to operate under prolonged armed occupation. At ZNPP, a reduced workforce has been forced to manage complex maintenance cycles under extreme military and psychological duress.
- **The governance void and the fog of attribution:** The International Atomic Energy Agency (IAEA) presence on the ground is essential, but the Agency currently lacks the statutory mandate and operational capabilities to enforce security or attribute acts to perpetrators.

Drawing on the foresight framework used in the Ploughshares–Horizon 2045 Nuclear Futures Fellowship, the paper adopts 2045 as its analytical horizon. This lens places nuclear piracy within interconnected shifts in governance, technology, infrastructure, and warfare and supports the mapping of three possible futures:

1. **Status Quo (Drift)**, in which gray-zone occupations remain unresolved anomalies;
2. **Normalization (The Broken Atom)**, in which state occupation of nuclear sites becomes a more routine instrument of coercion;
3. **Strategic Resilience**, in which governments, international institutions, and industry strengthen legal commitments, harden facilities, and improve crisis preparedness.

1. Introduction

The international nuclear security framework is being challenged by a significant normative and strategic shift. This challenge has exposed vulnerabilities in an international framework designed for a different threat environment. In the early nuclear era, the primary concern was state-espionage and the theft of nuclear materials or technology by states. By the 1970s, attention shifted toward the risks posed by non-state actors, particularly the theft of nuclear material and sabotage of nuclear facilities by terrorist groups. The dissolution of the Soviet Union increased concerns over illicit trafficking and the security of “loose nukes.” Following the 9/11 terrorist attacks, threat

perceptions resulted in the development of a more comprehensive international nuclear security regime against nuclear terrorism.²

However, this regime remains rooted in assumptions and institutional logics shaped by earlier threat perceptions. As a result, there is a widening gap between contemporary security realities and the mechanisms intended to address them. More recent state-to-state armed conflicts—especially the Russia–Ukraine war and the Israeli and U.S. attacks on Iranian nuclear facilities—have further exposed these limitations, demonstrating that a framework designed to counter non-state threats is ill-equipped to address the deliberate occupation, militarization, and exploitation of civilian nuclear infrastructure by state actors.

The paper uses the term “nuclear piracy” to describe the deliberate seizure, occupation, or coercive exploitation of a sovereign civilian nuclear facility by a state or state-backed actor for strategic leverage.³ The concept includes using a nuclear installation as a radiological shield, as a source of radiological compellence, or as a tool of broader geopolitical coercion. Although debate continues over terminology, some scholars and policymakers still describe the phenomenon as “nuclear terrorism,” or describe it as “state terrorism,” or “nuclear security 2.0.” Yet, as Mariana Budjeryn (MIT) argues, “terms such as nuclear terrorism do not do justice to the kind of violations and the kind of infringement that happened at the occupation and takeover of Zaporizhzhia NPP.”⁴ This paper therefore uses “nuclear piracy” as a normative and analytical term rather than a strict legal category. Although international lawyers may resist the term because “there is a legal definition of piracy,” the occupation of nuclear facilities is so far beyond ordinary expectations that, as Laura Holgate (former US Ambassador) rightly points out, we may need to “borrow concepts and language from other domains to describe it more accurately.”⁵ This shift also requires reframing the issue conceptually. The emerging threat, therefore, should be understood primarily as a nuclear security problem, not solely as a matter of conventional armed conflict.⁶

² Muhammed Ali Alkış, “Non-Western approach to nuclear security.” *Journal of Radiation Research and Applied Sciences* 16, no. 2 (2023/06/01/ 2023): 100535. <https://doi.org/10.1016/j.jrras.2023.100535>

³ Muhammed Ali Alkış and Bethany Goldblum, “Lessons from Zaporizhzhia: How to protect reactors against ‘nuclear piracy’.” *Bulletin of the Atomic Scientists* (2023). <https://thebulletin.org/2023/09/lessons-from-zaporizhzhia-how-to-protect-reactors-against-nuclear-piracy/>.

⁴ Mariana Budjeryn, interview by Muhammed Ali Alkış, *Nuclear Futures Fellowship Capstone Project*, 22 January 2026.

⁵ Laura Holgate, interview by Muhammed Ali Alkış, *Nuclear Futures Fellowship Capstone Project*, 19 March 2026.

⁶ Scott Roecker, interview by Muhammed Ali Alkış, *Nuclear Futures Fellowship Capstone Project*, 23 January 2026.

At first glance, this may appear to be a semantic shift. Yet it carries important normative implications. Under classical international law, piracy was declared *hostis humani generis*—an enemy of all humankind—not merely because of where it occurred, but because it represented an indiscriminate threat to global commerce and shared security that any state could exercise universal jurisdiction to suppress. This paper uses “nuclear piracy” as a normative analogy rather than a strict legal equivalence. By intentionally risking a transboundary radiological disaster, a state that weaponizes a captured reactor transcends bilateral conflict. It generates an indiscriminate risk to neighboring states and the global environment, mirroring the universal threat profile that originally justified the *hostis humani generis* designation.

The emergence of state-level threats to civilian nuclear facilities is a strong sign of the broader vulnerability of critical infrastructure. While governments consider expanding nuclear power to meet climate goals and strengthen energy security, this expansion intersects with the evolution of modern conflict—often characterized as “War 3.0”—which includes hybrid and asymmetric military tactics. As disruptions to critical infrastructure can trigger cascading public health, economic, and political emergencies, complex civilian energy assets are increasingly exposed to coercive targeting. The growing number of nuclear facilities across potentially volatile regions tests the limits of traditional security paradigms that rely on localized guard forces and fixed design basis threats (DBTs). Civilian nuclear infrastructure is no longer only a domestic energy asset; it has become a strategic vulnerability that adversarial states may exploit to achieve outsized geopolitical effects and regional paralysis without crossing the threshold into direct nuclear weapons use.

To understand the contemporary landscape of nuclear facility weaponization, it is necessary to distinguish between two principal models of state-level intervention: the historical “Begin Doctrine” and the emergent Russian Hybrid Model. Traditionally, state-on-state attacks against nuclear facilities were grounded in the Begin Doctrine, named after former Israeli Prime Minister Menachem Begin. The doctrine holds that Israel may undertake preventive military action to prevent an adversarial state from acquiring nuclear weapons capabilities. This counter-proliferation logic was established by Israel’s 1981 airstrike against Iraq’s Osirak reactor and later re-applied through the 2007 destruction of Syria’s Al Kibar reactor.

