Countering Illegal Foreign Interference and Disinformation as Hybrid Threats in the Republic of Albania 2025–2030

Contents

List of Table

Executive Summary

Hybrid threats represent one of the most complex and destabilizing challenges facing democratic states. They combine cyber operations, disinformation campaigns, economic coercion, legal manipulation, and influence operations—often conducted below the threshold of armed conflict.

Recognizing this evolving threat landscape, the Republic of Albania has formally identified **Hybrid Threats** as **one of the five strategic pillars of the National Cyber Security Strategy 2025–2030**, with **illegal foreign interference and disinformation** as core risk vectors.

This Strategic Plan sets out a **whole-of-government, whole-of-society framework** led by AKSK to:

- prevent, detect, attribute, and respond to foreign hybrid operations.
- protect democratic institutions, public trust, and national security.
- strengthen legal, institutional, and operational resilience.
- align Albania with EU, NATO, and transatlantic best practices.

Strategic Context and Threat Environment

The Evolution of Hybrid Threats

Hybrid threats are characterized by:

- ambiguity of actors and intent,
- deniability and proxy execution,
- synchronization of cyber, informational, political, and economic tools.

Foreign state and non-state actors increasingly exploit:

- digital platforms,
- social media algorithms,
- cyber vulnerabilities,
- legal and institutional asymmetries.

Illegal Foreign Interference

Illegal foreign interference includes:

- covert influence on elections and public opinion,
- manipulation of political discourse,
- financing or coordination of influence networks,
- cyber-enabled operations targeting institutions and critical information flows.

These activities directly threaten:

- constitutional order,
- sovereignty,
- democratic legitimacy.

Disinformation as a Strategic Weapon

Disinformation is no longer incidental—it is **strategic**:

- persistent,
- data-driven,
- psychologically targeted,
- often combined with cyber intrusions or leaks.

National Strategic Anchoring

Hybrid Threats as a Pillar of the Cyber Security Strategy 2025–2030

The National Cyber Security Strategy 2025–2030 defines **five core pillars**, one of which is:

"Countering Hybrid Threats, including disinformation, foreign interference, and cyber-enabled influence operations."

AKSK is designated as:

- **national coordinator for cyber-enabled hybrid threats**, and
- **technical authority for detection, analysis, and response**.

Albania's International Positioning

In **June 2024**, Albania signed the agreement to become the **36th member of the European Centre of Excellence for Countering Hybrid Threats**.

This membership:

- anchors Albania within the European hybrid threat community,
- enables access to strategic analysis, training, and exercises,
- strengthens interoperability with EU and NATO partners.

Legal and Institutional Foundations

National Legal Framework

This Plan is grounded in:

- the Constitution of the Republic of Albania,
- national security and cybersecurity legislation,
- laws on data protection, media, and electronic communications,
- national crisis management and civil protection frameworks.

Parliamentary Disinformation Commission (2024)

In **2024**, Albania established a **Parliamentary Commission on Disinformation**, marking a critical step in democratic oversight and strategic awareness.

The Commission

- investigates systemic disinformation risks,
- examines foreign influence vectors,
- proposes legislative and policy measures,
- strengthens accountability and transparency.

AKSK provides

- technical expertise,
- cyber intelligence inputs,
- risk assessments and incident analyses.

Institutional Mandates and Coordination

Table 1: Institutions and Role

Institution	Core Role
AKSK	National coordinator for cyber & hybrid threats
AKSHI	National support for cyber & hybrid threats
Council of Ministers	Strategic direction & crisis decisions
Intelligence Services	Strategic intelligence & attribution
Law Enforcement	Criminal investigation
Media & Regulatory Authorities	Platform oversight & standards
Parliament	Oversight, legislation, democratic control

Strategic Vision and Objectives

Vision

A resilient Albanian state and society capable of resisting, absorbing, and recovering from hybrid threats without democratic erosion or institutional destabilization.

