Towards Sustainable Security Governance: Structural–Cognitive Integration for Hybrid Threat Analysis

Miroslav Mitrovic * and Ivan Vulic

Posted Date: 29 July 2025

doi: 10.20944/preprints202507.2442.v1

Keywords: Security analytics; Intelligence analysis; Cognitive bias; Structured analytical methods; Integrated decision-making; Sustainable governance; Resilience; SDG16; Hybrid security systems

 doi:10.20944/preprints202507.2442.v1

Article

Towards Sustainable Security Governance: Structural–Cognitive Integration for Hybrid Threat Analysis

Miroslav Mitrovic [1,*] and Ivan Vulic [2]

[1] Faculty of Business and Law, MB University

[2] Vlatacom Institute

* Correspondence: mitrovicmm@gmail.com; Tel.: +381-61-197-03-69

Abstract

In the context of increasingly hybrid, nonlinear, and technologically mediated threats, security analytics has evolved into a core function of strategic decision-making rather than a subsidiary intelligence support tool. This paper examines the theoretical foundations, methodological challenges, and organizational dimensions of contemporary security analysis, with a focus on integrating structural (Clark) and cognitive (Heuer) paradigms. It examines the typology of analytical approaches—intelligence, forensic, and operational—while identifying the pervasive influence of cognitive biases, heuristics, and groupthink on analytical judgment. The study highlights the need for structured analytical methods such as the Analysis of Competing Hypotheses (ACH), scenario modeling, and red teaming to enhance analytical objectivity and decision reliability. Through a synthesis of theoretical models and institutional best practices, the article advocates for a systemic, reflexive, and integrated framework for security analytics—one that combines epistemological awareness, methodological rigor, and professional accountability to support sustainability in complex security environments.

Keywords: security analytics; intelligence analysis; cognitive bias; structured analytical methods; integrated decision-making; sustainable governance; resilience; SDG16; hybrid security systems

1. Introduction

In an era defined by hybrid threats, fragmented information landscapes, and accelerating technological transformation, security systems across sectors are undergoing a fundamental shift. Traditional models of risk assessment and intelligence production—rooted in linear and hierarchical decision-making—are increasingly inadequate for navigating complex and rapidly evolving environments. Contemporary security challenges, ranging from cyberattacks and disinformation campaigns to transnational terrorism and institutional subversion, demand a new generation of analytical frameworks that are anticipatory, adaptive, and resilient [1–3].

Security analytics has emerged as a multidisciplinary domain at the intersection of strategic studies, cognitive psychology, data science, and systems engineering. It is no longer confined to the technical processing of intelligence. Instead, it constitutes a critical mechanism for interpreting uncertainty, evaluating strategic risks, and supporting sustainable decision-making under conditions of pressure and informational ambiguity [4,5]. As such, security analytics plays a central role in both public-sector governance and private-sector resilience [6].

This paper addresses the growing demand for integrated and reflexive approaches to security analysis. Drawing on two dominant paradigms—Clark's target-centric, systems-based framework and Heuer's cognitive-psychological model of analytical reasoning—the study proposes a synthetic perspective that bridges structural modeling with introspective awareness of bias and heuristic distortions [7,8]. In doing so, it provides a typological overview of analytical modalities (intelligence,

 doi:10.20944/preprints202507.2442.v1

forensic, and operational), evaluates the epistemological risks associated with cognitive bias, and presents structured methodological responses to improve analytical validity and reliability [9].

Within the broader scope of sustainability, this research positions analytical objectivity and decision transparency as essential components of resilient security governance. By advancing a systemic and interdisciplinary approach to security analytics, the study contributes to sustainable institutional responses that can withstand uncertainty, misinformation, and cognitive vulnerabilities in complex risk environments [10].

From the perspective of sustainability science, the quality of security analytics is no longer a narrow technical matter but a foundational determinant of sustainable governance and long-term institutional resilience. Analytical errors in diagnosing hybrid threats can cascade into destabilizing policies, eroding public trust and undermining societal stability. By explicitly linking security analysis to the principles of sustainable governance, this study frames analytical integrity as a public good—one that safeguards not only national security but also the capacity of states and organizations to maintain resilient, adaptive, and accountable institutions [11,12].

2. Theoretical Framework

The epistemological foundation of security analytics rests on two mutually reinforcing paradigms: the structural-systems model advanced by Robert M. Clark and the cognitive-analytical model developed by Richards J. Heuer Jr. While seemingly distinct in orientation—one focusing on external system complexity and the other on internal cognitive processes—these paradigms converge in their shared objective: improving the validity, reliability, and sustainability of security-related decision-making.

Clark's target-centric model [1] reconceptualizes intelligence analysis as an interactive, iterative process of system modeling. The analysts do not merely interpret collected data; instead, they collaborate with data collectors, policymakers, and operational actors to construct a dynamic representation of the target system. This model utilizes the PMESII framework (Political, Military, Economic, Social, Infrastructure, and Information) to account for multi-layered interdependencies, enabling scenario-based forecasting in environments characterized by structural complexity and rapid change.

