ESCUELA NAVAL DE CADETES
"ALMIRANTE PADILLA"
Honor y Tradición

OnBoard Knowledge Journal

Article

Analysis of the Interaction between the State and Non-State Actors in the Maritime Domain through a Virtual System of Systems (SoS)

Análisis de la interacción entre el Estado y los actores no estatales en el dominio marítimo mediante un sistema de sistemas virtual (SoS)

Gustavo Andrés Guerra La Rotta [1]

[1] Loger Group, Escuela Naval de Cadetes "Almirante Padilla", Cartagena, 111321, Colombia; wargx@outlook.es

* Correspondence: wargx@outlook.es

Citation: Guerra La Rotta, G.A. Analysis of the Interaction between the State and Non-State Actors in the Maritime Environment through a Virtual System of Systems (SoS). *OnBoard Knowledge Journal* **2026**, 2, 5. https://doi.org/10.70554/OBJK2026.v02n01.05

Received: 17/03/2026, Accepted: 28/04/2026, Published: 05/05/2026

DOI: https://doi.org/10.70554/OBJK2026.v02n01.05

Abstract: This article proposes a heuristic analytical framework based on a Virtual System-of-Systems to examine interactions between ten archetypes of non-state actors and the State in the maritime domain. Its contribution integrates an archetype typology, Maier's framework, Sterman's causal notation, and the system of interest from ISO/IEC/IEEE 15288:2023, with an assessment of conceptual compatibility with Maier's attributes. The archetypes are classified by legitimacy, function, and technological domain. The system of interest uses four measures of effectiveness: critical service availability, public legitimacy, informational integrity, and cyber resilience. The causal structure includes one reinforcing loop and one balancing loop. The interaction matrix presents two auditable structural hypotheses for qualitative maritime system analysis purposes.

Keywords: National security, Cybersecurity, Critical infrastructure, Systems analysis, Governance, Non-state actor.

Resumen: Este artículo propone un marco analítico heurístico basado en un Sistema Virtual de Sistemas para examinar las interacciones entre diez arquetipos de actores no estatales y el Estado en el dominio marítimo. Su contribución integra una tipología de arquetipos, el marco de Maier, la notación causal de Sterman y el sistema de interés de ISO/IEC/IEEE 15288:2023, con una evaluación de compatibilidad conceptual con los atributos de Maier. Los arquetipos se clasifican por legitimidad, función y dominio tecnológico. El sistema de interés emplea cuatro medidas de efectividad: disponibilidad de servicios críticos, legitimidad pública, integridad informacional y resiliencia cibernética. La estructura causal incluye un bucle reforzador y un bucle equilibrador. La matriz de interacción presenta dos hipótesis estructurales auditables para el análisis cualitativo del sistema marítimo.

Palabras clave: Seguridad nacional, Ciberseguridad, Infraestructura crítica, Análisis de sistemas, Gobernanza, Actor no Estatal.

© 2026 by authors.
Licensed by Escuela Naval de Cadetes "Almirante Padilla", COL.
This article is freely accessible and distributed under the terms and conditions
of Creative Commons Attribution (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

A hybrid threat is characterized by an adaptive mix of state and non-state actors and tactics that combine conventional and unconventional, overt, and covert means to exploit state vulnerabilities and pursue political and strategic objectives [14] . This convergence comprises military coercion, insurgency, subversion, sabotage, terrorism, and illicit economies, linked to cyber operations and informational influence that affect the political, military, economic and social domains at the same time [45], [46]. Technology does not act as an auxiliary asset but as an operational multiplier: digital platforms, encryption, cloud services, and automation reduce coordination friction, extend reach, and accelerate execution. The convergence of information technology (IT) and operational technology (OT) increases the probability of material breakdown in critical infrastructure and increases the strategic cost of incidents that begin as digital events [16].

The central institutional challenge in this context is Unified Action between government, the ICT sector and Military Forces, based on inter-agency coordination with clear areas of authority, interoperability and control of duplication [16], [13], [21]. This articulation operates under IHL and IHRL and requires legality, proportionality, and accountability when the response incorporates technical capabilities, such as surveillance, analytics, and cyber defense, that may place rights at risk in the absence of safeguards. In strategic terms, the center of gravity comprises the neutralization of armed actors and the protection of state continuity and public trust. Operational resilience, digital security of critical services, and institutional narrative coherence are necessary conditions to preserve legitimacy in contested scenarios [16], [13], [21], [15].

The report of the National Intelligence Council [35] documents the increased influence of Non-State Actors (NSAs) on global and security dynamics. It adopts a broad definition that covers both non-governmental entities and territorial entities and proposes their inclusion in strategies for stronger Unified Action. However, the report leaves a central issue of institutional design unresolved: the technical capabilities, digital infrastructures, and novel technologies that enable NSA influence, coordination, and disruption, as well as the differentiated legal and political status of each type of actor. NSA typologies available in the literature on international relations and security studies [52], [34], [42], [50], provide useful descriptive classifications, but they do not treat the technological dimension as a structural axis and do not connect the typology to a formal systemic model that explains how interaction across archetypes modifies state capacity. The absence of this systemic framework with verifiable polarities limits the operational value of these typologies for the design of institutional capacity and response prioritization.

Based on this gap, this study poses the research question: what systemic structure, with documented polarities and explicit technological interfaces, allows analysis of the interaction between non-state actor archetypes and the State to orient Unified Action in hybrid-threat scenarios? The contribution of the study lies not in its individual components. The archetype typology derives from [35], [52], [34], [42], [50]; the Virtual System of Systems (SoS) framework derives from Maier [29]; the causal notation derives from Sterman [47]; and the system of interest derives from ISO/IEC/IEEE 15288:2023 [25]. Its contribution lies in the disciplined assembly of these theoretical bodies in a domain where prior literature lacks comparable systemic frameworks, with compatibility assessment relative to Maier's five attributes, declared polarities via bibliographic reference and application to the maritime domain.

For any State, the interaction among non-state actors, critical technologies, and connected infrastructures creates a problem with institutional implications. The governance of these interactions is decisive because the effect of these actors on state capabilities depends on their legitimacy, the technological interface involved, and the conditions under which the relation occurs. Under auditable conditions aligned with institutional purposes, these actors may complement state capabilities. Under coercive, illicit, or weakly governed conditions, technological interdependence may increase systemic risk.

In this context, Unified Action depends not only on the relations between actors or on technological adoption, but also on verifiable governance capacities for digital security, control, audit and operational resilience [6;10]. From this framework, the analysis identifies two relevant patterns for institutional response: documented cooperation within actor subsystems and the evolution of technological capabilities with potential effects on system stability. Sections 4 and 5 develop both patterns.

The article has six sections. Section 3 presents the method. Section 4 develops the results: characterization, typology, the Virtual System-of-Systems analytical framework with its loops, the interaction matrix, sensitivity analysis, and application to the maritime domain. Section 5 discusses the position of the framework in relation to prior typologies and its implications. Section 6 develops institutional implications for Unified Action, with future research in its final subsection. Section 7 presents the conclusions.

2. Contributions

- The article proposes a heuristic Virtual System-of-Systems framework to examine State and non-state actor interaction in the maritime domain. Its contribution lies in the integration of actor typologies, System-of-Systems theory, causal notation, and ISO/IEC/IEEE 15288:2023. This synthesis turns a descriptive classification into an auditable systemic architecture for maritime security, critical infrastructure, and state capacity.
- The study introduces an interaction matrix with qualitative polarities, technological interfaces, and institutional measures of effectiveness. This structure identifies critical relations among legitimate actors, illegitimate actors, and the State, with emphasis on IT, OT, IT–OT convergence, and the informational interface. Its innovation lies in an ordered, verifiable model for future validation.
- The article offers a conceptual tool to guide Unified Action against hybrid threats, transnational crime, cyber risks, and informational disputes. Its contribution supports port traceability, critical-service protection, cyber resilience, interinstitutional cooperation, and public legitimacy. The study links systemic theory, maritime governance, and strategic decisions.

3. Materials and Methods

3.1. *Type of Study*

This work is a conceptual article on typology and model, in Jaakkola's sense [26]. Its purpose is to build an explicit analytical framework to classify archetypes of non-state actors and to represent their systemic interactions with the State, not to estimate causal effects with primary data.

3.2. *Literature Integration Strategy*

The literature review was selective and structured according to conceptual relevance. Four types of sources had priority: peer-reviewed articles, international technical standards and frameworks, official military doctrine, and reports from specialized bodies. The search was organized around three cores: typologies of non-state actors, System-of-Systems architecture, and causal models applied to national security and the maritime domain.

3.3. *Four-Phase Methodological Design*

The design used four consecutive phases, with internal consistency control at the end of each phase.

- **Phase 1: Identification of conceptual gap.** This phase defined the conceptual gap as the absence of frameworks that integrate typology, technological dimension, and systemic representation of interactions [35], [52], [34], [42], [50].
- **Phase 2: Construction of the typology.** This phase built the typology through three complementary analytical dimensions: legitimacy, function, and the primary technological domain. These dimensions were assigned according to the functional and technological predominance documented in sources [48], [9], [24], [11].
- **Phase 3: Formalization of the model.** This phase represented the ten archetypes as constituent systems of a Virtual System-of-Systems, while the State was represented as the system of interest. It also assessed conceptual compatibility with Maier's attributes and expressed relations through causal loop diagrams in Sterman's notation [29], [25], [47].

- **Phase 4: Exploratory application to the maritime domain.** This phase applied the model to three documented mechanisms: technological enablement, operational cooperation, and the use of supply chains by transnational crime.

3.4. Separation Between Description and Prescription

Sections 4 and 5 present and discuss the model. Section 6 translates the results of the model into institutional implications for Unified Action. This structure separates analytical development from normative implications and prevents recommendations from predetermining the study's analytical structure.