Similar preventive logics have also shaped repeated covert and kinetic operations targeting elements of Iran’s nuclear program, including facilities at Natanz, Fordow, Isfahan, and Parchin. During the Iran–Iraq War, Iraq also repeatedly bombed Iran’s Bushehr nuclear power plant, although these attacks occurred within the broader context of interstate warfare rather than a strict counter-proliferation doctrine. Similarly, during the breakup of Yugoslavia, military activities within the vicinity of the Krško Nuclear Power Plant raised concerns about the security and governance of the

facility, suggesting how political fragmentation and armed instability can endanger the safe and secure operation of nuclear facilities even without direct military targeting.⁷

This preventive logic can destabilize regional security architectures, particularly in the Middle East. As Jasmine Auda (Ambit Advisory) notes, Israel remains the “big elephant in the room” regarding infrastructure attacks; regional states feel they “can’t have a meaningful, really honest, credible conversation about anything so long as we have an undeclared nuclear power in the region.”⁸ Because the international community has often failed to condemn past preventive strikes, emerging nuclear states in the Middle East may lack sufficient confidence that their civilian infrastructure will not be unilaterally targeted. Although there are currently no active threats reported in local media against newer facilities such as Egypt’s El Dabaa, the broader precedent leaves the region vulnerable to asymmetric compellence.

By contrast, the Russian Hybrid Model shifts the strategic objective from preventive destruction to active compellence through military occupation. The occupation of the ZNPP exemplifies this emerging risk. Although the initial stages of Russia’s broader invasion of Ukraine reflected poor planning and strategic improvisation, the operation to capture ZNPP appears to have involved a notable degree of operational readiness. The integration of specialized *Rosgvardia* units—forces trained for the physical security of nuclear facilities—into the occupation structure suggests that the seizure and subsequent management of the plant was a pre-planned operational objective.⁹

A narrower interpretation, however, is also possible. *Rosgvardia*’s presence at ZNPP was consistent with Russia’s domestic practices for protecting nuclear installations and therefore does not, by itself, prove that the plant’s seizure was planned before the invasion. The IAEA subsequently reported the presence of *Rosgvardia* troops at the site.¹⁰ This evidence supports the conclusion that specialized forces were integrated into the occupation structure, but it cannot conclusively distinguish advance planning from rapid operational adaptation after the plant was captured. Yet whether the occupation was a calculated pre-war objective or a dangerous improvisation in which military forces captured and exploited civilian assets opportunistically, the strategic outcome is the same. In this hybrid model, the aggressor does not seek to destroy the

⁷ Darya Dolzikova, *Nuclear Facilities as Targets of Military Attack*. London: Royal United Services Institute, 2025.

⁸ Jasmine Auda, interview by Muhammed Ali Alkış, *Nuclear Futures Fellowship Capstone Project*, 22 January 2026.

⁹ Budjeryn, interview.

¹⁰ IAEA, *Nuclear Safety, Security and Safeguards in Ukraine*, Vienna: International Atomic Energy Agency, 2023, https://www.iaea.org/sites/default/files/documents/gov2023-59_8.pdf.

facility to prevent proliferation; it seeks to capture a peaceful asset and harness its disruptive potential as an instrument of statecraft.

By establishing physical control over a complex, high-consequence asset, an occupying state can transform the facility into a “radiological shield.” The operational logic of military occupation rests on nuclear brinkmanship. The occupying force embeds military assets within or near civilian infrastructure, betting that the opponent’s military—and the broader international community—will avoid actions that could risk catastrophic consequences near critical reactor components. This was demonstrated when Ukrainian national guardsmen ceased defensive fire upon realizing that advancing Russian military forces were not deterred by the prospect of heavy weaponry detonating near critical reactor systems. The facility itself becomes a hostage, neutralizing the defending state’s conventional military options, complicating rules of engagement, and paralyzing international response mechanisms.

This dynamic changes the parameters of strategic compellence. The aggressor acquires the coercive leverage typically associated with nuclear weapons without facing the immediate geopolitical, normative, or military retaliation that would inevitably follow an actual nuclear detonation. As Stephen Herzog (James Martin Center for Nonproliferation Studies) observes, “what occupying a nuclear power plant does is to take the abstract threat of nuclear coercion and literally put it on someone’s territory close to their cities, [where] you can see the physical manifestations; it is a new way of reconfiguring compellence with nuclear weapons.”¹¹

The emergence of nuclear piracy also requires a reassessment of international humanitarian law (IHL). Although Article 56 of Additional Protocol I to the Geneva Conventions establishes a limited prohibition of attacks against nuclear electrical generating stations, the occupation of Zaporizhzhia exposes a gap between prohibition and enforcement. The rule helps articulate what should not happen, but it offers no practical mechanism to prevent a state from seizing a facility, militarizing it, and then using the radiological risks surrounding it to constrain the defender’s response. In practice, the occupying force can exploit the defending state’s legal and political caution while benefiting from the very dangers the law was meant to contain.

¹¹ Stephen Herzog, interview by Muhammed Ali Alkış, *Nuclear Futures Fellowship Capstone Project*, 27 February 2026.

2. Tactical Realities and Disruptive Technologies

I. Military Occupation Beyond the Design Basis Threat (DBT)

The global nuclear security architecture is designed around a foundational regulatory concept—the DBT. The DBT serves as the fundamental baseline defining the physical protection requirements and security measures for civilian nuclear power plants.

Traditionally, most DBT models have been designed around threats such as sabotage, terrorism, and small-scale armed assault by non-state actors. These include scenarios involving a small group of highly motivated but lightly armed terrorists or saboteurs attempting to breach perimeter fences, bypass access control systems, or infiltrate vital areas. For instance, prior to the Russian invasion, the standard DBT for Ukrainian facilities was modeled against an assault by approximately 14 heavily armed terrorists equipped with light armored vehicles and rocket-propelled grenades.¹² Consequently, the defensive architecture relies heavily on commercial guard forces, layered physical barriers, and tactical delay mechanisms designed to stall attackers just long enough for off-site law enforcement or specialized response teams to arrive.

Nuclear piracy falls outside this traditional paradigm. The central flaw in applying the DBT to state actors is that the concept belongs to nuclear security, not military planning. As Dmitry Kovchegin (independent researcher) points out, an invading military planner is not constrained by site-level threat assumptions; the objective is embedded within the broader strategic defense and offense of the state.¹³ When thousands of regular combat troops, armored vehicles, and supporting units confront a commercial nuclear facility, perimeter defenses designed for terrorist intrusion become functionally obsolete within minutes.¹⁴

This capability mismatch alters the operational reality on the ground. When facing a state actor, security no longer relies on physical site denial; rather, the site's survival depends on the aggressor's political calculations and their fear of initiating a transboundary radiological disaster. As Geoff McCabe (NB Power) points out regarding the stark reality of military overmatch: “As has been seen in real-world situations,

¹² Budjeryn, interview.

