REPUBLIC OF ALBANIA
NATIONAL CYBER SECURITY AUTHORITY

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

Adress: Street "Papa Gjon Pali II", nr.3, Tiranë
WEB: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax : 04 2221 039

# CONTENTS

## 1. Purpose of the Policy

The purpose of this Policy is to establish a coherent national framework for preventing, detecting, attributing, and responding to illegal foreign interference and disinformation as hybrid threats to the Republic of Albania. The Policy operationalises Albania's strategic commitment under the National Cyber Security Strategy 2025–2030, which identifies hybrid threats as one of its five strategic pillars. It aims to safeguard democratic institutions, constitutional order, public trust, and national security by strengthening legal, institutional, technical, and societal resilience. The Policy further seeks to ensure Albania's alignment with EU, NATO, and transatlantic approaches to countering hybrid threats, while fully respecting fundamental rights, freedom of expression, and democratic oversight.

## 2. Scope of Application

This Policy applies to all public institutions, independent authorities, and state bodies whose responsibilities relate to national security, cybersecurity, information integrity, electoral processes, crisis management, and the functioning of democratic governance. It establishes a comprehensive and coordinated framework through which these actors contribute to the prevention and management of hybrid threats affecting the Republic of Albania.

The scope of the Policy extends to cyber-enabled hybrid threats in all their manifestations, including illegal foreign interference, disinformation and coordinated influence operations, as well as activities aimed at disrupting elections, undermining public institutions, and compromising critical information flows. It addresses threats that exploit digital technologies, information ecosystems, and institutional or societal vulnerabilities to weaken democratic processes, public confidence, and national resilience.

Recognising that hybrid threats transcend institutional and sectoral boundaries, this Policy also applies, where appropriate, to cooperation with private sector actors, digital platforms, media organisations, academia, and civil society. Such cooperation is pursued in line with a whole-of-society approach, reflecting the understanding that effective prevention, resilience, and response require shared responsibility, structured collaboration, and sustained engagement across all segments of society.

## 3. Fundamental Principles

The implementation of this policy is grounded in full respect for the sovereignty and constitutional order of the Republic of Albania, ensuring the protection of institutional independence and the democratic functioning of the state. All envisaged measures are undertaken in accordance with the principles of the rule of law and proportionality, ensuring that actions taken to counter hybrid threats do not undermine freedom of expression, media pluralism, or fundamental human rights.

The policy promotes transparency, accountability, and democratic oversight through the roles of the relevant institutions and through periodic public reporting. A key element of this approach is intergovernmental and societal cooperation, aimed at strengthening inter-institutional coordination and ensuring the involvement of public, private, and academic stakeholders.

At the same time, the policy ensures full alignment with Euro-Atlantic standards and policies, harmonizing national actions with the frameworks of the European Union and NATO.

## 4. Roles and Responsibilities

Within the framework of this policy, the National Cyber Security Authority (AKSK) exercises a coordinating role in addressing hybrid threats. AKSK acts as the national technical authority responsible for the identification, analysis, and management of such threats, while simultaneously serving as the national coordinating centre for early warning, risk analysis, and coordinated incident response. In this context, AKSK also serves as the primary international liaison point for technical and operational cooperation with regional, European, and Euro-Atlantic partners.

In fulfilling this role, AKSK conducts periodic national risk assessments, develops and disseminates intelligence related to hybrid threats and influence operations, and coordinates inter-institutional responses in cases of hybrid incidents or crises. In parallel, AKSK leads institutional capacity-building processes and provides strategic advisory support to state institutions, with the aim of strengthening national resilience and enhancing preparedness to address complex and evolving threats.

The effective implementation of the policy is further supported by a clear allocation of roles and responsibilities among other state institutions. The Council of Ministers provides strategic direction and adopts decisions in crisis situations, ensuring high-level political and institutional coordination. Intelligence services contribute through the identification and analysis of foreign actors, as well as through strategic assessments of the security environment. The State Police and prosecutorial authorities exercise their respective competencies in the investigation and prosecution of offences related to foreign interference and unlawful activities.

Electoral authorities hold specific responsibilities for safeguarding the integrity of electoral processes, in close cooperation with AKSK and other relevant institutions, particularly during electoral periods. Media and regulatory authorities contribute to ensuring standards of transparency, pluralism, and accountability within the information space. Parliament, through democratic oversight mechanisms and the legislative process, ensures institutional control, accountability, and the continuous updating of the legal framework in line with the evolving nature of hybrid threats.