3.5. Study Limits

The study has four limits. First, it is a conceptual and documentary proposal, not an empirical one. Second, it uses qualitative polarities and documented mechanisms, with no magnitude estimates; quantification through stock-and-flow diagrams remains a future task [47]. Third, the absence of direct support for a specific relation reflects a limit of the reviewed corpus, not proof that the interaction does not exist. Fourth, the interaction matrix (Table 7) comes from single-coder documentary coding; cell counts in Sections 4.6.2, 5.3, and 7 operate as structural hypotheses, not empirical findings. Internal matrix consistency does not validate the corpus or the framework, since bibliographic selection precedes polarity assignment. Both require external contrast through double coding, complementary coverage, and inter-coder agreement statistics.

4. Results

4.1. General Characterization of Non-State Actors

Non-state actors (NSAs) occupy a relevant place in international and domestic security. Firms, civil society organizations, academic institutions, transnational networks, and individuals with influence capacity affect governance through channels distinct from traditional state authority. They mobilize economic resources, expert knowledge, social legitimacy, access to digital platforms, and network coordination capacity [35], [52], [34], [42], [50]. This study defines an NSA by three positive criteria: decisional autonomy from the State, its own resource base, and internal governance independent of public-administration hierarchy. An NSA mobilizes these resources to influence public agendas, even at the transnational level. The relevance of each archetype depends on the sector, the context, and the comparative advantages under its control; it does not imply a replacement of the state order. The consulted literature documents functional reconfiguration between the State and NSAs, not a linear decline of state power. Technology amplifies the scope, speed, and coordination capacity of archetypes that act in cyberspace or rely on connected infrastructure. With the convergence between information technology (IT) and operational technology (OT), a cyber incident may result in operational disruption with concrete material costs [48], [9]. In the maritime domain, the digitalization of port logistics chains and navigation systems increases this sensitivity [7], [33], [43], [39].

4.2. Proposed Typology: Three Analytical Axes

The ten archetypes are ordered through three complementary analytical dimensions: legitimacy, function, and the primary technological domain.

The illegitimate category is adopted in North's sense: an actor whose action violates the formal rules of the institutional order [36]. Table 1 summarizes the typology. Transnational crime and terrorist groups separate by primary intent (illicit-economy versus political-coercive), not by capability profile. Table 1 shows a consistent analytical pattern. The six legitimate archetypes are concentrated in IT and the informational domain, whereas three of the four illegitimate archetypes extend their radius of action toward OT or IT-OT convergence. This suggests higher potential capacity to affect physical processes. Transnational crime operates mainly in IT and informational domains, although it may produce material effects through the use of physical chains under third-party control. Two clarifications limit the scope: NSA incidence is sectoral and contingent; territorial entities correspond to subnational state actors, not to NSAs [37], [53].

Table 1. Typology of the ten archetypes by three analytical axes

Archetype	Legitimacy	Function	Primary tech. domain	Secondary tech. domain
Commercial firms	Legitimate	Productive	IT	IT-OT
Academic institutes	Legitimate	Cognitive	IT	Informational
Civil society	Legitimate	Civic	Informational	—
Super-empowered individuals	Legitimate	Civic	Informational	IT
Transnational actors	Legitimate	Civic	Informational	IT
Non-violent movements	Legitimate	Civic	Informational	—
Armed militants	Illegitimate	Coercive	Informational	OT
Cybercrime and hackers	Illegitimate	Criminal	IT	IT-OT
Terrorist groups	Illegitimate	Coercive	Informational	IT-OT
Transnational crime	Illegitimate	Criminal	IT	Informational

Note: Own elaboration based on this study.

4.3. *Summary Description of the Ten Archetypes*

Table 2 presents a descriptive characterization of the archetypes on the basis of the documentary review.

Table 2. Summary description of the archetypes

Archetype	Legitimacy	Function
Commercial firms	Control of data, platforms, cloud systems, automation, digital supply chains, and critical-infrastructure control systems [32;51;53].	Definition of industrial standards, influence on economic policy, and transfer of private cyber risks to essential State services [43].
Academic institutes	Computational tools, data repositories, and digital collaboration systems [7].	Knowledge production and expert advice for public policy [4;19].
Civil society	Social media, message systems, and evidence repositories [7;33].	Human-rights oversight, public-agenda mobilization, and campaign escalation in the informational domain [3;44].
Super-empowered individuals	Platforms, audience networks, and technological finance [7].	Discourse formation, financial support for initiatives, and unofficial diplomatic roles [12].
Transnational actors	Remote-cooperation platforms and shared information management [7;33].	Pressure for international norms and multilateral accords [12;30;31].
Non-violent movements	Message systems, social media, and basic communication protection [7;27].	Public pressure through protest, civil disobedience, and strikes [38].
Armed militants	Encrypted command-and-control systems, digital micro-diffusion, and connected civilian infrastructure [40;41].	Regional destabilization, accelerated coordination, and military challenge to state authority.
Cybercrime and hackers	Initial access, persistence, extortion, sale of access, and escalation across transnational digital infrastructures [23;27;39].	Espionage, intellectual-property theft, hacktivism, and possible state tolerance or support.
Terrorist groups	Digital propaganda and radicalization, plus own or outsourced cyber capabilities against critical infrastructure [5;7;33;43].	Conversion of cyberspace into an operational domain and escalation due to critical-system dependence.
Transnational crime	Cross-border coordination through platforms and encryption, data and geolocation management, and financial mobilization [18;22;28;54].	Violent control over routes and markets, organizational resilience under state pressure, and cocaine traffic through containers.

Note. The table synthesizes the technological capacities and recurrent influence mechanisms associated with each archetype. It offers an analytical overview rather than an exhaustive account of the empirical heterogeneity within each category.

4.4. Virtual System-of-Systems Model

4.4.1. **Conceptual Compatibility Assessment**

The analytical correspondence summarized in Table 3 justifies the use of Maier's framework as an interpretive lens for the model, without equating this compatibility with empirical validation of the system.

Table 3. Conceptual compatibility assessment with Maier's five attributes

Attribute	Verification	Compliance
Operational independence	Each archetype operates with its own budget, decision-making capacity, and agenda, without authorization from the State.	Full
Managerial independence	Each archetype maintains internal governance independent from the State.	Full
Geographic distribution	The archetypes operate across different jurisdictions, including transnational spaces.	Full
Emergent behavior	The whole produces effects on national security that no isolated archetype produces on its own.	Full
Evolutionary development	The archetypes transform over time without a central schedule.	Full

Note. Conceptual compatibility assessment of the NSA/INSA set in relation to the State as the system of interest. Own elaboration.

4.4.2. **Model Architecture and Ontological Hierarchy**

For this academic exercise, an analytical framework was structured according to Figure 1 and organized into three levels.

- **Upper level N3: the State as the system of interest.** In terms of ISO/IEC/IEEE 15288:2023 [25], the State is delimited as the system of interest (SoI) at the level of abstraction of aggregated Unified Action. The standard requires an explicit declaration of the SoI boundary; this boundary is declared in Section 4.4.3. The state of the SoI is observed through four measures of effectiveness (MoE), in the strict sense of ISO/IEC/IEEE 15288:2023: availability of critical services (D), public legitimacy (L), informational integrity (I), and cyber-resilience of critical infrastructure (R). These four MoE are not aggregated into a scalar index. Maier [29] establishes that a Virtual SoS lacks both central authority and a shared purpose; therefore, global aggregation is not applicable. The state of the SoI is represented as the vector $C_e = (D, L, I, R)$, with each component observed separately through public sectoral sources; strict-sense operationalization belongs to Section 6.5.

- **Intermediate level N2: ontological hierarchy of technological interfaces.** The four interfaces that mediate every flow between the archetypes and the State are organized into two distinct ontological levels, based on Floridi's [17] distinction between the physical-digital layer and the semantic-cognitive layer. The first three interfaces, namely IT, OT, and IT–OT convergence, belong to the physical-digital level and are anchored in NIST SP 800-82 Rev. 3 [48], IEC 62443 [9], and IMO MSC.428(98) [24]. The fourth interface, the informational interface, belongs to the semantic-cognitive level and is anchored in JP 3-13 [11]. The transition between levels occurs when a physical-digital flow, such as an intrusion into control systems, produces a cognitive effect, such as loss of public trust, or when a semantic flow, such as disinformation, produces a material effect, such as operational disruption.

- **Lower level N1: the ten archetypes grouped into two containers.** The lower level includes the ten archetypes grouped into two containers: six legitimate archetypes and four illegitimate archetypes. This separation corresponds to the legitimacy axis presented in Table 1.

- **Qualitative nature of the framework.** This article does not assign magnitudes, weights, or coefficients to the flows among archetypes, interfaces, and the state of the SoI. The representation is qualitative: each flow is characterized by its direction, expressed as positive or negative polarity ($+$ or $-$), by the

archetype that controls it, and by the technological interface through which it operates. The assignment of numerical values, the calibration of sensitivity coefficients, and the dynamic simulation of the vector C_e belong to the anticipated formal development of the research program. The elements of this later phase are presented in Section 6.5, in line with the extension toward stock-and-flow modeling in Sterman's sense.