Strategic Objectives

1. Detect and disrupt illegal foreign interference early
2. Reduce the impact of disinformation campaigns
3. Strengthen institutional coordination
4. Protect elections and democratic processes
5. Enhance public trust and societal resilience
6. Align Albania with EU and NATO hybrid defense standards

Threat Typology and Risk Assessment

Primary Threat Actors

- hostile foreign state actors,
- proxy organizations and fronts,
- coordinated online networks,
- cyber-criminal groups aligned with geopolitical interests.

High-Risk Scenarios

- election periods,
- major geopolitical crises,
- cyber incidents affecting public services,
- social polarization events.

Operational Pillars of the Plan

Pillar I – Detection & Early Warning

- national hybrid threat monitoring framework,
- cyber-disinformation correlation analysis,
- social media signal detection,
- AI-supported trend analysis.

Pillar II – Attribution & Analysis

- technical cyber forensics,
- information operation mapping,
- intelligence fusion (cyber + HUMINT + OSINT),
- cooperation with international partners.

Pillar III – Prevention & Resilience

- institutional hardening,

- secure communication,
- platform cooperation,
- media literacy initiatives.

Pillar IV – Response & Crisis Management

- coordinated incident response playbooks,
- strategic communications protocols,
- legal and diplomatic escalation mechanisms.

Pillar V – Recovery & Trust Restoration

- post-incident transparency,
- public confidence rebuilding,
- institutional learning cycles.

Role of AKSK

AKSK acts as:

- national technical authority,
- hybrid threat fusion hub,
- international coordination point,
- strategic advisor to government and parliament.

Key AKSK functions:

- national risk assessments,
- threat intelligence sharing,
- operational coordination,
- capacity-building leadership.

Inter-Institutional Coordination Model

- National Hybrid Threat Task Force (standing mechanism)
- Secure information-sharing channels
- Joint exercises and simulations
- Crisis escalation protocols

International Cooperation

- Hybrid CoE participation and exercises
- EU mechanisms (NIS2, Digital Services Act cooperation)
- NATO hybrid threat frameworks
- Bilateral strategic partnerships

Elections and Democratic Safeguards

- election-period threat monitoring
- coordination with electoral authorities
- rapid response to information manipulation
- Protection of voter trust

Technology & Capability Development

- AI-SOC for disinformation correlation
- national cyber-information fusion platforms
- advanced analytics and threat modeling
- secure government communications

Capacity Building & Training

- specialized hybrid threat training
- scenario-based exercises
- cross-sector workshops
- academic and research cooperation

Legal Development Roadmap

- clarification of foreign interference offenses
- transparency rules for political advertising
- platform cooperation obligations
- safeguards for freedom of expression

Governance, Oversight & Accountability

- parliamentary oversight mechanisms
- independent audits
- annual public reporting
- human rights compliance

Implementation Roadmap (2025–2030)

Phase I (2025–2026)

- institutional setup
- legal alignment
- monitoring capabilities

Phase II (2027–2028)

- advanced analytics
- international integration
- election-focused readiness

Phase III (2029–2030)

- maturity & sustainability
- regional leadership role
- continuous improvement

Conclusion

Hybrid threats are a **long-term strategic challenge**, not a temporary crisis. Through this Plan, Albania affirms its commitment to:

- democratic resilience,
- rule of law,
- strategic sovereignty,
- European and transatlantic security values.

AKSK stands ready to lead this effort with professionalism, transparency, and international partnership.

Legal, Institutional, and Euro-Atlantic Alignment Framework

ANNEX I: Legal Annex – Draft Legislative Amendments

Purpose of the Legal Annex

This Legal Annex provides a **structured roadmap for legislative amendments** required to effectively counter **illegal foreign interference and disinformation** as hybrid threats, while fully safeguarding:

- freedom of expression,
- media pluralism,
- constitutional order,
- fundamental rights.

The proposed amendments are **preventive, proportionate, and EU-aligned**, avoiding censorship while closing strategic legal gaps exploited by foreign actors.

Identified Legal Gaps

Current legislation presents limitations in addressing:

- covert foreign influence operations,
- cross-platform disinformation coordination,
- cyber-enabled manipulation below criminal thresholds,
- attribution and response authority during hybrid incidents.