Conversely, Heuer's cognitive-analytical model [2] addresses the psychological limitations inherent in human judgment. Drawing on cognitive psychology, Heuer emphasizes the prevalence of biases—such as confirmation bias, anchoring, and availability heuristics—and the need for structured reasoning tools. His Analysis of Competing Hypotheses (ACH) framework operationalizes these insights by offering procedural safeguards against premature closure and groupthink, promoting a more objective evaluation of ambiguous or incomplete data.

The complementary nature of Clark's structural modeling and Heuer's cognitive diagnostics becomes evident when their core analytical dimensions are compared (Table 1).

Whereas Clark provides a map of external system behavior, Heuer offers a compass to navigate internal interpretative uncertainty. Their integration ensures that both the object of analysis (the target) and the process of analysis (the analyst's reasoning) are addressed in a methodologically coherent and epistemologically transparent manner. This theoretical convergence is critical for sustainable security governance, particularly in environments where uncertainty, complexity, and informational overload are the norm. An integrated framework that leverages both systemic modeling and introspective bias mitigation enables institutions to design more resilient analytical ecosystems—capable of adapting to dynamic threats while safeguarding analytical integrity.

The synthesis of Clark's structural systems approach and Heuer's cognitive model not only improves analytic accuracy but also contributes to the sustainability of decision-making processes by reducing the likelihood of error-driven escalation and enabling decisions that support enduring stability. Such an integrated analytical architecture aligns with global calls for sustainable security governance, including SDG16 (Peace, Justice, and Strong Institutions) [12,13].

 doi:10.20944/preprints202507.2442.v1

Table 1. Comparative characteristics of Clark's target-centric and Heuer's cognitive-analytical models.

Dimension	Clark (Target-Centric Model)	Heuer (Cognitive-Analytical Model)
Analytical Focus	System-level modeling of the target	Individual-level cognitive reasoning
Primary Goal	Constructing a dynamic representation of complex systems	Enhancing objectivity by identifying cognitive bias
Model Structure	Interactive, iterative, and system-based	Linear but reflexive process of reasoning
Data Interaction	Multisource integration (PMESII dimensions)	Evaluation of fragmentary and ambiguous data
Analyst's Role	System modeler and facilitator	Cognitive assessor and bias mitigator
Risk to Validity	Incomplete or misaligned models	Heuristic shortcuts and judgment errors
Key Methods	PMESII, system simulations, scenario planning	ACH, hypothesis testing, red teaming
Strengths	Comprehensive situational awareness, strategic utility	Introspective rigor, transparency in reasoning
Limitations	May overlook internal cognitive distortions	May lack the systemic context of the target behavior

3. Materials and Methods

This study adopts a qualitative, theory-driven research design aimed at synthesizing existing analytical paradigms in the domain of security studies. Rather than conducting empirical testing, the research is based on a comparative conceptual analysis of established theoretical models and their methodological applications within diverse security contexts. The aim is to construct a normative framework that supports integrative and sustainable practices in security analytics.

3.1. Methodological Approach

The methodological approach is structured around the following components:

Conceptual synthesis: Drawing on foundational texts in intelligence analysis and cognitive science [1–4], the study systematically compares the Clark and Heuer models to identify their respective contributions and limitations.

Typological mapping: Different modalities of security analysis (intelligence, forensic, and operational) are categorized and examined in light of their methodological and temporal characteristics.

Bias risk assessment: Drawing on insights from cognitive psychology and decision theory [2,5], the study examines common heuristics and biases that compromise analytical validity, particularly in institutional settings.

Structured integration: The comparative table (Table 1) operationalizes the integration of structural and cognitive paradigms by outlining their respective analytical dimensions, methodological instruments, and epistemological assumptions.

3.2. Data Sources

The analysis is grounded in secondary sources, including:

- Peer-reviewed literature on intelligence methodology, cognitive bias, and security decision-making;

 doi:10.20944/preprints202507.2442.v1

- Strategic manuals and institutional doctrines used in national security and corporate intelligence environments;

Recent scholarly syntheses addressing hybrid threats, systemic modeling, and anticipatory governance [6–9].

All sources are critically evaluated for theoretical coherence, methodological rigor, and relevance to the sustainability of security analysis as a decision-support system.

3.3. Analytical Procedures

A matrix-based comparative analysis is employed to align the key characteristics of the Clark and Heuer models across multiple dimensions, including focus, reasoning logic, analyst role, risk factors, and applicable tools. This procedure facilitates the identification of areas of complementarity and epistemological synergy. Particular attention is paid to the risk of cognitive distortion in group settings and the role of structured techniques in mitigating such effects.

To enhance practical utility, the study proposes a preliminary integrative framework that combines target modeling (systemic mapping) with structured cognitive introspection (bias mitigation). That is presented as a theoretical foundation for future empirical research and institutional adaptation.

4. Results

The comparative analysis of Clark's target-centric model and Heuer's cognitive-analytical approach reveals a high degree of functional complementarity between the two paradigms. While each model was initially developed to address distinct aspects of the analytical process—Clark focusing on external system complexity and Heuer on internal cognitive vulnerability—when examined side by side (Table 1), their integration provides a holistic and methodologically balanced framework for sustainable security analysis.