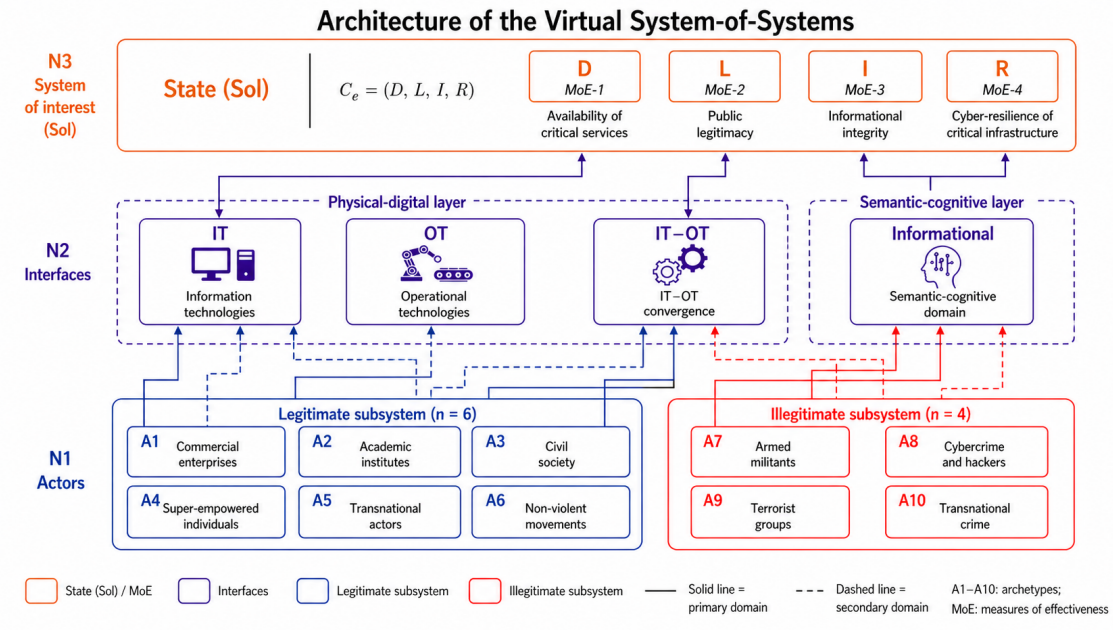

Figure 1. Architecture of the Virtual System-of-Systems analytical framework of non-state actors in relation to the State.

4.4.3. **Boundary of the System of Interest and Level of Abstraction**

ISO/IEC/IEEE 15288:2023 [25] requires the explicit declaration of the SoI boundary. This article delimits the SoI as the State, understood as an aggregated agent in the exercise of Unified Action. This delimitation deliberately excludes intra-state dynamics, such as divergence of interests among agencies, sectoral regulatory capture, and bureaucratic competition, since their analysis belongs to a different level of abstraction documented in [1]. The boundary choice is methodological, not ontological: it does not claim that the State is unitary in the real world; rather, it states that the analysis of flows between NSAs and the State at the level of Unified Action can be treated under an aggregation assumption. Future studies that disaggregate the SoI into constituent systems, such as the Ministry of Defense, cybersecurity agencies, and territorial entities, represent natural extensions of the model.

4.5. Causal Dynamics of the Model

The flows between archetypes and the State are represented through causal loop diagrams (CLDs) in Sterman's notation [47]. Three theoretical clarifications define the status of this instrument, directly derived from Sterman. The model identifies two main loops, R1 and B1, and three inter-archetype interactions (Figure 2).

- A CLD is a structural dynamic hypothesis, not an empirical causal estimate. Sterman [47, Ch. 5.2] states that the validation of a CLD derives from its coherence with mechanisms documented in the literature, not from data fit or econometric identification. Consequently, the arcs of the model are read as structural postulates with bibliographic support for each arc, not as identified causal relations.
- An arc with positive polarity (+) postulates that an increase in the source variable is associated with an increase in the target variable, *ceteris paribus*. An arc with negative polarity (-) postulates an inverse association. The loop type is determined by the algebraic product of the polarities within each individual

loop: a positive product classifies the loop as a positive-feedback loop, whereas a negative product classifies it as a negative-feedback loop. The interaction between loops that share nodes is not resolved by product, but by loop dominance [47, Ch. 5.3], which remains qualitative in this model.

- Sterman [47, Ch. 11] reserves delays and quantitative simulation for stock-and-flow diagrams, not for CLDs. Therefore, the absence of delays and simulation does not invalidate the selected instrument, although it does delimit the analytical scope of the study. The extension toward a stock-and-flow model is proposed as future work.

Polarity in this model operates component-by-component on the vector C_e = (D, L, I, R). No scalar order is assumed. Each arc that names C_e as source or target carries the same sign across the four components: positive across (D, L, I, R) for R1 arcs and negative across (D, L, I, R) for B1 arcs. Mixed-sign cases lie outside the present scope and belong to the stock-and-flow extension. Agency attribution per arc. [47, Ch. 6] requires the declaration, for each arc of a loop, of the actor that controls the source variable. In loops R1 and B1, this attribution is made explicit in Tables 4 and 5.

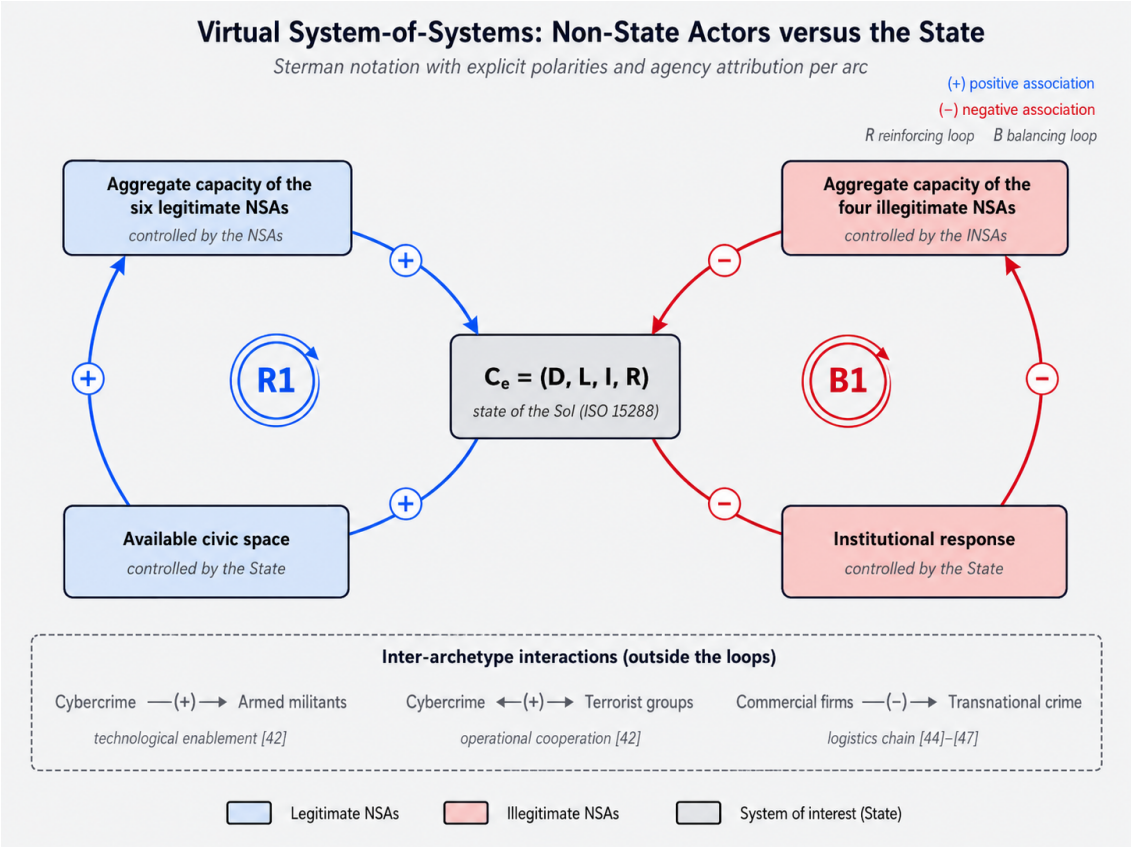

Figure 2. Virtual System of Systems (SoS) Non-State Actors Vs. the State. Own elaboration.

4.5.1. **R1 Positive-Feedback Loop and B1 Negative-Feedback Loop**

On the variable "aggregate capacity of the six NSAs", Maier, Section 4, excludes global scalar aggregation in a Virtual SoS [29]. The expression "aggregate capacity" is defined as the vector projection of the flows from the six archetypes onto the four technological interfaces: IT, OT, IT–OT, and Informational. It is not an algebraic sum; it is an observable vector, interface by interface. The same definition applies to the "aggregate capacity" of the four INSAs represented in B1.

The structural interpretation of R1 comprises three arcs. Arc 1: the vector projection of the NSAs onto the four interfaces is associated with positive shifts in the C_e components, through services (D), knowledge (I), legitimacy (L), and demand for institutional quality (R). Signs per component are declared in the new sign

table. Arc 2: the C_e vector is associated with a rise in functional civic space, expressed in stable regulatory frameworks, public research funds, contracts with the private sector, formal channels for participation, and procedural safeguards for peaceful protest; this arc is controlled by the State. Arc 3: functional civic space is associated with a rise in the capacity of the legitimate NSAs. The State controls the source variable through the same institutional conditions declared in Arc 2; the loop closes through coevolution, which Sterman admits as a valid agency pattern when one actor sustains the precondition that other actors then exploit. This structure is a coevolution loop in Sterman's sense, not one-way causation: civic space is partly endogenous to NSAs, and that endogeneity is precisely the object of the feedback loop [47].

Table 4. R1 positive-feedback loop

Arc	Origin	Destination	Polarity	Actor that controls the source variable
1	Aggregate capacity of the six NSAs	C_e	+	The six NSA archetypes, under operational independence.
2	C_e	Available civic space	+	The State, through regulatory and institutional decisions.
3	Available civic space	Aggregate capacity of the six NSAs	+	The State, through the institutional conditions declared in Arc 2; the loop closes through coevolution among the six archetypes.

Note. Structure of the R1 positive-feedback loop with agency attribution. Product of polarities: $(+)(+)(+) = +$. Classification: positive feedback. Own elaboration.

The structural interpretation of B1 comprises three arcs. Arc 1: the vector projection of the four INSAs onto the interfaces is associated with negative shifts in the C_e components: service disruption and infrastructure damage (D, R), legitimacy loss (L), and informational degradation through illicit asset concealment (I). Arc 2: negative shifts in any C_e component are associated with a rise in institutional response, expressed in military operations, prosecution, financial regulation, cyber defense, and international cooperation [2;13–16]; the polarity of this arc is negative because lower C_e implies greater response pressure. Arc 3: institutional response is associated with a decline in the capacity of the INSAs.

Table 5. B1 negative-feedback loop

Arc	Origin	Destination	Polarity	Actor that controls the source variable
1	Aggregate capacity of the four INSAs	C_e	−	The four illegitimate archetypes.
2	C_e	Institutional response	−	The State, through capability mobilization decisions.
3	Institutional response	Aggregate capacity of the four INSAs	−	The State, through response execution.