Draft Legislative Amendments (Indicative)

A. Amendments to National Cybersecurity Legislation

Proposed additions:

- Formal legal definition of *cyber-enabled hybrid threats*

- Explicit mandate for AKSK to:
    - detect and analyze cyber-disinformation convergence,
    - coordinate national response to foreign cyber-information operations,
    - issue technical risk advisories to institutions and regulators.

B. Amendments to Criminal and Administrative Law

New legal concepts to be introduced:

- *Illegal foreign interference* as a distinct offense when:
    - conducted covertly,
    - coordinated by foreign actors,
    - aimed at destabilizing democratic institutions.

Graduated response model:

- administrative measures → criminal prosecution → diplomatic escalation.

C. Amendments to Media and Electoral Frameworks

Key proposals:

- transparency obligations for political advertising and sponsorship,
- disclosure of foreign funding or coordination,
- election-period safeguards against coordinated disinformation campaigns,
- emergency coordination mechanisms between AKSK, election bodies, and regulators.

D. Platform Cooperation Provisions

Without imposing content control:

- legal obligation for platforms to cooperate during declared hybrid threat situations,
- rapid data preservation for attribution purposes,
- compliance with EU Digital Services Act principles.

Role of the Parliamentary Disinformation Commission

The **Parliamentary Disinformation Commission (established 2024)**:

- reviews legislative gaps annually,
- proposes amendments based on threat evolution,
- receives classified and non-classified briefings from AKSK,
- ensures democratic oversight and proportionality.

ANNEX II - Institutional Mandate Matrix (AKSK vs Other National Actors)

Objective

This matrix clarifies **roles, responsibilities, and boundaries**, preventing overlap while enabling rapid coordination.

Mandate Matrix

Table 2: Role of Stakeholders

Institution	Primary Mandate	Role in Hybrid Threats	Coordination with AKSK
AKSK	National cybersecurity authority	Detection, analysis, coordination of cyber-enabled hybrid threats	Lead coordinator
AKSHI	Government Agency for Information Society	In cooperation with AKSK Detection, analysis, coordination of cyber-enabled hybrid threats	Co- Lead coordinator
Council of Ministers	Strategic governance	National crisis decisions, policy direction	Strategic oversight
Intelligence Services	National security intelligence	Attribution, foreign actor analysis	Intelligence sharing
State Police / Prosecution	Law enforcement	Criminal investigation and prosecution	Evidence & referrals
Electoral Authorities	Democratic process integrity	Election security	Joint election-period protocols
Media Regulator	Media standards	Oversight of compliance & transparency	Risk alerts
Parliament	Democratic oversight	Legislative control & accountability	Hearings & reporting

AKSK's Coordinating Authority

AKSK does **not**:

- censor content,
- replace law enforcement,
- interfere with editorial independence.

AKSK **does**:

- act as technical risk authority,
- issue hybrid threat alerts,
- coordinate national response mechanisms.

ANNEX III - EU & NATO Alignment Mapping

Strategic Rationale

Albania's approach to hybrid threats is **fully aligned with Euro-Atlantic security doctrine**, ensuring:

- interoperability,
- legal coherence,
- trust among partners.

EU Alignment

Table 3: Area of EU Instrument

EU Instrument	Alignment Area
NIS2 Directive	Cyber resilience & incident coordination
Digital Services Act (DSA)	Platform transparency & systemic risk
EU Action Plan Against Disinformation	Strategic communication & resilience
EU Hybrid Toolbox	Sanctions, diplomacy, resilience

AKSK acts as the **national technical interface** for these instruments.

NATO Alignment

Table 4: Nato Alignment

NATO Framework	Alignment Area
NATO Hybrid Warfare Strategy	Whole-of-government response
NATO Cyber Defence Policy	Cyber-hybrid convergence
Strategic Communications Doctrine	Counter-influence operations
Resilience Baselines (Article 3)	Societal resilience

Hybrid CoE Membership

In **June 2024**, Albania became the **36th member** of the **European Centre of Excellence for Countering Hybrid Threats**.

This membership enables:

- access to classified and unclassified threat analysis,
- participation in hybrid exercises,
- doctrinal alignment with EU and NATO members,
- regional leadership opportunities.