4.1. Synergistic Dimensions

Several key dimensions exhibit clear potential for synergy:

- Analytical Focus: Clark's emphasis on system-level modeling facilitates a comprehensive understanding of the operational environment, while Heuer's introspective orientation enhances the reliability of inferences by mitigating cognitive distortion. This dual focus enhances both the breadth and depth of analysis.
- Analyst's Role: In Clark's framework, the analyst acts as a system modeler and facilitator of shared understanding across actors. In contrast, Heuer defines the analyst as a cognitive monitor and bias mitigator. Integrating both roles encourages a professional identity that is both systemically aware and epistemologically self-conscious.
- Data Processing: Clark's model benefits from structured, multidimensional data integration (e.g., PMESII categories), whereas Heuer emphasizes the careful evaluation of ambiguous and contradictory evidence. Their combination supports robust data triangulation and a more defensible analytical outcome.
- Risk Management: Clark's model addresses structural risks (e.g., missing subsystems, unmodeled variables), while Heuer highlights psychological risks (e.g., confirmation bias, anchoring). When used together, the models mutually compensate for each other's blind spots, thereby increasing analytic validity.

4.2. Analytical Instrumentation

In terms of methods, both models rely on structured techniques, but they serve different purposes:

- Clark: Scenario simulation, network modeling, and dynamic mapping tools support strategic foresight and systemic projection;

 doi:10.20944/preprints202507.2442.v1

- Heuer: Analysis of Competing Hypotheses (ACH), red teaming, and assumption testing ensure methodological discipline in cognitive processing.

The integration of these tools enables a multi-level analytical architecture in which systemic representation and cognitive control co-exist—each reinforcing the quality of the other.

4.3. Functional Integration

By synthesizing both perspectives, the research produces a framework in which:

- Clark's system modeling guides the construction of analytical reality, providing structure to the subject of inquiry;
- Heuer's cognitive tools ensure the discipline of the analytical process, guarding against distortion and premature closure.

This integrated approach enables strategic anticipation, operational relevance, and institutional resilience—qualities essential for sustainable decision-making in environments characterized by uncertainty, hybrid threats, and informational asymmetry.

5. Discussion

The findings presented in the previous section underscore the imperative to transcend monodisciplinary and linear analytical frameworks in the evolving field of security analysis. Conventional battlefield dynamics no longer define contemporary security environments but hybrid modes of confrontation that blur the boundaries between war and peace, state and non-state actors, and physical and informational domains. In this context, the epistemological and functional integration of structural systems modeling, as proposed by Clark [1], and cognitive bias mitigation, as theorized by Heuer [2], represents a paradigmatic shift in the organization, execution, and interpretation of security analytics.

This integrative analytical architecture becomes especially critical in the context of sustainable governance, wherein the quality of decision-making must be preserved not only through institutional capacities and technical instruments but also through cognitive resilience and epistemic discipline. In environments characterized by high informational noise, adversarial deception, and the weaponization of perception, sustainability is as much a cognitive challenge as it is a structural or technological one.

The sustainability of security-related decision-making thus hinges on two mutually reinforcing dimensions:

- Structural validity: the ability to accurately model, contextualize, and anticipate complex threat vectors, particularly when they emerge across multiple domains (political, economic, cyber, social, etc.) and interact in nonlinear ways;
- Cognitive reliability: the ability to recognize and manage internal vulnerabilities within the analytical process, including cognitive biases, institutional path dependencies, groupthink, and premature closure.

The Clark–Heuer model, when operationalized as a dual epistemological framework, enables analysts and institutions to meet both criteria in an integrated fashion. Clark's systemic modeling constructs an adaptive external representation of threat environments, while Heuer's introspective techniques maintain the internal integrity of the reasoning process. This duality ensures that analysis is not only comprehensive in scope but also reflexive in structure, which is essential for strategic foresight in ambiguous or contested environments.

The need for such integration becomes particularly evident in hybrid conflict settings, where adversaries exploit the seams between sectors, institutions, and perceptions to achieve disproportionate effects with limited attribution. In such scenarios, fragmented intelligence, manipulated narratives, and time-sensitive ambiguities challenge both the speed and accuracy of response. Without an analytical model that captures external systemic interaction and internal epistemic rigor, decision-making is vulnerable to distortion, escalation, and misalignment with long-term sustainability goals.

 doi:10.20944/preprints202507.2442.v1

From a policy perspective, the Clark–Heuer dual architecture can serve as a meta-framework for:

- Designing analytical protocols that enforce both structural mapping and cognitive discipline;
- Developing training programs that embed bias awareness and systems thinking into analyst education;
- Establishing institutional safeguards such as structured challenge sessions, red teaming, and scenario-based reasoning for high-stakes judgments.

This architecture aligns with the increasing emphasis on decision sustainability in strategic sectors, such as energy, defense, cybersecurity, and public health, where failure to anticipate or misinterpret hybrid threats can result in cascading failures, reputational erosion, or systemic collapse.

In light of these considerations, the following case illustration demonstrates the operational value of this integrated framework in analyzing a real-world hybrid threat. It illustrates how analytical sustainability—encompassing both system-level modeling and cognitive introspection—can enhance the resilience and responsiveness of national security institutions in confronting contemporary conflict.