Note. Structure of the B1 negative-feedback loop with agency attribution. Product of polarities: $(-)(-)(-) = -$. Classification: negative feedback. Own elaboration.

The R1+B1 topology supports a conditional conjecture of mutual non-eradication, contingent on bounded institutional response, civic-space coevolution, and absence of exogenous collapse. Sterman Chapter 5.3 reserves loop-dominance claims for state-dependent analysis, not for topology alone [47]; under state monopoly in Tilly's sense, the conjecture lapses [49].

4.5.2. **Inter-Archetype Interactions**

The R1 and B1 loops capture intra-subsystem dynamics. Table 6 formalizes three inter-archetype interactions relevant to the maritime domain, each one with a mechanism documented in a specific source.

Table 6. Inter-archetype interactions and their effect on the loops

#	Interaction	Type	Documented mechanism	Effect
1	Cybercrime–armed militants	Technological enablement	Provision of cyber tools and services through illicit markets [23].	Amplifies the negative effect of B1.
2	Cybercrime–terrorist groups	Operational cooperation	Functional convergence documented in cyberterrorism literature [23].	Amplifies the negative effect of B1.
3	Commercial firms–transnational crime	Logistics chain	Use of legitimate infrastructure, such as transport, finance, and platforms, by illicit networks [18;22;28;54].	Transfers capacity from R1 to B1.

Note. Own elaboration.

The third interaction is especially relevant to the maritime domain. Port logistics chains support legitimate foreign trade and may reinforce R1; however, the reviewed literature also documents their use as a vector for cocaine trafficking through containers, which may reinforce B1 [18;21;22;28;54]. Thus, the same port system can participate in both loops, depending on the actor, purpose, and governance condition.

4.6. Interaction Matrix and Sensitivity Analysis

4.6.1. Interaction Matrix

The model includes eleven nodes: ten archetypes and the State. Among them, there are 110 possible directed relations. Table 7 records only the cells with sufficient direct documentary evidence to assign polarity. Therefore, the inclusion criterion reflects bibliographic support, not the real existence or absence of interaction. The cells coded as 0 do not indicate empirical absence. They indicate insufficient direct documentary evidence at this stage of the analysis.

Table 7. System-of-Systems interaction matrix.

Origin \ Destination	Emp	Aca	CS	Ind	Tns	NoV	Mil	Cyb	Ter	Crm	State (reg. interface)
Commercial firms (Emp)	—	+	0	+	+	0	0	±	0	−	+
Academia (Aca)	+	—	+	+	+	+	0	0	0	0	+
Civil society (CS)	+	+	—	0	+	+	0	0	0	0	+
Individuals (Ind)	+	+	+	—	+	+	0	0	0	0	+
Transnational actors (Tns)	+	+	+	+	—	+	0	0	0	0	+
Non-violent movements (NoV)	0	+	+	+	+	—	0	0	0	0	+
Armed militants (Mil)	−	0	0	0	0	0	—	0	+	+	−
Cybercrime (Cyb)	−	0	0	0	0	0	+	—	+	+	−
Terrorist groups (Ter)	−	0	0	0	0	0	+	+	—	+	−
Transnational crime (Crm)	−	0	0	0	0	0	+	+	+	—	−
State (reg. interface)	+	+	+	±	+	±	−	−	−	−	—

Note. The cell $(row, column)$ indicates the documented dominant effect of the row actor on the column actor. Convention: $+$, dominant positive effect; $-$, dominant negative effect; $\pm$, ambivalent effect; 0, insufficient direct documentary evidence. Own elaboration.

Thus, a cell with assigned polarity and a cell coded as 0 do not differ by nature; they differ by level of bibliographic support. The Emp/Cyb cell $(\pm)$ represents the exposure of commercial firms to cybercrime. In this relation, firms act mainly as victims, although unfair competitive use may exist. The State/Emp cell $(+)$ represents the State's regulatory relation with firms through supervision, critical-chain protection, and public procurement. These cells belong to different dimensions. According to Sterman's net-polarity rule, each cell represents the predominant relation in its own dimension, not an aggregation of all possible dimensions [47]. The cells marked as $(\pm)$ indicate documented ambivalence. The State response to super-empowered

individuals may oscillate between cooperation and regulation. The State response to non-violent movements may oscillate between democratic openness and restriction of civic space. The State row and column in Table 7 represent the regulatory interface, not the system of interest defined in Section 4.4.2. This clarification avoids conflating the State as a matrix node with the State as the model's SoI.

4.6.2. **Quadrant-Based Interpretation**

Three conclusions derive from decomposition of the quadrant.

- The analysis posits a relative concentration of intra-illegitimate cooperation as a structural hypothesis: eleven of twelve coded cells receive positive polarity under single-coder documentary review. The count reflects coding choices, not an independent finding, and requires validation through double coding with inter-coder agreement statistics.
- In the quadrant that records the influence of the legitimate subsystem on the illegitimate subsystem, only one of twenty-four cells receives negative polarity: commercial firms–transnational crime. The study posits this relation as the best-documented transfer hypothesis from the legitimate subsystem to the illegitimate subsystem, with the framework as a representation tool and the reviewed corpus as evidence base. The assignment may reflect bibliographic selection bias; other plausible routes (academic platforms, cloud infrastructure, lawful financial networks) fall outside the corpus rather than outside the phenomenon.
- The State response to legitimate archetypes is not uniformly positive. Ambivalent cells State–individuals and State–non-violent movements reflect tensions among civic openness, regulation, and public order.

4.6.3. **Qualitative Sensitivity Analysis**

The conditions in Table 8 must be read as a qualitative exploration of structural rupture scenarios, not as a quantitative sensitivity analysis in the strict sense [22;28;45;46;54].

Table 8. Conditions for structural persistence rupture and affected loop

#	Condition	Loop	Mechanism
1	State capture by private NSA interests	R1	The loop loses its virtuous character because civic space closes to other legitimate archetypes.
2	Co-option of academia or civil society by INSAs	R1 degradation and B1 reinforcement	Transfer of legitimate capacity to the illegitimate subsystem. This condition operates as a model extension, not as a sensitivity probe of the declared topology; it is presented for future-work prioritization.
3	Military overextension of the institutional response	B1	The institutional response loses proportionality and erodes C_e through cost and legitimacy loss.
4	Reinforcement of intra-illegitimate interactions	B1	The illegitimate subsystem becomes more resilient to institutional response.
5	Expansion of the leakage point Commercial firms → transnational crime	R1 → B1	Legitimate economic infrastructure becomes effective infrastructure for the illegitimate subsystem.

Note. Own elaboration.

4.7. Application to the maritime Domain

The application to the maritime domain is developed at an exploratory level through three mechanisms documented in the reviewed literature.

- **Mechanism 1: Capacity transfer through container transport.** The logistics chains operate both as infrastructure for legitimate foreign trade and as a vector for cocaine traffic through containers

[18;22;28;54]. In the analytical framework, this dual use is represented as a negative relation between commercial firms and transnational crime. In analytical terms, this relationship suggests that port traceability and technology-assisted customs control constitute sensitive control points [20].

- **Mechanism 2: Cyber enablement of armed operations.** Armed dissident groups operate on river corridors and along the borders. Civil digital infrastructure, such as mobile networks, encrypted message services, and cryptoassets, supports their logistics and financial operations [18]. In the analytical framework, this interaction is represented as a positive relation between cybercrime and armed militants, in the sense of functional enablement among illegitimate archetypes. At an exploratory level, this result suggests the relevance of financial intelligence and cross-border cooperation.
- **Mechanism 3: Contest over the informational domain of naval operations.** The projection of narratives on actions of the navy occurs in the informational domain, with participation of the media, civil society, influential individuals, and, at times, disinformation networks with non-state links [21]. In the model, this mechanism is mainly linked to the integrity of the information (I), as a component of the vector C_e.

4.8. *Synthesis of Results*

- The interaction matrix turns the typology into a systemic network. The ten archetypes operate as nodes with polarities derived from the reviewed literature, not as isolated categories. Each cell rating depends on the selected corpus and constitutes an auditable structural hypothesis, not an independent empirical result.
- The structural persistence of the System-of-Systems, under the R1+B1 topology, depends on five auditable conditions.
- For this study, the maritime domain presents three concrete application mechanisms. Their doctrinal formulation is developed in Section 5.

4.9. *Qualitative Criteria for Structural Model Assessment*

Sterman proposes a set of criteria to evaluate system dynamics models [47, Ch. 21]. Some of those criteria require quantitative simulation and remain outside the scope of this study. The rest can be examined qualitatively in a CLD. Table 9 summarizes the analytical correspondence of the framework with those criteria, without equivalence to empirical validation of the model.

Taken together, the framework shows analytical correspondence with qualitative criteria of structure, boundary, and consistency applicable to a CLD. Quantitative contrast remains a later agenda, linked to extension toward stock-and-flow, in line with the declared limits of the study.

5. Discussion

5.1. *Position Relative to Prior Typologies*

The typologies proposed by Wijninga et al., Muñoz, Restrepo, Trejos, and the National Intelligence Council report provide useful descriptive classifications; however, none of them incorporates the technological dimension as a structural axis or formalizes interactions among archetypes within a systems architecture framework. Table 1 of this article preserves the categories recognized by that literature and introduces two verifiable modifications [34;35;42;50;52]. First, the technological domain ceases to be a secondary descriptor and becomes a classification axis, anchored in sectoral technical standards [9;11;24;48]. Second, the typology is linked to a systemic model with source-based polarities, which converts the archetypes into nodes of an auditable network. In this sense, the article proposes a different analytical level. Prior typologies operate mainly at the level of classification, whereas the model proposed here operates at the level of systemic architecture, with a structural dynamic hypothesis in Sterman's sense [47, Ch. 5]. The difference is therefore one of analytical function: prior typologies describe actor categories, whereas the proposed model postulates interaction mechanisms that can be examined through qualitative validation tests [47, Ch. 21].