¹³ Dmitry Kovchegin, interview by Muhammed Ali Alkış, *Nuclear Futures Fellowship Capstone Project*, 21 January 2026.

¹⁴ Geoff McCabe, interview by Muhammed Ali Alkış, *Nuclear Futures Fellowship Capstone Project*, 03 February 2026.

occupying forces are likely large in numbers and capabilities compared to the on-site response and would quickly overwhelm the on-site security team.”¹⁵

This state-level challenge to the DBT requires a broader approach to infrastructure defense. Military planners and nuclear regulators can no longer compartmentalize nuclear safety and security into separate silos. When an aggressor state’s military force exceeds the assumptions built into the DBT, civilian operators are immediately placed under extreme duress and must maintain complex reactor safety protocols inside an active combat zone. Addressing this failure point requires moving beyond terrorism-centered models and acknowledging that critical civilian infrastructure is increasingly exposed to conventional military planning.

II. The Proxy Threat and the “Wagner Loophole”

The vulnerability of nuclear facilities is further intensified by the evolution of modern conflict. This new era of warfare is characterized by hybrid operations and asymmetric tactics, which, *inter alia*, make attribution complicated. One of the most concerning developments is the increasing use of private military companies (PMCs) and proxy forces to serve strategic objectives of the state.¹⁶

This dynamic creates what this paper refers to as the “Wagner loophole,” a term used here to describe the attribution and accountability gap that may arise when a state employs a PMC or proxy force, such as Russia’s Wagner Group, to threaten or interfere with nuclear infrastructure. By using PMCs or proxy forces to threaten nuclear infrastructure, state actors can create a gray zone around attribution thresholds in international law. Under the doctrine of state responsibility, establishing that a state exercises “effective control” over a proxy group sets a high evidentiary bar. In practice, this allows states to design their relationships with proxy actors in ways that disguise direct control. This, in return, leads to preserving plausible deniability while still advancing strategic objectives. Aggressor states may leverage this ambiguity to generate radiological risk as a form of coercive pressure while insulating themselves from legal and political accountability. This possibility unsettles the foundations of traditional nuclear deterrence and non-proliferation frameworks as these frameworks depend on state accountability as a basis for sanctions, retaliation, and legal enforcement. When a PMC or proxy force crosses the threshold into a nuclear facility, the international response may be delayed, fragmented, and legally uncertain.

Furthermore, these groups often lack the specialized technical knowledge, which is needed for safe and secure operation within a high-consequence nuclear environment.

¹⁵ McCabe, interview.

¹⁶ For further discussion on security implications, see “Rising Power of Non-State Actors,” Horizon 2045 Radar, Issue 68, available at: https://radar.horizon2045.org/?pg=issue_BBosPXroS8CDOSlex8lcRQ

*While a state's regular military might deploy specialized units—such as Russia's Rosgvardia—proxies and PMCs are far more unpredictable, increasing the likelihood of operational errors during such a scenario. As Aybars Gürpınar (Ret. Director of the Nuclear Installation Safety Division-IAEA) observes, while threats from state military force emerge as a growing critical concern, the most unpredictable threat has shifted away from traditional terrorist organizations to quasi-independent PMCs. As these actors increasingly gain access to asymmetric capabilities, including drones and UAVs, they may challenge physical protection systems designed primarily around conventional perimeter defense and stand-off attack scenarios.*¹⁷

This proxy dynamic challenges both the traditional nuclear terrorism model and the conventional state-on-state warfare model. It adds an additional layer of legal and geopolitical ambiguity to nuclear piracy by allowing states to threaten or exploit nuclear infrastructure indirectly, through actors whose conduct may be difficult to attribute in real time. The result is a more fragmented response environment in which legal responsibility, deterrence, and escalation management all become more uncertain.

III. Asymmetric Drone Warfare and Grid Vulnerability

Not all attacks on nuclear-connected infrastructure constitute nuclear piracy as defined in this paper. However, they may produce similar coercive effects by exploiting the safety dependencies of a civilian nuclear facility without requiring direct occupation of the reactor site itself.

The tactical realities of nuclear piracy are being accelerated by the democratization of disruptive technologies. The proliferation of unmanned aerial vehicles (UAVs) and drone swarms has introduced an era of asymmetric warfare that bypasses the traditional physical security perimeters of a nuclear power plant. Security postures that invest millions in reinforced gates, vehicle barriers, and armed perimeter patrols do not offer sufficient protection against low-cost, high-impact systems capable of precise strikes.

The most severe threat posed by drones, however, is not necessarily a direct kinetic strike on the reactor core. Reactor containment buildings are massive, heavily reinforced concrete structures. Analyses conducted internationally in the wake of the September 11 attacks found that many modern reactor containments could withstand a direct commercial aircraft impact without a major radiological release. Instead, the primary vulnerability lies in auxiliary systems and the facility's connection to the external grid. Adversaries do not need to target the hardened reactor core when switchyards and electrical distribution systems remain structurally exposed and

¹⁷ Aybars Gürpınar, interview by Muhammed Ali Alkış, *Nuclear Futures Fellowship Capstone Project*, 05 February 2026.

difficult to defend. Severing a facility from the grid also achieves a major strategic effect: the loss of baseline electrical generation for the defending state. A nuclear power plant's safety is directly linked to the off-site electrical grid, which provides the continuous power required to run coolant pumps that prevent the reactor core and spent fuel pools from overheating.

Even where an adversary does not physically occupy a facility, it may still seek to exploit the plant's radiological risk indirectly by targeting exposed auxiliary systems and off-site power connections. Such attacks are not identical to nuclear piracy in its strictest sense of seizure and coercive control, but they can operate within the same broader logic of radiological coercion. Drone warfare allows state actors and their proxies to execute precision strikes against highly exposed, unhardened critical infrastructure, such as transformer stations, high-voltage transmission lines, and emergency diesel generator intake systems. As George Foster (Amport Risk) highlights: "That's a really gray area now in terms of some of the weaponry available to state and non-state actors, low cost high impact, such as drones as a classic example of that ... you don't need to attack a nuclear power plant itself to have the requisite consequences that you desire because you can just go for the transformer stations, you can go for the grid."¹⁸

By targeting the grid, an adversary can force a station blackout (SBO), initiating a race against time before emergency backups fail and a severe accident sequence begins. In that sense, the tactic converts a security vulnerability into a safety crisis and turns the plant's radioactive inventory into a source of coercive pressure and potential mass disruption. Remote drone strikes or cyber intrusions into industrial control systems also allow the attacking state to maintain plausible deniability, reducing the direct political fallout that would accompany a physical troop occupation.