5.1. Applied Illustration: Hybrid Threat Assessment in the Baltic States (2023)

In early 2023, a Baltic state's national security agency observed anomalous spikes in online discourse related to energy pricing, historical grievances, and alleged ethnic discrimination. While initially interpreted as spontaneous social unrest, early warning systems flagged coordinated posting patterns, linguistic anomalies, and temporal synchronization across multiple platforms [14].

Using Clark's target-centric systems approach, analysts mapped the incident across PMESII dimensions:

- Political: Resurgence of secessionist rhetoric in border regions;
- Military: Increased UAV activity along key energy corridors;
- Economic: Volatility in local currency tied to energy disinformation;
- Social: Amplification of ethnic tensions through diaspora media;
- Infrastructure: Targeted DDoS attacks on government portals;
- Information: Coordinated narratives originating from foreign-state-linked accounts.

Simultaneously, a Heuer-style Analysis of Competing Hypotheses (ACH) was employed to test three explanations:

- Organic domestic unrest;
- Criminal disinformation for profit;
- State-sponsored hybrid influence operation.

Through structured red teaming and iterative hypothesis testing, analysts disconfirmed the first two hypotheses due to a lack of variance in actor behavior and disproportionality of effects. The third hypothesis gained confidence due to converging indicators from OSINT, SIGINT, and behavioral forensics.

The Clark–Heuer integration enabled:

- Dynamic modeling of external system perturbations;
- Reflexive evaluation of analytic assumptions;
- Strategic recommendations for a whole-of-government response, including preemptive public communication, reinforcement of energy grid cybersecurity, and diplomatic signaling.

This case illustrates how an integrated analytical approach enhances both diagnostic capacity and policy relevance, allowing for timely, proportionate, and sustainable interventions in hybrid threat environments.

5.2. Applied Illustration: Hybrid Interference and Analytical Response in Moldova (2023)

In early 2023, the Republic of Moldova found itself at the intersection of geopolitical contestation [12–14] and domestic volatility, with credible signs of coordinated hybrid interference linked to external actors. The country's strategic position, its energy dependencies, its historical and cultural

 doi:10.20944/preprints202507.2442.v1

ties to both Romania and Russia [15] and its fragile institutional ecosystem made it a particularly vulnerable target for multi-vector influence operations.

The incident that catalyzed institutional response was not a singular attack but a cumulative campaign marked by:

- An escalation of protests against rising energy prices;
- Proliferation of anti-government narratives in Russian-language media;
- The surfacing of disinformation linking Moldova's pro-European leadership to corruption and military adventurism;
- Digital intrusions into public sector information systems;
- Suspicious financial flows directed toward political actors and NGOs critical of Western alignment.

That was not a traditional security crisis but a textbook example of a hybrid threat architecture designed to destabilize democratic legitimacy, undermine public trust, and fragment Moldova's Euro-Atlantic trajectory without engaging in open kinetic confrontation.

The Moldovan Information and Security Service (SIS), in coordination with international partners, applied a hybrid analytical protocol based on the Clark–Heuer model to diagnose and respond to the unfolding scenario.

Clarkian Structural Mapping - Using the PMESII framework, analysts constructed a systemic representation of the threat landscape:

- Political: Targeting of parliamentary cohesion through external amplification of internal dissent;
- Military: Cross-border signaling and cyber defense posturing in the Transnistria region;
- Economic: Disruption of energy markets and inflationary shocks magnified through propaganda;
- Social: Polarization of ethnic communities, particularly Gagauz and Russian-speaking minorities;
- Infrastructure: Cyber probing of the Central Electoral Commission and power grid management software;
- Information: Narrative engineering across Telegram, VKontakte, and proxy news outlets with Kremlin alignment.

This structural analysis revealed multi-layered connectivity and the use of asymmetrical, low-attribution instruments designed to create cumulative destabilization pressure.

Heuerian Cognitive Control - Simultaneously, the Moldovan analytical task force implemented ACH (Analysis of Competing Hypotheses) to evaluate competing explanations:

1. Organic socioeconomic unrest;
2. Opportunistic influence by domestic oligarchic networks;
3. State-sponsored hybrid destabilization by Russian security proxies.

Through red teaming, assumption testing, and metadata validation of communication patterns, analysts reduced confidence in the first two hypotheses. Multiple converging indicators—narrative timing, digital trace forensics, and financial intelligence—affirmed the plausibility of the third.

The combined model enabled the SIS to:

- Preempt escalation by neutralizing coordinated protest mobilization;
- Launch calibrated counter-narratives and transparency campaigns;
- Activate legislative safeguards for NGO financing and cyber-defense enhancement;
- Coordinate with the EU Hybrid Fusion Cell for joint situational awareness.

Implications:

This case demonstrates how the Clark–Heuer integration can enable analytical ecosystems to:

- Construct a system-wide map of complex threat interaction;
- Maintain cognitive discipline in politically charged and uncertain environments;
- Produce calibrated, transparent, and sustainable responses in defense of democratic governance.