5.2. *Theoretical Contribution of the Model*

The article's contribution rests on the disciplined assembly of three mature theoretical bodies.

5.2.1. Maier applied to non-state actors. The five attributes of the Virtual System-of-Systems, namely operational independence, managerial independence, geographic distribution, emergent behavior, and evolutionary development, are verified point by point in Table 3 for the set of ten archetypes in relation to the State [29]. This application addresses a theoretical tension left open by prior literature on non-state actors: how to analyze a set of entities without common authority or shared purpose without recourse to scalar aggregation. Maier explicitly excludes global aggregation in a Virtual SoS, which requires the state of the system of interest to be represented as a vector, (D, L, I, R), not as an index [29]. The result is a model that preserves the ontological heterogeneity of the set without loss of analytical tractability.

Table 9. Qualitative criteria for structural model assessment in relation to Sterman.

Criterion	Content	Analytical correspondence
Boundary adequacy	System boundary appropriate for the purpose	Boundary declared in Section 3.4.3; SoI at the level of aggregated Unified Action.
Structure assessment	Structure consistent with knowledge of the real system	Conceptual compatibility with Maier's attributes assessed in Section 3.4.1 and Table 3.
Dimensional consistency	Units consistent across variables	C_e vector defined by four distinct MoE, observed by component and without scalar aggregation; technological interfaces explicitly declared.
Parameter assessment	Assumptions and conventions consistent with descriptive knowledge	Appendix A strengthens transparency by showing each coded relation, its sign, source, and brief justification. This is an auditability improvement, not a correction of inconsistency.
Extreme conditions	Plausible behavior under extreme conditions	Five rupture conditions in Table 8; limit case of state monopoly in Tilly's sense, as stated in Section 3.5.1 [49].
Integration error	Not applicable to CLD	Not applicable.
Behavior reproduction	Requires quantitative simulation	Outside the scope; reserved for stock-and-flow.
Behavior anomaly	Requires quantitative simulation	Outside the scope.
Family member	Model applicable to systems of the same family	Potential extension to NSA typologies in other countries, with archetype adjustment and later empirical contrast.
Surprise behavior	Identification of unanticipated behavior	Intra-illegitimate hypothesis posited by the study from the consulted corpus: eleven of twelve cells with positive polarity. The 'emergent' label remains conditional on validation through independent double coding.
Sensitivity analysis	Model response to structural shifts	Qualitative exploration of structural rupture scenarios in Section 3.6.3 and Table 8.
System improvement	Model guides intervention	The framework highlights the best-documented transfer hypothesis, Commercial firms/Transnational crime; Section 5 develops its implications.

Note. Own elaboration.

5.2.2. ISO/IEC/IEEE 15288:2023 applied to the State as the system of interest. The delimitation of the SoI at the level of aggregated Unified Action is explicitly declared in Section 3.4.3 [25]. The boundary decision does not assert the ontological unity of the State. It states that the analysis of flows between NSAs and the State at the level of Unified Action is tractable under an aggregation assumption. The treatment of the SoI state through four independent measures of effectiveness, in the strict sense of the standard, anchors the discussion in dimensions that are observable in principle:

availability, legitimacy, informational integrity, and cyber-resilience. It does so without commitment to a composite index.

5.2.3. Sterman applied to national security. The formalization of NSA/INSA–State flows as causal loop diagrams with polarities and agency attribution per arc constitutes an uncommon application in the field of national security with non-state actors [47]. The distinction between structural persistence and dynamic equilibrium resolves a recurrent problem in the hybrid warfare literature, where the term "equilibrium" is often used as a metaphor [47, Ch. 5.5]. The model makes explicit that the property of mutual non-eradication between the State and INSAs is a topological property of the R1+B1 loop system. It is conditional on the declared topology and is not universal. Under strong state monopoly conditions in Tilly's sense, the topology changes and the property no longer applies [49].

5.2.4. Copi as a criterion of argumentative validity. The model's inferences are distinguished by their logical status. Statements about loop structure are deductive: they derive necessarily from the declared topology. Statements about empirical patterns, such as intra-illegitimate cooperation visible in maritime corridors, are inductive, and their force depends on cited support, not on authorial assertion [8]. This distinction is not decorative; it defines what is demonstrated and what is conjectured with support, and it removes circular argument patterns identified in the original text.

5.3. Emergent Patterns of the Model

The interaction matrix allows the identification of two patterns that deserve attention within the proposed framework. They are not presented here as conclusive empirical findings, but as analytical results that help order the discussion and guide the institutional interpretation of the problem.

The first hypothesis concerns intra-illegitimate cooperation. In the intra-illegitimate quadrant, eleven of the twelve cells receive positive polarity under the study's documentary coding. The result does not demonstrate a general rule. It is not an independent system finding either, since coding and pattern observation come from the same source. Its value is heuristic: it orients future validation with double coders under a declared protocol. In the Colombian case, it is therefore reasonable to design the State response under the assumption of opportunistic cooperation among these actors, not under the expectation that they will automatically compete with one another.

The second hypothesis concerns transfer concentration from the legitimate subsystem. In the NSA–INSA quadrant, only one of twenty-four cells receives negative polarity: commercial firms–transnational crime. The study posits this relation as the best-documented transfer hypothesis from the legitimate subsystem to the illegitimate subsystem within the reviewed corpus. The postulation represents neither ontological exclusivity nor an independent finding. It is the best-supported cell within the matrix constructed in the study and constitutes a hypothesis with documentary support that requires external contrast for prioritization. For this reason, measures such as supply-chain due diligence, transaction oversight, and port traceability appear as reasonable intervention priorities.

5.4. Design Implications

The model exhibits four properties. The first property is the declaration of the SoI state through four observable components, (D, L, I, R), which replaces rhetorical references to "security" with delimited dimensions. The second property is the decomposition of every interaction through four technological interfaces, IT, OT, IT–OT, and Informational, anchored in technical standards [9;11;24;48]. This removes the vague category of "advanced technologies". The third property is the ontological distinction between the physical-digital level and the semantic-cognitive level, derived from Floridi, which makes the transition between layers explicit and avoids an undeclared mixture of analytical planes [17]. The fourth property is the classification of each flow with declared polarity and documentary reference, which converts the model into an auditable artifact. The systems architecture position is not a peripheral addition. It is the framework that sustains the analysis and distinguishes the article from a strictly doctrinal or strategic contribution.

5.5. Limits of the Study

Three limits define the scope of the conclusions. The first is the qualitative character of the polarities. The model declares direction and sign but not magnitude. Sterman reserves magnitude for stock-and-flow diagrams, whose incorporation constitutes the natural extension of the model [47]. The second is the absence of delays. The selected instrument, the CLD, does not admit delays; these belong to the stock-and-flow level. An extension with delays would permit the analysis of temporal trajectories and the discrimination of scenarios by response horizon. The third is the application to a single domain with bibliographic asymmetry: the corpus concentrates on container traffic and under-samples other plausible transfer routes, so the concentration in Sections 4.6.2 and 5.3 may reflect this asymmetry rather than the system itself. Sterman's ninth test, family member, indicates that the model can extend to other domains, such as land-border, air, and space domains, with adjustment of dominant archetypes and without change to the theoretical structure [47, Ch. 21].

5.6. Falsifiability Conditions

The framework declares three refutation conditions: (i) independent double coding of Table 7 below Cohen's $\kappa = 0.60$ collapses the structural-hypothesis status of the matrix; (ii) documented transfer routes with empirical weight comparable to the firms–transnational-crime route invalidate the priority of Section 4.6.2; (iii) systematic mixed-sign behavior in C_e components under the same arc breaks the polarity rule of Section 4.5.

6. Institutional Implications for Unified Action

This section translates the model results into institutional implications. Its separation from Sections 4 and 5 preserves the methodological criterion defined in Section 3.4. Each strategy has support in a table or in a loop of the model.

6.1. Core Principle: Control of the Best-Documented Transfer Hypothesis

The analysis treats the commercial firms–transnational crime relation as the best-documented transfer hypothesis from the legitimate subsystem to the illegitimate subsystem within the reviewed corpus. The proposed framework represents this relation; it does not validate it empirically. The hypothesis has documentary support, but its priority still requires external assessment and broader bibliographic coverage. In the NSA–INSA quadrant, only one of the twenty-four possible cells has negative polarity, and that cell links commercial firms to transnational crime. This result should not be read as ontological exclusivity, but as the best-supported relation within the constructed matrix. For this reason, supply-chain control, financial transaction oversight, and port traceability emerge as reasonable initial intervention priorities, because they address the main logistical and financial channels through which legitimate infrastructure may be exploited by transnational crime. These measures are not exhaustive; they derive directly from the transfer hypothesis identified in the matrix, a point that is also consistent with the reviewed literature on the illicit use of legitimate logistical, financial, and port infrastructure by transnational crime. This principle guides the strategies that follow and is especially relevant to the maritime domain, particularly to the mechanism associated with container transport.

6.2. Differentiated Strategies by Actor and Institutional Function

The seven strategies are organized by the position of the relevant actors and institutional functions within the framework, their relation to the interaction matrix in Table 7, and their contribution to loops R1 or B1.

5.2.1. Local Governance of Territorial Entities. Territorial entities are not part of the non-state actor typology. However, they remain decisive for the model because a significant part of critical service continuity and cyber-resilience depends on the subnational level. Therefore, this strategy proposes clear coordination between national and territorial levels, explicit distribution of competencies, minimum operational continuity capacities, and common criteria for incident response. It also

requires transparency in policy implementation and basic follow-up mechanisms that identify what works, where gaps persist, and which capacities require reinforcement. In model terms, this strategy acts mainly on cyber-resilience (R) and reinforces the institutional conditions that support Arc 2 of loop R1.

5.2.2. Regulation and Incentives for Commercial Firms. Within the model, commercial firms occupy an especially sensitive position because the Commercial firms–Transnational crime relation represents the best-documented transfer hypothesis from the legitimate subsystem to the illegitimate subsystem. Therefore, this strategy deserves preferential treatment within the proposed set of measures. Its content combines three lines of action: strict application of Law 1340 against restrictive practices and corporate concentration; tax incentives conditioned on verifiable supply-chain due diligence and responsible data management; and risk-based supervision supported by information systems, RegTech and SupTech tools, plus independent audits. The objective is not indiscriminate expansion of control, but the reduction of criminal infiltration opportunities in logistics, financial, and platform infrastructure without harm to legitimate economic activity.

