The Trojan Horse of Geoengineering

Threats in the Architecture of Stratospheric Aerosol Injection

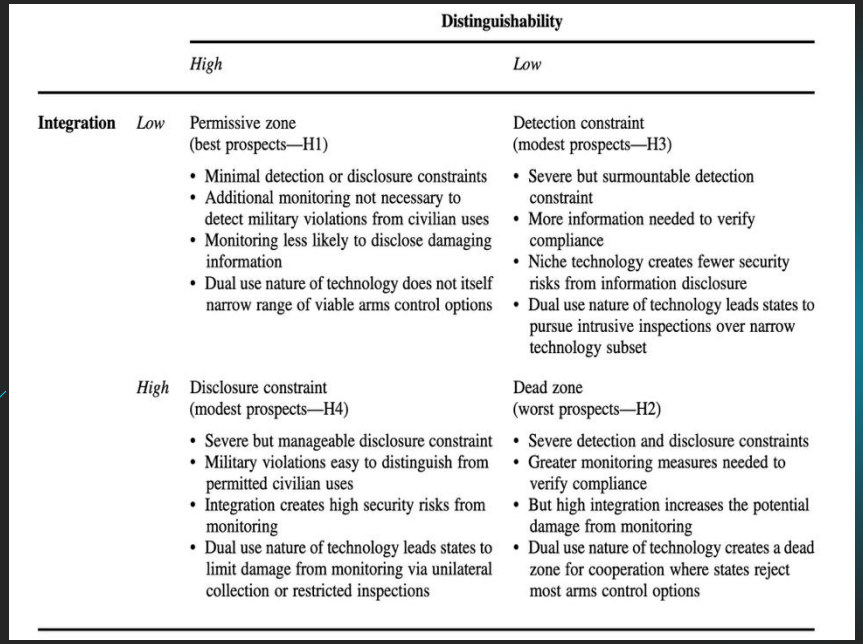
William Morrissey & Andrew Lockley

OVERVIEW

1. Securitization & SRM Architecture Risks
2. Dual-Use Technology Monitoring
3. Escalation Scenarios
    - Platform Ambiguity
    - Vulnerability Nodes
    - Proliferation Risks

SRM Architecture Securitization

Dual-Use Technology Monitoring



		Distinguishability: *High*	Distinguishability: *Low*
Integration	*Low*	Permissive zone (best prospects—H1) • Minimal detection or disclosure constraints • Additional monitoring not necessary to detect military violations from civilian uses • Monitoring less likely to disclose damaging information • Dual use nature of technology does not itself narrow range of viable arms control options	Detection constraint (modest prospects—H3) • Severe but surmountable detection constraint • More information needed to verify compliance • Niche technology creates fewer security risks from information disclosure • Dual use nature of technology leads states to pursue intrusive inspections over narrow technology subset
	High	Disclosure constraint (modest prospects—H4) • Severe but manageable disclosure constraint • Military violations easy to distinguish from permitted civilian uses • Integration creates high security risks from monitoring • Dual use nature of technology leads states to limit damage from monitoring via unilateral collection or restricted inspections	Dead zone (worst prospects—H2) • Severe detection and disclosure constraints • Greater monitoring measures needed to verify compliance • But high integration increases the potential damage from monitoring • Dual use nature of technology creates a dead zone for cooperation where states reject most arms control options

Vaynman, Jane, and Tristan A. Volpe. 2023. "Dual Use Deception: How Technology Shapes Cooperation in International Relations." *International Organization* 77 (3): 599–632.

Distinguishability:

- "The relative ease of differentiating between a technology's military and civilian applications"

Integration:

- "reflects a technology's range and depth of use within military enterprises and the broader civilian economy"

CS/CS/SB 56 — Geoengineering and Weather Modification Activities

by Rules Committee; Environment and Natural Resources Committee; and Senators Garcia, Leek, Yarborough, and Gruters

Go to Bill: SB 56

This summary is provided for information only and does not represent the opinion of any Senator, Senate Officer, or Senate Office.

Prepared by: Environment and Natural Resources Committee (EN)

The bill prohibits geoengineering and weather modification activities and provides such activities are a third-degree felony, punishable by up to five years' imprisonment and fines of up to $100,000, except aircraft operators and controllers who are subject to a fine of up to $5,000 and five years' imprisonment. All funds collected must be deposited in the Air Pollution Control Trust Fund. The bill directs the Department of Environmental Protection (DEP) to establish a dedicated e-mail address and online form to allow people to report suspected geoengineering and weather modification activities. DEP must investigate reports warranting further review and must refer reports to the Department of Health or the Division of Emergency Management when appropriate.

The bill provides that, beginning October 1, 2025, publicly owned airports must report monthly to the Florida Department of Transportation (DOT) any aircraft equipped for geoengineering or weather modification activities. DOT may not expend state funds to support public airports that do not comply.

The bill also removes DEP's authority to conduct studies, research, experimentation, and evaluations in the field of weather modification.

If approved by the Governor, or allowed to become law without the Governor's signature, these provisions take effect July 1, 2025.

Vote: Senate 28-9; House 82-28

Downloads

- PDF of this Summary (PDF)
- All 2025 Bill Summaries for Environment and Natural Resources Committee (PDF)

SAI Architecture Threat Vectors

01

Platform Ambiguity

Deployment and Monitoring platforms are viewed as an airspace threat or intelligence collection platform

02

Vulnerability Nodes

Ground-based deployment infrastructure is a target for attack, sabotage, or espionage

03

Proliferation Risks

Competitor states are able to access advanced technology or to leapfrog capabilities