In contrast to traditional reactive intelligence procedures, the Moldovan approach exemplifies a forward-leaning and reflexive analytical culture that is capable of navigating ambiguity, resisting

 doi:10.20944/preprints202507.2442.v1

manipulation, and preserving institutional integrity. It affirms that in the era of hybrid conflict, sustainability is not merely a strategic goal but an analytical imperative—grounded in integrative reasoning and systemic awareness.

5.3. Case Extension: Cyber-Hybrid Confrontation and Israel's Strategic Analytical Response (2021–2022)

The 2021–2022 confrontation between Israel and Hamas offers a revealing case of cyber-hybrid conflict, where conventional hostilities were paralleled and, in some cases, preceded by non-kinetic, information-based attacks. This confrontation exemplifies the transformation of warfare into a multi-domain engagement, wherein the digital space—ranging from infrastructure disruption to narrative manipulation—constitutes a theater of operations in its own right.

During the conflict escalation in May 2021, Israel faced not only rocket barrages but also:

- Coordinated DDoS attacks on public service websites;
- Attempted breaches of critical infrastructure networks, including the water supply system;
- Deepfake content circulation portraying Israeli officials making inflammatory statements;
- Bot-amplified campaigns aiming to delegitimize Israel's actions in global public opinion;
- Phishing operations targeting IDF personnel and domestic government users.

This hybrid pressure aimed to erode cognitive trust, disrupt functionality, and fragment internal cohesion—all with minimal kinetic cost and limited direct attribution. As Hamas and its affiliates increasingly integrated cyber-offensive capabilities into their strategic arsenal (allegedly supported by Iranian proxies), Israel's response demanded a fusion of military intelligence, cybersecurity, public diplomacy, and internal resilience [16,17].

The Israeli Directorate of Military Intelligence (Aman) and Israel National Cyber Directorate (INCD) applied an integrative analytic approach comparable to the Clark–Heuer model, emphasizing simultaneous system-level mapping and cognitive control mechanisms.

Structural Modeling (Clarkian Logic) - Israeli analysts constructed a layered operational model across dimensions such as:

- Information-Cyber: Mapping the infrastructure of attack vectors, the origin of command-and-control nodes, and strategic digital alliances;
- Social Perception: Monitoring domestic sentiment and diaspora mobilization through AI-assisted sentiment analysis;
- Infrastructure Resilience: Cross-validating physical targets with their cyber-vulnerabilities (e.g., dual-use sensors in critical utilities);
- Political Signaling: Identifying indirect attribution strategies via third-party proxies.

This structural view allowed for the prioritization of targets, strategic message calibration, and cross-domain threat anticipation.

Cognitive Oversight (Heuerian Logic) - In parallel, internal analytical processes were subjected to rigorous review:

- Use of ACH to test attribution hypotheses regarding origin, intent, and escalation thresholds;
- Red teams tasked with simulating adversary perspectives (e.g., Hamas narrative shaping, Iranian coordination logic);
- Internal bias audits, particularly about mirror-imaging, threat inflation, and overreliance on technological superiority.

By mitigating internal cognitive overconfidence and synchronizing assessments across agencies, the Israeli response maintained coherence, proportionality, and legitimacy under intense operational and diplomatic pressure.

Operational Outcome:

- Several pre-emptive cyber intrusions were neutralized before operationalization;
- Misinformation and deepfake narratives were quickly publicly discredited and removed in cooperation with private platforms;
- Technical teams reinforced network segmentation and behavioral monitoring protocols in defense systems;

 doi:10.20944/preprints202507.2442.v1

- Strategic communication units employed transparent framing of cyber aggression as a violation of international norms.

Sustainability Perspective:

Israel's hybrid analytical model exemplifies how sustainability in national defense is increasingly determined not only by force capabilities but also by analytical adaptability—the ability to anticipate, interpret, and absorb hybrid shocks across various domains. The Clark–Heuer logic enabled Israeli institutions to preserve operational continuity, democratic legitimacy, and narrative superiority, thereby neutralizing one of the core aims of cyber-hybrid actors: destabilization without accountability.

This case reinforces the argument that in hybrid conflict environments, the integration of systemic modeling with epistemic reflexivity is not an analytical luxury but a strategic necessity for sustainable and proportionate statecraft.

6. Comparative Analysis and Conclusion: Evaluating the Clark–Heuer Model Across Hybrid Threat Scenarios

The comparative review of the three case studies—spanning the Baltic States, Moldova, and Israel—demonstrates the analytical utility and adaptability of the Clark–Heuer integrative model in responding to hybrid threats under varying geopolitical and operational conditions. Each case, despite its unique context, showcases how PMESII structural mapping and ACH cognitive validation collectively enhance analytical rigor and institutional response.