The strategic paralysis created by deniability is significant. Tatsujiro Suzuki (Nagasaki University) highlights a recent East Asian war simulation in which unidentified drones attacked a South Korean spent fuel pool, producing a massive transboundary radiological cloud. In the scenario, because "it is very difficult to identify who did it," the defending state was effectively paralyzed and concluded that "it is not possible for the country to send the military missions" in retaliation without risking severe escalation.¹⁹

However, the inability to attribute these attacks is often an institutional and political problem, not only an engineering one. As Fedchenko clarifies, drone and missile debris

¹⁸ George Foster, interview by Muhammed Ali Alkış, *Nuclear Futures Fellowship Capstone Project*, 17 February 2026.

¹⁹ Tatsujiro Suzuki, interview by Muhammed Ali Alkış, *Nuclear Futures Fellowship Capstone Project*, 21 January 2026.

possess distinct signatures that can make technical attribution feasible: “forensics-wise, that’s possible, it is not a technical problem but a political one.”²⁰ Aggressor states can exploit this political gridlock, knowing that even where physical evidence exists, divided international bodies may fail to formally attribute the attack.

IV. Implementing the “Disruptive Technology” Lever

To reduce risks from modern conflict and the weaponization of the grid, the international nuclear community should use the technology lever to strengthen facility resilience. Governments, regulators, and industry should incorporate security-by-design principles into current and future reactor deployments, including the emerging global fleet of small modular reactors (SMRs).

Security-by-design, as used here, refers to embedding security and resilience features into the architecture of a facility from the outset rather than treating protection as an external add-on. In practice, this requires that facilities do not rely exclusively on human guard forces or external grids for survival. To reduce the asymmetric advantages of drones, cyber sabotage, and proxy incursions, next-generation facilities should incorporate resilient, air-gapped, and non-networked analog shutdown mechanisms. Critical cooling infrastructure should also be an integral part of the facility or placed within hardened, protected structures rather than left exposed in open switchyards.

By structurally reducing dependence on vulnerable off-site systems and strengthening passive safety features, the nuclear sector cannot eliminate the strategic logic of nuclear piracy, but it can reduce the coercive leverage an aggressor may derive from the facility. The objective is not only to prevent sabotage in the traditional nuclear security sense; it is also to make civilian nuclear infrastructure less useful as a hostage, a radiological shield, or a pressure point in state-to-state conflict. The defense of nuclear infrastructure must therefore evolve beyond denying unauthorized access and toward limiting the strategic value an aggressor can extract from the facility under conditions of crisis or occupation.

3. Strategic Impacts, Insider Threats, and the “Uninsurable” Atom

I. The Staffing Trap and Accelerated Degradation Under Duress

The operational viability of a nuclear facility depends heavily on its workforce. Safe operation requires highly trained personnel who can carry out technical and regulatory tasks without coercion. Under conditions of nuclear piracy, that basic premise breaks

²⁰ Fedchenko, interview.

down. When a sovereign military occupies a civilian nuclear facility, the operational workforce may be reduced to a limited number of staff forced to manage critical infrastructure under severe military and psychological pressure.

This creates an immediate vulnerability: maintenance degradation under duress. Routine nuclear safety depends on continuous inspection, testing, and repair cycles. During armed occupation, those cycles may be delayed, narrowed, or disrupted altogether. Although a portion of maintenance personnel may remain on-site to manage the most vital safety systems, reduced staffing, restricted access, and disrupted supply chains make comprehensive upkeep difficult. At Zaporizhzhia, for example, slightly more than one-third of maintenance personnel are estimated to remain as of early 2026. Although this skeleton crew is “doing the best they can on the most important things,” Robert Budnitz (retired from Lawrence Berkeley National Laboratory) notes that managing a six-reactor complex—even in cold shutdown—under military duress means that “obviously it can’t be enough to prevent long-term degradation.”²¹

This maintenance problem can lead to a cascade of component failures. Exhausted staff are forced into reactive solutions, requiring them to manage emerging technical problems without the logistical support, spare parts, or rest required to maintain operational baselines. Operators also face acute technical dilemmas. They may be forced to rely on improvised maintenance procedures while managing accident risks in the presence of armed combatants. The socio-technical resilience of the facility erodes, increasing the risk that mechanical failures and human fatigue will compromise safety.

II. Military Occupation Beyond the Traditional Insider-Threat Model

This environment of continuous physical and psychological duress exposes the limits of the traditional “insider threat” model when applied to military occupation. Historically, national nuclear security regimes have relied heavily on vetting, behavioral monitoring, and psychological evaluations designed to identify and neutralize isolated rogue employees or ideologically motivated saboteurs. State-level military occupation falls outside much of this defensive framework. When the facility’s legitimate management is replaced by a hostile state military apparatus, the operational workforce faces acute professional constraints that no regulatory playbook currently addresses.

Emma Jones (PhD researcher) captures the limits of applying this personal reliability framework under conditions of military occupation, stating: “In extreme conditions where people working on these facilities don’t trust the organization or the kind of

²¹ Robert Budnitz, interview by Muhammed Ali Alkış, *Nuclear Futures Fellowship Capstone Project*, 02 February 2026.

individuals controlling the nuclear facility, it becomes an exceptionally challenging situation because they're more focused on survival of themselves ..."²²

Operators are forced into a severe operational dilemma that pits basic human self-preservation against national loyalty and nuclear security. To protect their families from retaliation and to maintain physical access to the facility to prevent a transboundary radiological disaster, personnel may be coerced into signing employment contracts with the occupying state's nuclear corporation. Failure to comply, or attempts to execute subtle acts of sabotage to force a safe plant shutdown, can result in being treated as a hostile actor, including through detention, abuse, or disappearance.²³

Consequently, these coerced operators may be viewed by their own home nation not as compromised insiders operating under *force majeure*, but as potential collaborators with the enemy. This dilemma means that even if the facility is successfully liberated or diplomatically returned to sovereign control, post-conflict recovery could become a significant human resources challenge. National regulators and intelligence services may need to determine the reliability of a workforce that operated under enemy coercion for months or years. This environment could delay the safe restart of the facility, damage the institutional knowledge base of the plant, and increase the strategic loss of the energy asset.