5.2.3. Promotion of Science and Academia. Academic institutes channel their contribution to loop R1 through technical knowledge that supports informational integrity (I) and cyber-resilience (R). The strategy finances focused research on priority problems, promotes alliances with the public sector for knowledge transfer with technological management, and establishes dual-use research governance. This governance includes responsible disclosure with risk assessment, access control for data and infrastructure, and traceability. Rupture condition 2 in Table 8, co-option of academia, justifies the dual-use component.

5.2.4. Participation and Transparency for Civil Society and Non-Violent Movements. In the model, the relation between the State and civil society appears mainly positive, whereas the relation with non-violent movements includes documented ambivalence, associated with the tension among democratic openness, regulation, and public order. Therefore, the strategy should not rest on a generalized suspicion logic, but on protected participation, transparency proportional to risk, and clear rules for institutional dialogue. In operational terms, this implies the reinforcement of formal participation channels, accountability standards consistent with the nature of each actor, and use of oversight and data analysis tools only to detect capture, co-option, or illegitimate instrumentalization, without criminalization of protest or reduction of civic guarantees. This strategy acts mainly on public legitimacy (L) and, in contexts of narrative dispute, also on informational integrity (I).

5.2.5. Regulation of Super-Empowered Individuals. The State–super-empowered individuals cell appears as ambivalent in Table 7, which reflects the regulation–cooperation tension. The strategy defines verifiable criteria for significant influence: control of platforms and data, capacity for informational segmentation, and funds with effect on the public agenda. It also requires transparency of interests and traceability of intervention. Supervision focuses on information-system audits and automated decisions when these affect third parties, with a graduated sanction scheme for non-compliance. This strategy operates on the L and I components of C_e.

5.2.6. International Cooperation for Transnational Actors. The condition of a geographically distributed archetype by definition, verified as Maier's third attribute in Table 3, requires a coordinated response beyond national jurisdiction. The strategy combines three components: agile judicial assistance and preservation of digital evidence for cross-border cases; structured information exchange and operational coordination through incident response networks; and accountability in multilateral forums with traceability safeguards.

5.2.7. Capabilities Against Illegitimate Archetypes. The four illegitimate archetypes constitute the subsystem of loop B1. The result of high intra-illegitimate cooperation, with eleven of twelve positive cells, imposes an operational consequence: the institutional response cannot assume competition

among these actors, but must assume functional cooperation. The strategy develops counterinsurgency, counterterrorism, and organized-crime capabilities oriented to the degradation of adversarial recruitment, coordination, and fund flows, with intelligence integrated into information systems and data analysis. It protects infrastructure and critical services, sustains evaluated deradicalization programs, and guarantees legality, human rights, and accountability. It acts with particular emphasis on Arc 3 of loop B1.

6.3. Objectives for the Institutional Policy of the Colombian Armed Forces

The six objectives below derive from specific properties of the model, not from a generic authorial recommendation.

6.3.1. Solid Empirical Evidence. Every claim about NSA influence and impact must rely on verifiable data and reproducible metrics of performance and digital resilience: service availability and continuity, mean time to detect and respond, and functional degradation under attack. This objective corresponds to the operationalization of the vector $C_e = (D, L, I, R)$ as measures of effectiveness in the sense of ISO/IEC/IEEE 15288:2023, as stated in Section 4.4.2 [25].

6.3.2. Balanced Approach to Benefits and Externalities. NSA assessment requires a distinction between contributions, as input to loop R1, and risks, as input to loop B1, through a multi-criteria assessment that preserves proportionality, legality, and rights. This objective corresponds to the preservation of the R1+B1 structure of the model.

6.3.3. Nuanced Capability Analysis. The assessment of institutional adaptability requires digital maturity indicators for interoperability, data governance, incident management, digital skills, and institutional architecture across the four technological interfaces declared in Section 4.4.2 This assessment may use digital government maturity methods and comparative GovTech instruments.

6.3.4. Explicit Treatment of Counterarguments. Institutional policy must incorporate risks derived from the model: State dependence on private providers, with potential saturation of loop R1; bias and opacity in automated systems, with effects on I; technological overreaction, as rupture condition 3 in Table 8; and potential institutional abuse. It must recognize the trade-off between rapid technical competence acquisition and effective public control.

6.3.5. Measurable Links to Security Impacts. Every debate on social norms, disruptions, or digital influence must translate into measurable effects on the components of the C_e vector: interruption of critical services (D), effects on logistics chains, degradation of command and control, and loss of public trust (L). This objective anchors policy in observable components.

6.3.6. Specific Metrics and Indicators. Institutional policy requires an assessment cycle that combines technological maturity for adoption and cyber-resilience maturity (R), with priority on technologies of verifiable operational value and controlled risk. This objective corresponds to Sterman's tests 3, dimensional consistency, and 11, sensitivity analysis, applied to public policy [47].

With these objectives, the institutional policies of the Colombian Armed Forces can address the challenges and opportunities posed by NSAs with analytical rigor. Institutional doctrines should incorporate these concepts to counter hybrid warfare [13;15;34;50].

6.4. Ethical Considerations

The ethics of NSA analysis in national security is inseparable from the ethics of novel technologies. Data, platforms, automation, and cyber-physical systems amplify the influence of the archetypes and act through the four technological interfaces of the model, as defined in Section 4.4.2 The risk is not limited to lethal operations or disinformation. It includes intrusions against critical infrastructure, with effects on R; manipulation of the informational environment, with effects on I; and exploitation of digital chains.

This situation requires verifiable responsibility for design, deployment, and control of these capabilities. In contexts with weak regulatory frameworks, cyber ethics must make explicit the rules for data use, such as purpose, minimization, access control, and audit, and for digital surveillance, such as necessity, proportionality, and independent oversight, to avoid a drift of the State response toward social control.

The dual-use dilemma requires explicit safeguards: the same technologies that protect can also serve coercion or escalation. Human control and accountability must be preserved in critical functions. Effective enforceability of ethical standards on data, automation, surveillance, and dual use is a condition for the management of NSA impact without erosion of legitimacy (L) or democratic principles.

6.5. *Future Work*

The future research agenda comprises four lines derived from properties of the model.

- The first line extends the current CLD to a stock-and-flow diagram in the sense of Sterman [47, Ch. 11], with the incorporation of delays and the quantification of flows between archetypes and interfaces. This extension enables Sterman's tests 7 and 8, which remain outside the scope of the CLD, as shown in Table 9. The preliminary design of this extension is presented in Table 10.

Table 10. Initial design proposal for the quantification phase.

Element	Description
Initial proposal	To anticipate the transition from the heuristic framework to a formal quantitative model, this section presents the descriptors and mathematical structure proposed for future research. The terms below are design proposals, not estimated or calibrated parameters in the present study.
Flow intensity ω_{ij}	Descriptor of the relative magnitude of the flow from archetype i to interface j. In a later phase, ω_{ij} will be calibrated from sectoral documentary evidence and operational indicators for each technological interface.
Impact direction σ_{ij}	Categorical variable $\sigma_{ij} \in \{+1, -1\}$ that encodes the expected orientation of the flow on SoI stability. It corresponds to the quantitative translation of the qualitative polarity declared in this article.
Perturbation type τ_{ij}	Variable that distinguishes adaptive perturbations from disruptive perturbations. It permits separation between gradual-change trajectories and abrupt shocks in the simulated behavior.
Sensitivity coefficient α_{jk}	Coefficient that links each interface j to each component $k \in \{D, L, I, R\}$ of the C_e vector. Calibration of α_{jk} will require primary data from the maritime domain and remains outside the scope of the present article.

Note. The present article provides the conceptual structure on which this quantification phase can be constructed. Own elaboration.

- The second line designs comparable measurement frameworks for the vector $C_e = (D, L, I, R)$, in the strict sense of ISO/IEC/IEEE 15288:2023 [25]. The integration of maturity frameworks for governance, identification, protection, detection, response, and recovery, together with operational metrics for detection time, recovery time, and functional degradation level, will convert the four declared MoE into instrumented measures.
- The third line develops instrumented studies of the maritime domain, including ports, logistics, cyber-physical infrastructure, and information networks. These studies require replicable measurements and dependency traceability for empirical tests of the three mechanisms presented in Section 4.7.
- The fourth line models the institutional competence-control dilemma and develops cyber safeguards for data governance, digital surveillance, and dual-use technologies, with risk assessment of informational manipulation and verifiable accountability in automated decisions. It also enables the disaggregation of the State as SoI, declared in Section 4.4.3, into constituent systems. This disaggregation constitutes a natural extension identified in the model boundary statement.

The mathematical structure proposed for the quantification phase is a state-dynamics expression of the form:

$$\frac{dC_k}{dt} = \sum_i \sum_j \omega_{ij}\, \sigma_{ij}\, \alpha_{jk}\, \Phi(\tau_{ij}), \quad k \in \{D, L, I, R\}, \quad t \in \mathbb{R}_{\geq 0}, \tag{1}$$

where $C_k(t) \in [0, 1]$ denotes the normalized state of each C_e component, with initial condition $C_k(0)$ obtained from the operational sources declared in Section 3.4.2; $\omega_{ij} \geq 0$, $\sigma_{ij} \in \{+1, -1\}$, $\alpha_{jk} \in \mathbb{R}$, and $\Phi : \{\text{adaptive, disruptive}\} \to \mathbb{R}$ is the transmission function. Equation (1) is a design proposal, not a calibrated model: parameter estimation, functional form of Φ, and feedback among C_e components belong to the later formal phase.

7. Conclusions

The article proposes a heuristic analytical framework based on a Virtual System-of-Systems to assess the interaction between non-state actors and the State in the maritime domain. The novelty of the work does not lie in the claim that elements developed by other traditions are original, but in their articulation within a single analytical architecture: an archetype typology, a system of interest defined under ISO/IEC/IEEE 15288:2023, and a causal representation based on Sterman's notation.