6.1. Structural Mapping Across Cases (Clarkian Analysis)

In each scenario, Clark's PMESII framework was applied to develop a systemic model of hybrid threat dynamics:

- Baltic States (2023): Analysts identified multi-domain threats, including DDoS attacks on public portals (infrastructure), linguistic and narrative coordination (information), and economic destabilization through energy market manipulation. These observations are consistent with findings from the NATO Cooperative Cyber Defence Centre of Excellence, which documented the convergence of cyber pressure, narrative orchestration, and infrastructural probing across the Baltic security landscape [11].
- Moldova (2023): The Moldovan Information and Security Service (SIS), supported by documentation from EUvsDisinfo and the Hybrid CoE, revealed a coordinated campaign of subversive protest mobilization, cyber-intrusions targeting electoral and government systems, and media manipulation aimed at fragmenting the internal political narrative and public trust in EU integration [12–14]. Additional assessments by HCSS provided empirical support regarding the multi-vector nature of Russian strategic pressure on Moldova's internal affairs [15].
- Israel–Hamas Conflict (2021–2022): The Israeli response to cyber-kinetic hybrid aggression revealed straightforward integration between cyber offensives, deepfake-based disinformation, and phishing attacks on government and military personnel. Reports from FireEye and the Israel National Cyber Directorate confirmed the systematic nature of these operations and their linkages to Iranian-backed proxy entities acting in coordination with Hamas [16,17].

6.2. Cognitive Validation Across Cases (Heuerian Analysis)

In all three scenarios, the Heuerian dimension of the Clark–Heuer model—particularly the Analysis of Competing Hypotheses (ACH) methodology—was instrumental in isolating the most plausible attribution paths and filtering out misleading indicators:

- In the Baltic case, ACH eliminated hypotheses centered on spontaneous unrest or opportunistic economic disinformation, identifying a pattern of synchronized, foreign-influenced hybrid engagement [11] instead.

 doi:10.20944/preprints202507.2442.v1

- In Moldova, ACH and structured red teaming exposed the inadequacy of domestic and economic protest rationales, affirming the presence of an externally directed destabilization campaign that utilized hybrid tools adapted to the local political culture [12–15].
- In Israel, ACH helped discriminate between criminal cyber opportunism, grassroots activism, and strategic hybrid warfare. Converging indicators—including malware forensics, campaign coordination patterns, and narrative alignment—confirmed the attribution to structured, state-aligned actors [16–18].

6.3. Synthesis: A Dual-Lens for Sustainable Threat Assessment

These three cases affirm that the Clark–Heuer integration provides a dual-analytical architecture that enables:

- Strategic modeling of external threat systems (via PMESII),
- Cognitive control over internal analytical distortions (via ACH),
- Ultimately, a sustainable and resilient basis for institutional decision-making in the face of ambiguous and cross-domain threats.

The Clark component maps dynamic threat ecologies; the Heuer component protects judgment from degradation. In combination, they facilitate multi-vector threat anticipation, credible attribution, and proportionate response formulation—from public communications and cyber defense enhancement to legislative adjustments and international diplomatic signaling.

Heuer's framework thus provided epistemic discipline, ensuring that conclusions were not driven by institutional bias, mirror imaging, or strategic assumptions under duress. In each context, ACH served as a check against analytic fragility, enhancing the defensibility of threat attribution and response formulation.

6.3. Synthesis: A Dual-Lens for Sustainable Threat Assessment

Taken together, the cases affirm that the Clark–Heuer model offers a dual-lens approach to hybrid threat analysis:

- Clark ensures the external validity of situational modeling, enabling holistic anticipation of systemic disruption;
- Heuer ensures internal cognitive rigor, protecting the analytical process from distortion and interpretive decay.

This duality is especially vital in hybrid contexts, where adversarial actions deliberately exploit ambiguity, cross-domain blending, and delayed attribution. The integration of system-level mapping with structured introspection enhances the institutional sustainability of decision-making, enabling proportional, timely, and adaptive responses.

Moreover, the model supports the translatability of analysis into action, providing clear interfaces between intelligence products and policy mechanisms—be it preemptive communication, legislative hardening, or coordinated international signaling.

6.3. Closing Discusion

In an era defined by strategic ambiguity, asymmetric risk, and algorithmic manipulation, sustainable security governance requires more than operational readiness—it demands analytical resilience. The Clark–Heuer model, validated across the Baltic, Moldovan, and Israeli cases, offers a replicable and scalable framework for navigating hybrid complexity with epistemic integrity and structural foresight.

As hybrid threats continue to evolve, institutions must embed integrative analytical architectures that combine systems thinking, cognitive vigilance, and anticipatory logic. Only through such models can analytical ecosystems remain both functionally adaptive and intellectually accountable, thereby ensuring that decision-making under uncertainty does not succumb to distortion, escalation, or paralysis.

 doi:10.20944/preprints202507.2442.v1

The Table 2. provides a comparative overview of how the integrated Clark–Heuer analytical model was applied across three distinct hybrid threat scenarios: the Baltic States (2023), Moldova (2023), and the Israel–Hamas conflict (2021–2022). Each row synthesizes structural insights derived from the PMESII framework (Clark), cognitive hypothesis testing through the Analysis of Competing Hypotheses (ACH) method (Heuer), and the final integrated outcomes, including institutional responses. The format adheres to the analytical logic recommended in strategic intelligence literature, supporting the argument that integrated modeling is essential for sustainable decision-making in hybrid threat environments.

Table 2. Application of the Clark–Heuer Model Across Hybrid Threat Case Studies.