III. The Uninsurable Atom and Macroeconomic Fallout

The localized collapse of operational reliability at an occupied plant also poses a broader systemic risk at the national and international levels. If the international community allows the normalization of facility occupation, the financial architecture supporting global nuclear energy could be undermined. The commercial nuclear sector relies on predictable risk modeling, state-backed liability mechanisms, and comprehensive global insurance markets. Yet, commercial insurance frameworks typically include war clauses that exclude liability for damages incurred during state-level military conflict and armed occupation.

The normalization of nuclear piracy could create an "uninsurable atom." If the geopolitical environment allows any commercial nuclear facility to be transformed into a strategic hostage or stripped from a nation's energy grid by an invading army, the

²² Emma Jones, interview by Muhammed Ali Alkış, *Nuclear Futures Fellowship Capstone Project*, 21 January 2026.

²³ "In a Nuclear Prison: How Rosatom Turned Europe's Largest Nuclear Power Plant Into A Torture Chamber And How Can the World Stop It," Truth Hounds, 2023, <https://truth-hounds.org/en/cases/in-a-nuclear-prison-how-rosatom-turned-europes-largest-nuclear-power-plant-into-a-torture-chamber-and-how-can-the-world-stop-it/>.

financial risk becomes difficult to quantify. Removing a major generating asset from a state—especially one that provides a substantial share of baseline electricity—can undermine grid stability and disrupt broader economic and industrial resilience.

This dynamic introduces a compounding risk into global energy markets. Private capital is sensitive to the high upfront costs and regulatory hurdles of nuclear development. If insurance risk premiums rise globally because of infrastructure seizures, they could deter the private investment required to finance the anticipated expansion of civilian nuclear power. The vulnerability is particularly acute for the deployment of SMRs, which are designed to be distributed in large numbers and may rely on private-sector ownership models driven by narrower commercial margins rather than state-subsidized security budgets.

The economic fragility of this model is significant. If SMRs are deployed at scale across a wider range of national settings, including countries with limited regulatory capacity or active insecurity, they could expand the global attack surface by increasing the number and distribution of civilian nuclear assets exposed to hybrid threats. At the same time, a high-profile occupation, sabotage event, or insurance shock involving even a small number of such facilities could have the opposite effect: it could raise premiums, undermine investor confidence, and slow the broader rollout of SMR business models. The strategic concern, therefore, is not simply expansion or contraction, but volatility. A distributed nuclear future may increase exposure in the short term, while major incidents could later constrain the very market that created that exposure.

4. The Governance Void and Eroding Legal Norms

The physical vulnerabilities and tactical realities of modern nuclear piracy are intensified by a systemic governance void at the international level. As indicated by the Horizon 2045 Foresight Radar, a macro-level decline in the rule of law and eroding constitutional norms are reshaping the global security environment. When applied to the nuclear domain, this broad unbalancing of geopolitical power reveals that foundational legal treaties and international organizations are not well equipped to address the state-level weaponization of critical civilian infrastructure. Without the application of legal rules and norms to establish clearer protections, the international community risks allowing nuclear piracy to operate within a legal vacuum.

I. The Statutory Gap in Relation to Nuclear Security

To diagnose the systemic legal gap at the international level, it is necessary to distinguish between the enduring relevance of the IAEA's statutory mandate and its limits in relation to modern nuclear security. The Agency's statute remains foundational for safeguards and for the broader international safety architecture. But nuclear security, as it is understood

today, was not embedded in the statute as a comparable legally binding function, and the Agency has no legal authority to defend facilities against state military assault or occupation. Although the IAEA has later become an important forum for nuclear security guidance, assistance, and coordination since the 1970s, that evolution did not produce an enforcement mandate capable of addressing the deliberate weaponization of civilian nuclear infrastructure by states.

This historical gap creates a statutory gray zone. The IAEA holds no legal authority to deploy protective forces, dictate military rules of engagement, or physically intervene when a member state violates the sovereignty of another state's nuclear infrastructure. In the face of modern hybrid warfare, the problem is not institutional inactivity but legal and operational limitation. The IAEA can convene, monitor, assist, and articulate technical principles, as the Zaporizhzhia case demonstrated, but it cannot compel compliance, protect a site by force, or impose consequences on an occupying state. In that sense, the response remains reactive and normatively important, yet structurally limited as a deterrent. This statutory void is also reinforced by contemporary state policy. Leading nuclear-armed states—including the United States, the United Kingdom, and France—have historically opposed binding international legal limits on attacks against nuclear facilities. This resistance is rooted in a military option to preserve operational flexibility and deterrence capabilities, including the option to conduct counter-proliferation strikes against adversarial, dual-use, or clandestine facilities. As a result, efforts to strengthen international law are frequently constrained by the very states required to enforce it.

II. Improvisational Diplomacy: The ISAMZ Precedent

In the absence of a comprehensive legal framework or a formal security mandate, the international response to the occupation of the ZNPP relied almost entirely on improvisational diplomacy. IAEA Director General Rafael Grossi recognized the catastrophic potential of this statutory void and chose to stretch the Agency's operational boundaries. As a result, Grossi expanded the IAEA's traditional scope to establish the IAEA Support and Assistance Mission to Zaporizhzhia (ISAMZ).

This deployment amounted to normative engineering. Because Grossi could not rely on a dedicated security mandate, he secured the mission through Ukraine's sovereign request for technical assistance and the Agency's existing safeguards obligations. To bypass the political paralysis of the UN Security Council, Grossi also articulated the Seven Indispensable Pillars of Nuclear Safety and Security. By grounding these pillars in preexisting, consensus-backed technical guidance documents, he established a baseline that neither belligerent could easily reject without appearing unreasonable.