## 5. Core Elements of the Policy

The Policy is structured around five interrelated operational pillars that together form a comprehensive framework for countering hybrid threats. The first pillar focuses on detection and early warning, establishing national monitoring capabilities for cyber, information, and digital indicators, including the use of advanced analytics and AI-supported tools to identify emerging threats at an early stage. The second pillar addresses attribution and analysis, relying on integrated cyber forensics, intelligence fusion, and close cooperation with international partners to enable accurate assessment and informed decision-making.

The third pillar emphasises prevention and resilience, through measures aimed at strengthening institutional safeguards, enhancing cooperation with digital platforms, promoting media literacy, and ensuring secure communications across public

institutions. The fourth pillar concerns response and crisis management, providing coordinated response playbooks, strategic communication protocols, and legal and diplomatic escalation mechanisms to ensure timely and proportionate action during hybrid incidents.

The fifth pillar focuses on recovery and trust reinforcement, prioritising post-incident transparency, institutional learning, and measures to rebuild public confidence, thereby reinforcing long-term democratic resilience and institutional credibility.

## 6. International Cooperation

International cooperation constitutes another key pillar of this policy, reflecting the cross-border and complex nature of hybrid threats. The policy provides for the active participation of the Republic of Albania, through the National Cyber Security Authority (AKSK), in international mechanisms and structures dedicated to countering hybrid threats, including engagement with the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). This engagement aims to enhance interoperability, facilitate the exchange of strategic analyses, support participation in exercises, and strengthen joint capacity-building efforts.

The policy also ensures full integration with the mechanisms and instruments of the European Union, including the NIS2 Directive, the Digital Services Act (DSA), and the EU Hybrid Toolbox, thereby guaranteeing coherence between national policies and the European regulatory framework. At the same time, the envisaged actions are aligned with NATO frameworks on hybrid threats and societal resilience, reinforcing Euro-Atlantic cooperation and Albania's contribution to collective security.

Within this framework, the policy promotes the development of bilateral and multilateral partnerships with partner states, international organizations, and counterpart institutions, with the objective of enhancing information exchange, operational coordination, and the implementation of joint initiatives in the areas of prevention and response to hybrid threats.

## 7. Legal Development and Oversight

The Policy is firmly grounded in the Constitution of the Republic of Albania and in the national legal framework governing security, cybersecurity, data protection, media, and electronic communications. It establishes a clear roadmap for legislative development to address identified legal and regulatory gaps, including those related to illegal foreign interference, cyber-enabled influence operations, cooperation with digital platforms, and the protection of electoral processes during election periods. Democratic oversight is ensured through Parliament, including the role of the Parliamentary Commission on Disinformation, which reviews emerging risks, proposes legislative and policy measures, and receives technical expertise and risk assessments from AKSK.

## 8. Implementation and Timeline (2025–2030)

The implementation of the policy is envisaged to take place in several phases over the period 2025–2030, reflecting a progressive and sustainable approach. The first phase, covering the period 2025–2026, focuses on institutional building and

consolidation, as well as on aligning the legal and regulatory framework with the emerging requirements arising from hybrid threats.

The second phase, covering the period 2027–2028, aims at the development of advanced analytical capacities, the strengthening of international coordination mechanisms, and deeper integration into European and Euro-Atlantic structures and initiatives. This phase is focused on enhancing operational readiness and improving institutional interoperability.

The third phase, spanning the period 2029–2030, aims to achieve full operational capability and to consolidate Albania's role as an active contributor and regional leader in addressing hybrid threats, ensuring that the mechanisms established are sustainable and capable of adapting to future developments.

## 9. References

This Policy draws upon the Constitution of the Republic of Albania, the National Cyber Security Strategy 2025–2030, and the relevant national legislation on security and cybersecurity. It is further informed by European Union legal and policy instruments addressing hybrid threats and disinformation, NATO hybrid defence and resilience frameworks, and the Strategic Plan on Countering Illegal Foreign Interference and Disinformation as Hybrid Threats (2025–2030), including its accompanying analytical and strategic documentation.

## 10. Review Frequency

This Policy is subject to periodic review in order to ensure its continued relevance and effectiveness. Reviews shall be conducted every two years or earlier where required by significant changes in the threat landscape, developments in EU or NATO obligations, or evolving national security priorities. The review process shall be coordinated by AKSK and submitted to the competent authorities and Parliament for consideration.