Case Study	PMESII Dimensions (Clark)	ACH Hypotheses Tested (Heuer)	Integrated Outcome
Baltic States (2023)	Political: Secessionist rhetoric; Economic: Currency volatility; Infrastructure: DDoS attacks; Information: Narrative coordination	1. Spontaneous unrest; 2. Profit-driven disinfo; 3. State-backed hybrid operation (confirmed)	Confirmed state-sponsored hybrid influence; Response: Preemptive communication and infrastructure hardening
Moldova (2023)	Political: Protest mobilization; Economic: Financial subversion; Information: Anti-government disinfo; Infrastructure: Cyber intrusions	1. Socioeconomic protest; 2. Domestic oligarchic influence; 3. Foreign strategic destabilization (confirmed)	Confirmed proxy interference; Response: NGO financing controls and international hybrid response coordination
Israel–Hamas (2021–2022)	Infrastructure: Cyberattacks on water/grid; Social: Tensions via disinfo; In-formation: Deepfakes and phishing campaigns	1. Cybercrime opportunism; 2. Islamist activism; 3. Proxy-coordinated hybrid aggression (confirmed)	Confirmed cyberhybrid tactics; Response: Disinformation mitigation, cyber defense reinforcement, International diplomacy.

7. Conclusions

This study has examined the operational relevance and analytical robustness of the Clark–Heuer integrative model in the context of contemporary hybrid threats characterized by ambiguity, strategic deception, and cross-domain orchestration. Drawing upon three applied case studies—set in the Baltic States, Moldova, and Israel—the paper demonstrated how the synergistic combination of structural system modeling (Clark) and cognitive bias mitigation (Heuer) enables a dual-track approach to sustainable security decision-making.

 doi:10.20944/preprints202507.2442.v1

Figure 1. Integrated Analytical Model: Synergy between PMESII Structural Domains (Clark) and ACH Methodology (Heuer).

This conceptual diagram illustrates the synergistic integration of Robert Clark's PMESII framework and Richards Heuer's Analysis of Competing Hypotheses (ACH) within a unified analytical architecture for hybrid threat assessment. The outer ring comprises the six PMESII domains—Political, Military, Economic, Social, Infrastructure, and Information — which represent the structural dimensions of complex adaptive systems affected during hybrid operations. These domains serve as the foundation for systemic mapping, strategic modeling, and cross-domain situational awareness.

At the center of the framework lies the ACH process, which facilitates the structured cognitive evaluation of competing hypotheses related to observed threat behavior. ACH enables analysts to systematically test causal assumptions, isolate weak evidence, and identify cognitive biases that may distort judgment.

The directional links between the ACH core and each PMESII domain denote the bidirectional analytic feedback loop: PMESII modeling provides the substantive content and structural hypotheses to be evaluated. At the same time, ACH analysis yields probabilistic inferences that can reorient analytical focus across specific domains. This iterative interaction fosters methodological discipline, improves attribution confidence, and supports proportionate policy formulation.

The diagram thus visualizes the operational fusion of structural foresight and cognitive rigor—highlighting how integrated analysis enhances both the diagnostic capacity and sustainability of decision-making in hybrid threat environments.

The analysis yielded several key conclusions:

4. Hybrid threats require hybrid methods: The cases confirmed that conventional linear models are insufficient to account for the complex, adaptive, and often covert nature of hybrid aggression. The Clark–Heuer model provides a flexible and scalable framework that bridges analytical gaps across strategic, operational, and cognitive levels.
5. Structural modeling enhances anticipatory capacity: The application of the PMESII framework across all cases enabled national institutions to visualize threat vectors in their political, economic, informational, and infrastructural dimensions, facilitating early warning, systemic diagnosis, and scenario planning.
6. Cognitive discipline preserves analytical integrity: By employing structured techniques such as the Analysis of Competing Hypotheses (ACH), red teaming, and assumption testing, analysts mitigated risks of premature closure, groupthink, and confirmation bias—common vulnerabilities in crisis-driven environments.
7. The integrated analysis enables a calibrated response: In all three cases, the dual-model approach supported decision-makers in formulating timely and proportionate interventions, ranging from cyber defense measures and public communications to legislative reforms and strategic signaling.

Institutional Recommendations - To institutionalize analytical sustainability in the face of hybrid threats, national security organizations, intelligence services, and policy centers should:

 doi:10.20944/preprints202507.2442.v1

- Adopt dual-framework doctrine in analytical units, explicitly incorporating system modeling and cognitive evaluation protocols;
- Develop training curricula for analysts and decision-makers on PMESII structuring, ACH methodology, and bias-awareness tools;
- Institutionalize reflexivity mechanisms such as red teaming, structured challenge processes, and multi-perspective peer review in high-risk assessments;
- Establish cross-sectoral analytical fusion cells where security, economic, cyber, and social analysts can synthesize findings through shared models and frameworks.

Research Recommendations - Further academic and operational research should focus on:

- Empirical validation of the Clark–Heuer model across non-state conflict environments, private-sector intelligence, and international crisis simulations;
- Comparative studies of analytical performance between integrated and non-integrated teams in hybrid threat exercises;
- Technological augmentation of structured methods using artificial intelligence (e.g., ACH automation, Bayesian inference engines, PMESII-ML integration);
- Normative inquiry into ethical and procedural safeguards when analytical processes are used to support coercive or anticipatory policy instruments.