Trevor Findlay (University of Melbourne) captures the essence of this institutional maneuver, stating that “While there was nothing in the IAEA Statute, nuclear security treaties, or existing mechanisms that foresaw the Zaporizhzhia crisis, Grossi was creative in inserting the Agency into the situation and ensuring continuing IAEA relevance and involvement.”²⁴

However, while ISAMZ represents a significant diplomatic and technical intervention, its role extends beyond monitoring. IAEA personnel assess safety and security conditions, liaise with plant personnel and the occupying authorities, report independently, and help identify technical needs. Their presence may also provide a measure of deterrence by increasing international visibility and the political costs of actions that endanger the facility or its personnel. The mission nevertheless remains vulnerable to access restrictions, coercion, and physical danger. Yet the protection of deployed international personnel is itself an important international norm, and their presence can reduce risk by facilitating communication, providing independent information, and making potentially dangerous actions more internationally visible. ISAMZ therefore demonstrates both the practical value of an international presence and the need for stronger legal and political arrangements to support it. At the same time, some experts emphasize that ISAMZ represents a useful precedent for crisis response. As Scott Roecker (Nuclear Threat Initiative) notes, the mission reflects “system improvisation” and provides a potential template should similar emergencies arise again.²⁵

III. Board Paralysis and Global South Positions

The fragility of ad hoc diplomacy is further compounded by political gridlock in the IAEA Board of Governors. While the IAEA’s technical secretariat attempts to manage the physical realities of nuclear piracy on the ground, the policymaking organs in Vienna have struggled to generate unified, enforceable consequences for state actors who weaponize civilian infrastructure. This is partly because, although the Board remains active in safeguards and budgetary matters, “almost everything else the Board of Governors does is political performance.”²⁶ This paralysis reflects broader strains on the rule of law and shifting geopolitical alignments.

A critical factor in this diplomatic gridlock is the voting behavior of many Global South states, which have frequently abstained from resolutions condemning Russian actions at ZNPP. This reluctance to form a unified front is rarely an endorsement of nuclear

²⁴ Trevor Findlay, interview by Muhammed Ali Alkış, *Nuclear Futures Fellowship Capstone Project*, 27 January 2026.

²⁵ Roecker, interview.

²⁶ Holgate, interview.

piracy. On the contrary, it is due to a complex web of historical grievances, economic dependencies, and geopolitical reasons. Many developing states rely on nuclear technology exports, fuel supplies, and financing from state-owned enterprises such as Russia's Rosatom or Chinese equivalents, making them hesitant to stand against critical energy partners even when such silence compromises the very safety and security norms that their own emerging nuclear programs will eventually rely upon.

Many states in the Global South also view externally defined nuclear security measures with suspicion. In the post-9/11 era, many developing states found it hard to implement costly security and regulatory measures promoted by Western nations. Some even considered these demands as heavy requirements that could negatively affect their legitimate rights to peaceful nuclear development under Article IV of the NPT. Consequently, when Western states attempt to leverage the Board of Governors to adopt resolutions to hold a state accountable for security violations, it can trigger historical resentments regarding sovereignty and technological equity.

Elena Sokova (VCDNP) outlines the nuances of this geopolitical divide, noting that the Global South's reluctance is driven by two distinct factors. Regarding Zaporizhzhia specifically, she notes that these nations are caught in an "uncomfortable situation" where they are "forced to choose between the West and Russia."²⁷ As Western states are generally reluctant to fund nuclear projects in developing nations, these countries may be reluctant to support resolutions against Russia, which remains highly competitive in exporting nuclear power. Sokova also highlights deeper historical resentment regarding broader nuclear security mandates. Many developing nations view Western-driven security protocols as unfunded mandates that affect economic development, and they sometimes use their resistance as leverage against nuclear-weapon states that have not fulfilled their own disarmament obligations.²⁸ This underlying friction weakens the Board's ability to act as an authority, reducing institutional consequences for violations against civilian nuclear sites.

IV. Institutional Paralysis and Broader Normative Decay

The failure to establish and enforce norms against nuclear piracy goes beyond the IAEA. It may have profound implications for the foundational global nuclear treaties, most notably the Treaty on the Non-Proliferation of Nuclear Weapons (NPT). The NPT remains central to the nuclear order, but it does not address a situation in which civilian nuclear infrastructure becomes an instrument of radiological coercion. Neither does any other specific convention.

²⁷ Elena Sokova, interview by Muhammed Ali Alkış, *Nuclear Futures Fellowship Capstone Project*, 03 February 2026.

²⁸ Sokova, interview.

As international nuclear governance remains poorly equipped to address facility weaponization, it risks being viewed as paralyzed. The normalization of nuclear piracy could become a major problem for international diplomacy, which undermines the trust required to sustain global non-proliferation efforts. This challenge was visible during the 2022 NPT Review Conference, which could not produce a consensus final document amid disputes over language addressing the military occupation of ZNPP. It remained visible in 2026, when the Review Conference again failed to reach consensus. Reporting from the conference indicates that disputes centered in part on attacks against safeguarded nuclear facilities in Iran, while draft language also expressed “grave concerns over any attack or threat of attack against nuclear facilities devoted to peaceful purposes” and separate concern about the safety and security of nuclear facilities and materials in Ukraine.

When a core pillar of the international order fails to address a nuclear security crisis, the institution’s legitimacy suffers. If states perceive that the NPT or nuclear order cannot protect their sovereign energy infrastructure, they may re-consider the value of their non-proliferation commitments. As Stephen Herzog observes, repeated failures to produce a consensus final document risk rendering the NPT and its review conference processes functionally paralyzed, which has started to mirror the institutional gridlock of the Conference on Disarmament.^{*29} The historical record sharpens this warning: the 2015, 2022, and 2026 Review Conferences all ended without a Final Document, meaning that States Parties have not adopted a substantive consensus outcome since 2010—a sixteen-year gap spanning three consecutive review cycles. These procedural failures are also symptoms of a deeper erosion of trust: nuclear-weapon and non-nuclear-weapon states remain divided over the pace of disarmament, while disputes over the implementation of non-proliferation obligations and attacks on safeguarded civilian nuclear facilities have made it harder to reaffirm even previously agreed commitments. Prolonged deadlock therefore threatens not only the credibility of the review process, but also confidence in the reciprocal bargain on which the NPT rests.

V. The Strategic Necessity of Legal Evolution

The convergence of statutory gaps, political gridlock, and institutional strain suggests that current international law is not sufficient to deter the rising threat of nuclear piracy. *Ad hoc* diplomacy and technical guidance are insufficient substitutes for clearer legal

*The Conference on Disarmament is the world’s single multilateral disarmament negotiating forum. Together with its predecessor bodies, it has been responsible for negotiating landmark arms-control agreements, including the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), the Chemical Weapons Convention, and the Comprehensive Nuclear-Test-Ban Treaty. Because the Conference operates by consensus, however, a single member state can block substantive negotiations.

²⁹ Herzog, interview.

boundaries. To reverse this trajectory, the international community should develop explicit international protocols or political commitments that prohibit the military occupation, coercive exploitation, or targeting of civilian nuclear facilities and their critical auxiliary systems.

Historically, major nuclear-armed states—including Russia—have resisted such binding prohibitions to preserve their own offensive flexibility. However, the contemporary evolution of armed conflict should lead to a recalculation of this self-interest. The strategic rationale for establishing these norms is no longer a concession by major powers, but a matter of recognizing current realities.