ANNEX IV - EU Accession – Chapter 31 Cross-Reference Table (Foreign, Security and Defence Policy)

Purpose of the Annex

This annex provides a structured cross-reference between:

- EU Accession Chapter 31 (Foreign, Security and Defence Policy) requirements, and
- Albania's Strategic Plan on Countering Illegal Foreign Interference and Disinformation as Hybrid Threats (2025–2030).

It demonstrates:

- substantive alignment with EU CFSP/CSDP objectives,
- institutional readiness,
- Albania's contribution to EU collective security,
- coherence between cybersecurity, hybrid threats, and foreign policy obligations.

Relevance of Hybrid Threats to Chapter 31

Hybrid threats, including:

- foreign interference,
- disinformation,
- cyber-enabled influence operations,

are now explicitly recognized by the EU as security challenges under CFSP and CSDP, and therefore fall squarely within Chapter 31 screening and alignment.

Albania's approach reflects:

- the EU Strategic Compass,
- the EU Hybrid Toolbox,
- the EU Action Plan Against Disinformation,
- EU cyber and resilience policies.

Chapter 31 Cross-Reference Table

Table 5: Cross Reference Table

Chapter 31 Requirement / Area	EU Expectations	Albanian Strategic Response	Responsible Authority
CFSP Alignment	Progressive alignment with EU foreign and security positions	Strategic Plan explicitly aligns with EU hybrid threat doctrine	Council of Ministers / MFA
Hybrid Threats	National capability to prevent and respond	Hybrid threats designated as a core pillar of Cyber Security Strategy 2025–2030	AKSK
Disinformation	Whole-of-society resilience	Parliamentary Disinformation Commission (2024) + AKSK technical role	Parliament / AKSK
Cybersecurity	National coordination authority	AKSK as national cyber & hybrid coordinator	AKSK
Election Security	Protection of democratic processes	Election-period hybrid threat monitoring & response	AKSK / CEC
Strategic Communication	Counter hostile narratives	Coordinated response & public trust restoration mechanisms	Government / AKSK
Legal Framework	Proportionate, rights-based approach	Draft legislative amendments (Annex I)	Parliament / Government
Institutional Capacity	Clear mandates & coordination	Institutional mandate matrix (Annex II)	Council of Ministers
EU Cooperation	Information sharing & joint response	Integration with EU hybrid mechanisms	AKSK / MFA
NATO-EU Coherence	Complementarity, no duplication	NATO-aligned cyber-hybrid model	AKSK / MOD

Contribution to EU CFSP and CSDP Objectives

Through this Strategic Plan, Albania contributes to:

- EU resilience against hybrid threats,
- security of the EU information space,
- protection of democratic institutions,
- collective situational awareness,
- transatlantic and European security coherence.

Albania positions itself not only as a policy taker, but as an active security contributor in the Western Balkans.

Institutional Readiness Assessment (Chapter 31 Perspective)

Table 6: Institutional Readiness Assessment

Dimension	Status
Political commitment	High
Legal alignment	In progress (draft amendments prepared)
Institutional coordination	Established
Technical capability	Operational and expanding
Parliamentary oversight	In place (since 2024)
EU interoperability	Strong
NATO coherence	Strong

Screening Narrative (Suggested EU Language)

Albania has demonstrated a high level of preparedness in addressing hybrid threats, including disinformation and foreign interference, through a comprehensive national strategy anchored in cybersecurity governance. The establishment of a Parliamentary Disinformation Commission and the designation of AKSK as the national coordinating authority provide a robust institutional and democratic framework aligned with EU CFSP and CSDP priorities.

Added Value for EU Accession

This Strategic Plan:

- strengthens Albania's **Chapter 31 credibility**,
- supports **horizontal alignment** with Chapters 10, 23, and 24,
- demonstrates **institutional maturity**,
- reduces regional security risks for the EU.

Conclusion

The inclusion of hybrid threats and disinformation within Albania's cybersecurity and national security architecture represents full conceptual and operational alignment with EU Chapter 31 objectives.

This annex confirms Albania's readiness to:

- engage constructively in CFSP,
- contribute to EU collective resilience,
- assume responsibilities of EU membership in the security domain.