On this basis, the study does not aim to offer empirical validation or a calibrated system simulation. Its contribution is more precise and, for that reason, more defensible: it orders relations, distinguishes technological interfaces, reveals interaction patterns, and opens a reasoned path for Unified Action. Within this framework, Table 3 shows conceptual compatibility with Maier's attributes, and Table 9 summarizes the model's correspondence with qualitative criteria for structural assessment applicable to a causal loop diagram.

The effect of non-state actors on governance and security is sectoral and contingent. It does not displace the State, but it modifies part of the conditions under which the State acts. Technological mediation amplifies this effect when archetypes control data, platforms, or cyber-physical systems. This does not amount to a linear decline of the State. Rather, it shows that State capacity depends, with increased force, on the simultaneous preservation of governance, technical competence, and accountability.

In the intra-illegitimate quadrant, eleven of twelve cells show positive polarity. Rather than prove a general law, this pattern suggests that, in the analyzed domain, functional cooperation among illegitimate actors may be more frequent than traditional security doctrine tends to assume. For Unified Action, the implication is concrete: it is more prudent to design the response under the assumption of opportunistic coordination among these actors than under the expectation that they will compete with one another automatically.

In the NSA–INSA quadrant, only one of the twenty-four possible cells shows negative polarity: Commercial firms–Transnational crime. Within the model, this relation represents the best-documented transfer hypothesis from the legitimate subsystem to the illegitimate subsystem. It should not be read as ontological exclusivity, but as the best-supported relation within the constructed matrix. For this reason, measures such as supply-chain due diligence, transaction oversight, and port traceability appear here as reasonable intervention priorities.

The main vulnerability of the State against illegitimate archetypes does not lie in the absence of instruments, but in the difficulty of sustaining critical services when disruption persists. Therefore, rather than accumulate capacities in abstract terms, it is preferable to secure a minimum threshold of continuity and cyber-resilience: verifiable basic controls, periodic exercises, defined notification and recovery times, and effective coordination between national and territorial levels. When data maturity permits, the use of digital twins may help identify critical dependencies and prioritize responses. This line of action is especially relevant for territorial entities, private operators, and academic actors that manage infrastructure or sensitive information, and it aims to reduce the probability that an intrusion becomes sustained disruption.

The influence of firms, super-empowered individuals, civil society, and academia increases when they control data, platforms, or automated processes. The State response should not rely on diffuse control or expansive surveillance, but on verifiable rules: effective competition, supply-chain due diligence, responsible

data management, independent audit, and clear proportionality limits. At the same time, the operational advantage of militant, cybercriminal, and transnational crime networks depends largely on distributed infrastructure and jurisdictional friction. For this reason, coordination between digital evidence preservation, cross-border cooperation, and joint work by response and investigation teams appears here not as an abstract ideal, but as an operational need.

In current security scenarios, technology cuts across both material operations and disputes over information and public perception. Therefore, the analysis cannot be limited to infrastructure and networks; it must also consider narratives, institutional trust, and content circulation. In the maritime domain, this dual dimension requires the combination of technical resilience, traceability, and rights protection. The proposed framework offers an ordered way to interpret these interactions and guide institutional decisions, without replacing the empirical test that remains as a subsequent task.

Funding: This research received no external funding

Institutional Review Board Statement: Not applicable. This study did not involve humans or animals, and no human-subject testing, intervention, survey, interview, experiment, or collection of personal data was conducted.

Informed Consent Statement: Not applicable. This study did not involve humans, patients, human-subject testing, surveys, interviews, experiments, or the collection of personal or identifiable data.

Acknowledgments: The author declares that no administrative, technical, material, or institutional support requiring acknowledgment was received for this study.

Conflicts of Interest: The author declares no conflict of interest. No funders had any role in the design of the study, in the collection, analysis, or interpretation of data, in the writing of the manuscript, or in the decision to publish the results.

References

1. Acemoglu, D. and Robinson, J. A. (2017). *Why nations fail: the origins of power, prosperity, and poverty*. Deusto. https://ia801506.us.archive.org/27/items/WhyNationsFailTheOriginsODaronAcemoglu/Why-Nations-Fail_-The-Origins-o-Daron-Acemoglu.pdf. Accessed: Apr. 22, 2025.
2. Armada Nacional de Colombia (ARC), Guerra La Rotta, G. A., Velandia, G. A. G., Sarria, R. S. F., and Rondon, H. L. (2024). *OP 3-4.1*. Armada Nacional de Colombia, Colombia.
3. Ataç, I., Schwiertz, H., Jørgensen, M. B., Vandevoordt, R., Hinger, S., and Spindler, S. (2023). Negotiating Borders through a Politics of Scale: Municipalities and Urban Civil Society Initiatives in the Contested Field of Migration. *Geopolitics*, 29(2):714–740. DOI: 10.1080/14650045.2022.2129732.
4. Balanzó, A., Nupia, C. M., and Centeno, J. P. (2020). Conocimiento Científico, Conocimientos Heterogéneos y Construcción de Paz: Hacia Una Agenda de Investigación sobre Políticas y Gobernanza del Conocimiento en Transiciones Hacia la Paz. *OPERA*, (27):13–44. DOI: 10.18601/16578651.n27.02.
5. Bolaños, R. M. (2024). Los Tenientes Generales Hablan: El Terrorismo como Causa de la Involución Militar. *Historia del Presente*, 43(2):119–133. https://dialnet.unirioja.es/servlet/articulo?codigo=9629490. Accessed: Sep. 30, 2024.
6. Bulla, P. and Lleras, M. E. (2022). *Impulsar la Acción Unificada Entre Civiles y Militares*, volume 9. Open Society Foundations, Bogotá, 1st edition. https://multimedia.ideaspaz.org/especiales/aunnoestarde-seguridad/docs/La-accion-unificada-entre-civile-militares-arranca.pdf. Accessed: Apr. 19, 2025.
7. Calvillo, J. M. C. (2024). Metaverso y Seguridad Internacional. Riesgos y Potenciales Amenazas. *Barataria. Revista Castellano-Manchega de Ciencias Sociales*, (35):1–14. DOI: 10.20932/barataria.v0i35.683.
8. Copi, I. M. and Cohen, C. (2013). *Introduction to Logic*, volume 1. Pearson Education Inc., Mexico, 2nd edition. https://logicaformalunah.wordpress.com/wp-content/uploads/2017/01/irving_m-_copi_carl_cohen_introduccion_a_la_log.pdf. Accessed: Apr. 1, 2018.
9. Da Silva, M., Mocanu, S., Puys, M., and Thevenon, P. H. (2025). Safety-Security Convergence: Automation of IEC 62443-3-2. *Comput. Secur.*, 156. DOI: 10.1016/j.cose.2025.104477.
10. Departamento Nacional de Planeación (DNP) et al. (2020). *Conpes 3995*. Departamento Nacional de Planeación, Colombia. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf. Accessed: Apr. 22, 2025.
11. Department of Defense (DoD) (2012). *JP 3-13, Information Operations*. Department of Defense, EE. UU. https://informationsecurity.info/wp-content/uploads/2021/04/jp3_13.pdf. Accessed: Apr. 19, 2025.