For example, while Russia has leveraged the occupation of ZNPP for compellence, its own civilian nuclear infrastructure is increasingly exposed to reciprocal vulnerabilities. Over the protracted course of the invasion since 2022, Ukraine has demonstrated an evolving capability to strike targets deep inside Russian territory. If a defending state facing existential pressure decided to target an attacker's nuclear power plant or its auxiliary systems in order to disrupt electricity supply, impose economic costs, or generate coercive pressure, the current asymmetry of vulnerability would diminish.

An adversary does not need to penetrate a reactor's hardest protective structures to achieve major strategic effects. By targeting exposed auxiliary systems—such as switchyards, water supply infrastructure, or external grid connections—it may be able to disable the facility, disrupt electricity supply, and generate coercive pressure. In that context, stronger legal and political restraints on attacks against civilian nuclear facilities should not be viewed only as protections against radiological catastrophe. They also serve broader interests in strategic stability, civilian protection, and the preservation of confidence in peaceful nuclear infrastructure. For that reason, such restraints increasingly align with the national security interests of states that have historically resisted binding limits on military operations against nuclear sites.

5. Opportunities for Action: The 2045 Horizon

The limitations of the current nuclear security architecture—demonstrated by state military threats beyond the scope of the DBT, the statutory constraints facing the IAEA, and the erosion of foundational nuclear treaties—require a shift from reactive crisis management to strategic foresight. This paper therefore applies the Horizon 2045 lens used in the Nuclear Futures Fellowship. The choice of 2045 is methodological rather than merely chronological: it provides a shared horizon for examining how interacting changes in governance, technology, infrastructure, warfare, and social systems could shape nuclear security.

Based on the Horizon 2045 Foresight Radar, which identifies structural shifts in global governance, technology, and warfare, it is possible to offer some plausible scenarios. Depending on the international community's willingness to adapt, the threat of nuclear facility weaponization could follow one of three divergent scenarios over the next two decades.

Scenario 1: The Status Quo (Incremental Degradation)

In this baseline scenario, the international community fails to establish binding legal frameworks or credible political commitments to deter state-level aggression against civilian nuclear sites. The geopolitical polarization currently paralyzing the IAEA Board of Governors and NPT Review Conferences becomes a durable feature of nuclear diplomacy. Occupations of nuclear plants and drone strikes on critical off-site power grids become tense but unresolved anomalies of modern conflict. The international response remains improvisational: the IAEA is forced to stretch its implied powers to deploy ad hoc missions combining technical assistance, liaison, assessment, and reporting in active war zones, risking the lives of international civil servants without enforcement mechanisms to support them. In this trajectory, while the norm remains shakily in place, the global nuclear security regime nonetheless suffers gradual degradation as state actors increasingly use critical infrastructure for coercive pressure in and around nuclear environments.

Scenario 2: Normalization (Systemic Destabilization)

This worst-case scenario represents systemic destabilization. The strategic benefit of nuclear piracy proves effective. More and more states start to incorporate such a tactic into the military doctrines. Therefore, the occupation of nuclear facilities, attacks against auxiliary systems, and the deployment of PMCs or proxy forces to seize or sabotage nuclear infrastructure become more routine while traditional nuclear security mechanisms designed around non-state threats fail each time. Adversaries begin to use more cyber operations and drone swarms to conduct difficult-to-attribute attacks. These involve damaging off-site power and creating radiological crises under plausible deniability. The normalization of these asymmetric attacks prevents further private capital investment and creates an "uninsurable atom." Private investment considers retreating from the nuclear sector, delaying advanced reactor deployment and undermining the global clean energy transition. The international community risks entering a period of compounding climate and security degradation, in which radiological risk and infrastructure warfare reinforce each other.

Scenario 3: Strategic Resilience (Restoring Security Norms)

In this adaptive scenario, the near-misses of the 2020s help states acknowledge the potential risks. This leads several states to move the international community beyond institutional inertia. Recognizing the threat that nuclear piracy poses to global energy

security as well as to civilian safety and strategic stability, states begin to act across three reinforcing levers: legal rules, technology, and conceptual models. Here, shifting conceptual models means reclassifying the occupation or coercive exploitation of civilian nuclear infrastructure not as an exceptional byproduct of war, but as a distinct strategic threat requiring dedicated deterrence, planning, and governance responses. The global community focuses on solutions to mitigate risks of nuclear piracy by establishing stronger legal rules or political commitments that prohibit the military targeting or occupation of civilian nuclear infrastructure. At the same time, the nuclear energy sector adopts advanced security-by-design principles, reducing the vulnerabilities of critical infrastructure by making next-generation facilities more resilient to external sabotage and grid severance.

I. Policy Recommendation 1: Regional Non-Attack Treaties (The Legal Lever)

To guide the global security architecture toward the optimistic turn, policymakers must confront the constraints of the current geopolitical environment. A universally binding global convention prohibiting attacks on nuclear facilities through the United Nations or the IAEA is unlikely in the near term. Many states resist sweeping multilateral prohibitions because they wish to preserve the operational flexibility to execute counter-proliferation strikes against facilities they deem clandestine or dual use.

Because global consensus is constrained by great power competition, the immediate path forward may rely on decentralized, regional diplomacy. As Suzuki emphasizes regarding the gridlock over infrastructure protection, “It may be difficult to have a global treaty, but the regional treaty or bilateral agreement could be possible.”³⁰ The international community should encourage joint commitments explicitly prohibiting attacks on operational, IAEA-safeguarded facilities that could produce severe radiological releases. Localized confidence-building measures—such as agreements in volatile regions including the Korean Peninsula or the Middle East not to attack one another’s nuclear facilities—could protect critical civilian infrastructure while offering a pragmatic compromise that major military powers may be more likely to endorse.³¹

The case for regional diplomacy is reinforced by the recent conflict between Armenia and Azerbaijan, during which threats were issued against the Metsamor nuclear plant. Such incidents demonstrate that state decision-makers acting in the fog of war may issue threats or consider actions without fully accounting for transboundary radiological risks. Localized confidence-building measures are therefore essential. One durable precedent is the 1988 Non-Attack Agreement between India and Pakistan, which has helped prevent kinetic strikes on declared nuclear facilities despite recurring conventional military crises between the two nations.