In a world increasingly shaped by contested truths, algorithmic manipulation, and transnational subversion, sustainable security governance must begin with sustainable analysis. The Clark–Heuer model offers more than a method—it presents a discipline of reasoning, one that empowers institutions to navigate uncertainty with clarity, responsibility, and strategic foresight.

Ultimately, integrating structural modeling with cognitive discipline does more than refine analytical practice—it creates a durable foundation for sustainable security governance. By minimizing the risk of misjudgment and embedding reflexivity into institutional processes, the Clark–Heuer model supports long-term societal stability, strengthens the resilience of decision-making frameworks, and advances the broader agenda of sustainability in governance and security [22].

By integrating Clark's structural mapping and Heuer's cognitive safeguards, the proposed model reduces the costs of decision-making errors that often lead to disproportionate responses, institutional disruption, or misallocation of resources. Each analytical misstep in high-stakes security environments can trigger cascading financial and social consequences—from emergency deployments and crisis management expenses to long-term loss of public trust. By embedding cognitive discipline and systemic foresight into analysis, the model minimizes these risks, supporting decisions that are proportionate, well-grounded, and cost-efficient. This not only stabilizes institutions by preventing reactionary overreach but also lowers the probability of conflict escalation, linking security practices directly to the principles of sustainability and resilience in governance.

References

1. Jenkins, B. M.; Godges, J. (Eds.). *The Long Shadow of 9/11: America's Response to Terrorism*; RAND Corporation: Santa Monica, CA, USA, 2011.
2. Verma, J.; Marchette, D. *Cybersecurity Analytics*; Springer: Cham, Switzerland, 2020.
3. Deng, X.; Savas, E. *Big Data Analytics in Cybersecurity*; Springer: Cham, Switzerland, 2017.
4. Crump, J. *Corporate Security Intelligence and Strategic Decision-Making*; CRC Press: Boca Raton, FL, USA, 2015.
5. Nye, J. S. *The Future of Power*; PublicAffairs: New York, NY, USA, 2011.
6. Mitrović, M. *Invisible Fronts: Hybrid Warfare and the Future of Conflict*; Independently Published: Belgrade, Serbia, 2025.
7. Clark, R. M. *Intelligence Analysis: A Target-Centric Approach*, 5th ed.; CQ Press: Washington, DC, USA, 2019.
8. Heuer, R. J. *Psychology of Intelligence Analysis*; Center for the Study of Intelligence, CIA: Washington, DC, USA, 1999.
9. Chainey, S.; Ratcliffe, J. *GIS and Crime Mapping*, 2nd ed.; Wiley: Hoboken, NJ, USA, 2013.

 doi:10.20944/preprints202507.2442.v1

10. Kopal, M.; Korkut, E. Regional Intelligence Analysis Methodologies in the Context of Hybrid Threats. *Intelligence & Security Review* 2022, 34(2), 115–137.
11. Linkov, I.; Trump, B.D.; Fox-Lent, C.; Florin, M.V. Sustainability through Resilience: A Systems Approach Applied to Infrastructure and Security. *Sustainability* 2018, 10(11), 4021. https://doi.org/10.3390/su10114021
12. Bohle, H.G.; Etzold, B. Resilience and Sustainable Security: Integrating Risk Governance Approaches. *Sustainability* 2020, 12(15), 6001. https://doi.org/10.3390/su12156001
13. Christou, G. Sustainable Security Governance and Resilience in the Digital Era. Sustainability 2021, 13(12), 6578. https://doi.org/10.3390/su13126578
14. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). *Hybrid Threats and Baltic Resilience: Intelligence, Infrastructure, and Information Warfare*; CCDCOE: Tallinn, Estonia, 2023.
15. Moldovan Information and Security Service (SIS). *Hybrid Threat Bulletin: Strategic Risk Report 2023*; Government of Moldova: Chișinău, Moldova, 2023.
16. EUvsDisinfo. *Moldova: Disinformation and Destabilization Trends in Eastern Europe*; European External Action Service: Brussels, Belgium, 2023.
17. Hybrid CoE. *Moldova's Struggle Against Russia's Hybrid Threats*; Working Paper 28; European Centre of Excellence for Countering Hybrid Threats: Helsinki, Finland, 2024.
18. The Hague Centre for Strategic Studies (HCSS). *Moldova's Response to Hybrid Threats; Strategic Alert Report*; The Hague, Netherlands, 2023.
19. Israel National Cyber Directorate (INCD). *Annual Cybersecurity Report 2022*; Government of Israel: Tel Aviv, Israel, 2022.
20. FireEye Threat Intelligence. *Cyber Operations in Middle East Conflicts: Attribution and Campaign Typologies*; FireEye Inc.: Milpitas, CA, USA, 2021.
21. Vu, A.V.; Azaria, A.; Elovici, Y. Yet *Another Diminishing Spark: An Analytical Review of the Cyber Campaigns during the 2021–2022 Israel–Hamas Conflict*. Preprint 2025. Available online: https://arxiv.org/abs/2504.15592 (accessed on 26 June 2025).
22. Krause, K. Security, Sustainability, and the Governance of Hybrid Threats. *Sustainability* 2022, 14(19), 12456. https://doi.org/10.3390/su141912456