12. Dumoulin, D. (2005). ¿Quién Construye la Aureola Verde del Indio Global? El Papel de los Distintos Actores Transnacionales y la Desconexión Mexicana. *Foro Internacional*, 45(1):35–64. http://www.jstor.org/stable/27738689. Accessed: Oct. 04, 2024.
13. Ejército Nacional de Colombia (EJC) (2019). *MCE 3-53.0*. Ejército Nacional de Colombia, Bogotá, Colombia. https://alianzaparalapaz.org/wp-content/uploads/CIMIC/B_MCE%203-53_Accion_Integral_y_Desarrollo.pdf. Accessed: Apr. 19, 2026.
14. Ejército Nacional de Colombia (EJC) (2017). *MFRE 3-0*. Ejército Nacional de Colombia, Colombia. https://www.ejercito.mil.co/enio/recurso_user/doc_contenido_pagina_web/800130633_4/458776/mfre_3_0_operaciones.pdf. Accessed: Apr. 19, 2025.
15. Ejército Nacional de Colombia (EJC) (2019). *MCE 3-53*. Ejército Nacional de Colombia, Bogotá, Colombia.
16. Ejército Nacional de Colombia (EJC) (2021). *MCE 3-24.0*. Ejército Nacional de Colombia, Colombia.
17. Floridi, L. (2014). *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford University Press, New York, NY, 1st edition. https://issc.al.uw.edu.pl/wp-content/uploads/sites/2/2022/05/Luciano-Floridi-The-Fourth-Revolution_-How-the-infosphere-is-reshaping-human-reality-Oxford-University-Press-2014.pdf. Accessed: Apr. 21, 2025.
18. García, J. C. P. and Hernández, A. W. C. (2024). FARC-EP Dissidents Groups: Continuation or New Criminal Groups? *Política y Sociedad*, 61(2):1–17. DOI: 10.5209/poso.87249.
19. García Peter, S. (2016). El Multiculturalismo como Modelo de Gobernanza en Chile: Estado, Academia y Brokers. *Universitas Humanística*, 82(82):307–334. DOI: 10.11144/javeriana.uh82.mmgc.
20. Guerra La Rotta, G. A. (2024). Maritime domain awareness and naval logistics. *Ensayos sobre Estrategia Marítima*, 8(19):23–46. DOI: 10.25062/2500-4735.4896.
21. Guerra La Rotta, G. A. and Rondón López, H. (2024). Historical Evolution of the Integral Action of the National Navy of Colombia. *Revista Rices*, 2(1). https://revistasrices.universu.com.co/rices/article/view/29/20. Accessed: Aug. 20, 2024.
22. Huertas Díaz, O. (2010). Global Society and Transnational Crimes. *Logos Ciencia & Tecnología*, pages 8–17. https://dialnet.unirioja.es/servlet/articulo?codigo=4163291. Accessed: Sep. 30, 2024.
23. Iftikhar, S. (2024). Cyberterrorism as a Global Threat: A Review on Repercussions and Countermeasures. *PeerJ Computer Science*. DOI: 10.7717/peerj-cs.1772.
24. International Maritime Organization (IMO) (2017). *Maritime Cyber Risk Management in Safety Management Systems*. International Maritime Organization, England. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf. Accessed: Apr. 19, 2025.
25. International Organization for Standardization (ISO) (2023). *Systems and Software Engineering – System Life Cycle Processes*. ISO/IEC/IEEE, Switzerland. https://cdn.standards.iteh.ai/samples/81702/5bd543dddf94457488c8cd8871897567/ISO-IEC-IEEE-15288-2023.pdf. Accessed: Apr. 19, 2025.
26. Jaakkola, E. (2020). Designing Conceptual Articles: Four Approaches. *AMS Review*, 10(1–2):18–26. DOI: 10.1007/s13162-020-00161-0.
27. Jamal, H., Algeelani, N. A., and Al-Sammarraie, N. A. (2024). Safeguarding Data Privacy: Strategies to Counteract Internal and External Hacking Threats. *Computer Science and Information Technologies*, 5(1):40–48. DOI: 10.11591/csit.v5i1.pp40-48.
28. Landaburo, L. S. (2016). Crimen Organizado y Economía Ilegal. *Revista Latinoamericana de Estudios de Seguridad*, (18):125–136. https://www.redalyc.org/journal/5526/552656690009/html/. Accessed: Sep. 30, 2024.
29. Maier, M. W. (1998). Architecting Principles for Systems-of-Systems. *Systems Engineering*, 1(4):267–284. DOI: 10.1002/(SICI)1520-6858(1998)1:4<267::AID-SYS3>3.0.CO;2-D.
30. Martínez Pinilla, I. L. (2024). Constitutionalizing Legal Transnational Actors: A Theoretical Legal Model to Counter the Wild Powers of Deregulated Globalization. *Revista Derecho del Estado*, (59):325–364. DOI: 10.18601/01229893.n59.11.
31. Mato, D. (2015). Redes Transnacionales de Actores Globales y Locales en la Producción de Representaciones de Ideas de Sociedad Civil. In *Políticas de Ciudadanía y Sociedad Civil en Tiempos de Globalización*, pages 67–93. https://www.globalcult.org.ve. Accessed: Oct. 04, 2024.
32. Mejía-Franco, N., Echeverri-Rubio, A., and Vieira-Salazar, J. A. (2021). Gobernanza Corporativa en Pequeñas y Medianas Empresas: Una Revisión Sistemática de Literatura. *Revista Venezolana de Gerencia (RVG)*, 26(93):245–263. https://www.redalyc.org/journal/290/29066223016/29066223016.pdf. Accessed: Apr. 22, 2025.
33. Moreno, A. C. C. (2024). Metaverso, Ciberespacio y Seguridad: Los Proyectos de China y Japón. *Barataria. Revista Castellano-Manchega de Ciencias Sociales*, (35):28–38. DOI: 10.20932/barataria.v0i35.684.

34. Muñoz, P. (2014). La Influencia de los Actores No Estatales en el Sistema Internacional. *AFESE: Revista de la Asociación de Funcionarios y Empleados del Servicio Exterior Ecuatoriano*, (58):100–112. https://afese.com/img/revistas/revista58/influencia.pdf. Accessed: Sep. 30, 2024.
35. National Intelligence Council (NIC) (2024). Non-State Actors Playing Greater Roles in Governance and International Affairs. Technical report, National Intelligence Council, Washington, DC. https://www.dni.gov/files/ODNI/documents/assessments/NICM-Non-State-Actors_23-01637_05-18-24_.pdf. Accessed: Jul. 22, 2024.
36. North, D. C. (1991). Institutions. *Journal of Economic Perspectives*, 5(1):97–112. https://www.jstor.org/stable/1942704. Accessed: Mar. 27, 2025.
37. OECD (2025). Subnational Governments Infrastructure Finance 2025. Technical report, OECD, Washington. https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/subnational-finance-and-investment/subnational-governments-infrastructure-finance-2025.pdf. Accessed: Dic. 29, 2025.
38. Piñero, R. and Rosenblatt, F. (2017). Tipos de Activistas en Organizaciones Partidarias. *Política y Gobierno*, XXIV(2):275–300. https://www.scielo.org.mx/pdf/pyg/v24n2/1665-2037-pyg-24-02-00275.pdf. Accessed: Oct. 04, 2024.
39. Potamos, G., Stavrou, E., and Stavrou, S. (2024). Enhancing Maritime Cybersecurity through Operational Technology Sensor Data Fusion: A Comprehensive Survey and Analysis. *Sensors*, 24(11). DOI: 10.3390/s24113458.
40. Re, M. (2018). The Process of Violent Radicalization Towards the Armed Struggle in Italy from the Far Left to Terrorist Militancy. *SCIO. Revista de Filosofía*, 14(14):195–221. https://revistas.ucv.es/scio/index.php/scio/article/view/491. Accessed: Oct. 04, 2024.
41. Reinares, F. (1997). Sociología Política de la Militancia en Organizaciones Terroristas. *Revista de Estudios Políticos (Nueva Época)*, (98):85–114. https://dialnet.unirioja.es/descarga/articulo/27477.pdf. Accessed: Oct. 04, 2024.
42. Restrepo, J. C. (2013). La Globalización en las Relaciones Internacionales: Actores Internacionales y Sistema Internacional Contemporáneo. *Revista Facultad de Derecho y Ciencias Políticas*, 43(119):625–654. http://www.scielo.org.co/scielo.php?script=sci_abstract&pid=S0120-38862013000200005. Accessed: Feb. 26, 2018.
43. Roumani, Y. and Alraee, M. (2025). Examining the Factors that Impact the Severity of Cyberattacks on Critical Infrastructures. *Comput. Secur.*, 148:104074. DOI: 10.1016/j.cose.2024.104074.
44. Saba, A. and Koehler, G. (2024). Contestation Movements and the Emergence of Eco-Social Contracts in India and Nepal Standard-Nutzungsbedingungen. Technical Report 2024-03, UNRISD, Bonn, Germany. https://www.unrisd.org. Accessed: Oct. 04, 2024.
45. Savolainen, J., Gill, T., Schatz, V., Ojala, L., Jakstas, T., and Kleemola-Juntunen, P. (2019). Hybrid CoE Handbook On Maritime Hybrid Threats: 10 Scenarios and Legal Scans. Technical report, Hybrid CoE, Helsinki. https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-5-handbook-on-maritime-hybrid-threats-10-scenarios-and-legal-scans/. Accessed: Oct. 15, 2024.
46. Schinas, M. and Gabriel, M. (2023). Hybrid Threats: A Comprehensive Resilience Ecosystem. Technical report, Luxembourg. DOI: 10.2760/867072.
47. Sterman, J. D. (2000). *Business Dynamics: Systems Thinking and Modeling for a Complex World*. McGraw Hill, Cambridge, MA, 1st edition. https://sa85c2e82e126a3ae.jimcontent.com/download/version/1360070105/module/6264585279/name/%E6%96%87%E5%AD%97BUSINESS_DYNAMICS.pdf. Accessed: Apr. 19, 2025.
48. Stouffer, K. et al. (2023). Guide to Operational Technology (OT) Security. Technical report, National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-82r3.
49. Tilly, C. (1993). *Coercion, Capital, and European States, AD 990-1992*. Wiley, Cambridge, 1st edition.
50. Trejos, L. F. R. (2016). Non-State Actors in the International Society: An Approach to Citizen Diplomacy in Colombia. *Investigación & Desarrollo*, 24(1):76–94. DOI: 10.14482/indes.24.1.8685.
51. Vintila, G. and Gherghina, S. C. (2012). An Empirical Examination of the Relationship between Corporate Governance Ratings and Listed Companies' Performance. *International Journal of Business and Management*, 7(22). DOI: 10.5539/ijbm.v7n22p46.
52. Wijninga, P., Oosterveld, W. T., Galdiga, J. H., and Marten, P. (2014). State and Non-State Actors: Strategic Monitor 2014. Technical report, La Haya, Países Bajos. https://www.jstor.org/stable/resrep12608.8. Accessed: Sep. 30, 2024.
53. Yañez, M. (2023). Subnational State-Owned Enterprises in Argentina: Organizational Hybridity and Aspects of Their Interjurisdictional Governance. *DAAPGE - Documentos y Aportes en Administración Pública y Gestión Estatal*, 24(41). https://bibliotecavirtual.unl.edu.ar/publicaciones/index.php/DocumentosyAportes/en/article/view/13396. Accessed: Apr. 19, 2025.
54. Zúñiga, L. (2016). El Concepto de Criminalidad Organizada Transnacional: Problemas y Propuestas. *Revista Nuevo Foro Penal*, 12(86):62–114. https://publicaciones.eafit.edu.co/index.php/nuevo-foro-penal/article/view/3646. Accessed: Sep. 30, 2024.

Authors' Biography

Gustavo Andrés Guerra La Rotta Academic in maritime logistics and strategy whose work examines how logistical capabilities shape naval power projection and maritime governance, with emphasis on causal links among resources, institutional coordination, and operational outcomes. A retired naval officer and doctoral student in Marine Sciences, he holds master's degrees in Logistics Management and in Geopolitics and Strategy from the War College, complemented by postgraduate studies in Maritime Policy and Strategy, Security, and Defense. His research agenda focuses on naval logistics theory, logistics under conflict and hybrid-threat conditions, as well as institutional design for state action across maritime and riverine spaces. His publications offer historical and doctrinal analyses of naval logistics, maritime domain awareness, hybrid warfare, plus institutional responses.

Disclaimer/Editor's Note: Statements, opinions, and data contained in all publications are solely those of the individual authors and contributors and not of the OnBoard Knowledge Journal and/or the editor(s), disclaiming any responsibility for any injury to persons or property resulting from any ideas, methods, instructions, or products referred to in the content.