This localized model should be adapted for high-tension regions embarking on nuclear expansion, particularly the Middle East, Eastern Europe, and East Asia. By negotiating non-attack pacts on a bilateral or regional basis, states can build localized confidence measures without requiring consensus among the P5 members of the UN Security Council. Regional agreements can limit adversaries’ ability to use critical infrastructure as a weapon of compellence, stabilize localized energy grids, and isolate actors that

³⁰ Suzuki, interview.

³¹ Suzuki, interview.

violate agreed norms. As Roecker summarizes the need for this strategic pivot, “regional gains are the big ones as the game is about regional now more than global.”³²

While negotiating regional non-attack treaties in current geopolitical flashpoints such as Eastern Europe or the Middle East remains a significant diplomatic challenge, such agreements should remain an important strategic objective. Because they may take years or decades to realize, deploying the technology lever—specifically security-by-design for SMRs—offers a more immediate defense mechanism. Policymakers should also pursue actionable interim steps to bridge the current diplomatic gap. Nuclear Threat Initiative’s (NTI) 2024 paper *Nuclear Facilities in Times of Crisis* recommends developing an international code of conduct for armed conflict near nuclear facilities and strengthening political and legal commitments to protect facilities during armed conflict.³³ However, the effectiveness of such an approach is constrained by limited political buy-in. As Roecker observes, while a code of conduct is “a great way” to strengthen norms, many states do not yet perceive threats to nuclear facilities as nuclear security risks to themselves.³⁴

Building on this approach, the IAEA Board of Governors should formalize a voluntary code of conduct regarding the inviolability of civilian nuclear infrastructure. Industry-level organizations such as the World Association of Nuclear Operators (WANO) should also be leveraged to establish operational safety and security norms independently of paralyzed state diplomacy. Baseline peer-review standards could create soft-power penalties for operators cooperating with occupying forces by limiting access to critical global safety data, international supply chains, and peer-to-peer technical support when cooperation undermines nuclear safety or security.

³² Roecker, interview.

³³ Nickolas Roth, Ross Matzkin-Bridger, and Jessica Bufford, *Nuclear Facilities in Times of Crisis* (Washington, DC: Nuclear Threat Initiative, 2024), https://www.nti.org/wp-content/uploads/2024/06/NTI_Paper_FITOC_FINAL_060724.pdf.

³⁴ Roecker, interview.

II. Policy Recommendation 2: Economic “Security-by-Design” (The Technology Lever)

While regional diplomacy addresses the legal and normative failures of the current system, policymakers must also deploy the technology lever to mitigate physical vulnerabilities associated with the potential expansion of civilian nuclear infrastructure. Traditional reactors should be hardened against the grid-severance tactics witnessed at Zaporizhzhia, while the expansion of SMRs presents both opportunities and risks in the context of nuclear piracy. On one hand, because SMRs possess significantly smaller radioactive inventories than traditional reactors, the radiological consequences of a successful attack may be comparatively limited. Many advanced reactor models also incorporate passive “walk-away” safety mechanisms—such as natural circulation cooling and advanced TRISO fuel—that could substantially reduce vulnerability to the grid-severance tactics threatening legacy light-water reactors. Dispersing energy generation across hundreds of smaller nodes may also prevent an aggressor from neutralizing a substantial portion of a nation’s energy grid through a single strike.

On the other hand, a distributed nuclear architecture and a broader global nuclear footprint increase the overall attack surface. The risk profile varies by deployment type and scale. Newly constructed large reactors may still present expansive physical footprints and exposed switchyards. Terrestrial microreactors designed for remote industrial use face challenges linked to isolation, while floating marine reactors introduce vulnerabilities related to maritime interdiction. Reliance on high-assay low-enriched uranium (HALEU) for many advanced designs also creates new interception risks across a more decentralized global supply chain. These vulnerabilities are compounded by the likelihood that many future facilities will be privately owned or operated and therefore subject to commercial constraints, although both private and state-owned facilities remain subject to national nuclear security requirements. If regulatory requirements remain based on a DBT that does not encompass state-level military threats, commercially operated facilities may have limited incentives to invest beyond mandatory standards in measures intended to address such exceptional contingencies.

To balance investment with sufficient physical protection, regulators should agree on security-by-design principles for new facility construction. Advanced protective measures—including non-networked analog shutdown systems and internalized ultimate heat sinks—should be considered for reactor architecture regardless of scale. Subterranean or hardened siting could also reduce the vulnerability of smaller facilities to asymmetric drone and missile strikes. These designs should integrate advanced attribution tools, including hardened off-site satellite monitoring and tamper-resistant cyber logging systems, to reduce ambiguity during attacks and strengthen attribution during crises. By reducing dependence on vulnerable external grids and minimizing

exploitable operational chokepoints, these measures can reduce the tactical leverage required for radiological compellence.

III. Policy Recommendation 3: Reframing Nuclear Piracy (The Conceptual Model Lever)

Legal reform and technical hardening will remain incomplete unless policymakers, military planners, and nuclear regulators also change how they conceptualize the threat. The occupation or coercive exploitation of a civilian nuclear facility should no longer be treated as an anomalous byproduct of conventional conflict or folded uncritically into the category of nuclear terrorism. It should be recognized as a distinct form of state-enabled coercion that sits at the intersection of nuclear security, critical infrastructure protection, and strategic deterrence. This reframing matters because terminology shapes planning assumptions, legal categorization, and threshold judgments about response. If states continue to misclassify the threat, they are likely to underinvest in the doctrinal, diplomatic, and regulatory changes needed to deter it.

Conclusion

The intentional weaponization of civilian nuclear facilities during state-to-state conflict should not be treated as a temporary anomaly. It reflects an evolution in modern warfare. By occupying or threatening critical civilian infrastructure, an aggressor can project the transboundary risk of a radiological disaster without crossing the political and military threshold of using a nuclear weapon.

The global nuclear security architecture is not fully equipped for this state-level threat. To address the realities of modern conflict, governments, international institutions, and industry should reinforce the non-attack norm, improve crisis preparedness, and adopt security-by-design approaches that reduce vulnerabilities in the global energy system.

Ultimately, achieving these technical and legal shifts requires a deeper change in the conceptual models held by policymakers, military planners, and nuclear regulators. The international community can no longer afford the institutional inertia of treating state military occupations of nuclear facilities as generic “military activities” or forcing them into the inadequate category of “nuclear terrorism.” Terminology shapes strategic response because it influences legal framing, threat perception, and policy design. “Nuclear piracy” captures the legal, operational, and strategic dimensions of this threat. It demands that these acts be recognized not as isolated incidents of war, but as deliberate violations of international nuclear security norms that require clearer preventive measures.

