American Center for Combating Extremism and Terrorism (ACCET)

High-Level Summit Report

COUNTERING COERCIVE AI

Regional Challenges and Strategic Dialogue on National Security in the Age of Artificial Intelligence

Organized by:

American Center For Combating Extremism and Terrorism (ACCET)

Tirana, Albania | June 9, 2025

Countering Coercive AI:

Regional Challenges and Strategic Dialogue on National Security in the Age of Artificial Intelligence

Summit Report | Tirana, Albania | June 9, 2025
Organized by the American Center for Combating Extremism and Terrorism (ACCET)
Supported by the Open Society Foundation

I. Executive Summary

On June 9, 2025, the American Center for Combating Extremism and Terrorism (ACCET), with support from the Open Society Foundation, hosted a high-level summit in Tirana, Albania, titled *"Countering Coercive AI: A Strategy Against Technological Aggression by Adversarial States."* The event convened government leaders, security professionals, international organizations, civil society actors, and academic experts to examine how artificial intelligence (AI) is reshaping the security landscape—both as a strategic tool and as a vehicle for exploitation by hostile states and extremist groups.

Discussions focused on the growing misuse of AI for surveillance, disinformation, radicalization, and cyber intrusion. Key concerns included the vulnerability of democratic institutions to external technological interference, the risks of under-regulated AI surveillance systems, and the urgent need for proactive, ethical approaches to AI governance in security contexts.

Albania was consistently recognized as a regional model—praised for its political will, repatriation efforts, and prevention-based strategies in countering violent extremism (CVE). The summit also underscored the unique role of civil society organizations in monitoring emerging threats, supporting reintegration, and extending institutional reach to underserved areas.

There was broad consensus that AI is not a future issue—it is a present, immediate challenge requiring cross-sector collaboration, public awareness, and a commitment to democratic values and rule-of-law principles. Participants called for stronger vetting of foreign technology partnerships, increased investment in digital literacy, and the continued inclusion of youth and community actors in shaping long-term responses to technological aggression.

II. Key Themes and Presentations

The summit opened with a series of high-level remarks and expert presentations exploring how artificial intelligence (AI) is shaping the future of counterterrorism and national security. Each session offered unique insights into the dual-use nature of AI and the urgent need for coordinated strategies that safeguard both security and democratic values.

Opening Remarks

The event began with welcoming remarks from four key leaders, each offering distinct perspectives from civil society, government, and multilateral institutions.

Mr. Arianit Shehu, Executive Director of the American Center for Combating Extremism and Terrorism (ACCET), formally opened the summit by welcoming participants and thanking the Open Society Foundations for sponsoring the event. He highlighted the pressing nature of the discussion and stressed the need for strategic cooperation to counter the threats posed by adversarial uses of AI.

“This is not just a conversation about technology,” Mr. Shehu said. “It is about protecting democratic systems, securing the rights of our citizens, and ensuring our institutions are prepared for the next generation of challenges.”

Ms. Lejdi Dervishi, Director of the Coordination Center for Countering Violent Extremism (CVE) – Albania Ministry of Interior, followed with remarks on Albania’s evolving experience with CVE. She stressed that while Albania’s risk profile may appear low today, that status is fragile—and continued investment in resilience, education, and inclusive governance is essential.

She cautioned against equating extremism solely with religion and noted that radicalization increasingly stems from ethnic, nationalist, or gender-based ideologies. “Resilience is only real when we invest in it consistently—especially through education and prevention. That work must continue,” she said.

Ms. Lejdi Dervishi
Director of the Coordination Center f
Countering Violent Extremism
Albania
Mr. Edward Anderson

Ms. Dervishi emphasized that CVE must remain a national priority, even as public and political attention shifts toward other security concerns. She noted a troubling rise in hate speech and antisemitism on Albanian-language platforms, often originating from outside Albania’s borders, but with the potential to radicalize domestic audiences.

She highlighted the unique vulnerability of youth online and the need to:

- Train community police and educators in digital safety and media literacy.
- Invest in AI tools that help detect and flag radicalization cues before harm occurs.
- Maintain a broad definition of extremism that includes ethnic, nationalist, and gender-based ideologies—not only religion-linked threats.

"Being proactive is always better than being reactive," she said. "When we're reactive, it's almost too late."

Dr. Dwaine Lee, Vice President for Global Programs at ACCET, offered a global perspective grounded in personal connection. Noting his Albanian family ties and professional background across fragile states, he framed the issue not just as a technological concern—but as a matter of trust, democracy, and shared values.

"AI is here. It's already changing how we live, how we work—and how we protect ourselves," he said. "It is being used to help. But it is also being used to harm."

Dr. Lee detailed how AI is now supercharging online recruitment, misinformation, and the erosion of institutional trust. He warned that malign actors—from terrorist groups to foreign governments—are exploiting digital tools to destabilize societies. The antidote, he argued, is proactive, principled collaboration.

"If we wait, we lose. If we act, we lead," he concluded. "And if we act together now—we can shape the future before it shapes us."

Mr. Edward Anderson, Head of the Public Safety and Community Outreach Department at the OSCE, closed the opening session by reminding participants of the OSCE's mandate to strengthen security and community resilience through practical cooperation. He previewed his upcoming presentation on the use and misuse of AI and noted that governments must not only adopt new tools—but understand their risks and limitations.

Featured Presentations

1. **The Role of AI in Counterterrorism and National Security**
   ***Mr. Scott Bates**, Former Senior Policy Advisor, U.S. House of Representatives Homeland Security Committee; Senior Fellow, American Security Project*

In the first formal presentation of the day, Mr. Bates outlined how AI is transforming the counterterrorism and defense landscape. He shared insights on both strategic opportunities and emerging threats—from border security and drone surveillance to deepfakes and AI-enabled propaganda.

He highlighted the low barrier to entry for terrorist groups and malign states using AI, warning that asymmetric actors now have tools once reserved for nation-states. He also described how the U.S. government is accelerating AI integration across military and civilian institutions under new executive directives.

“The imperative is clear,” Bates said. “Use these tools to stay one step ahead—or risk being overrun by adversaries who have no obligation to follow the rule of law.”

He also emphasized the potential for U.S. allies like Albania to integrate AI for defense applications, logistics, and institutional modernization—especially if supported through EU and transatlantic mechanisms.

2. **From Tool to Threat: Navigating the Use and Misuse of Artificial intelligence**
   Mr. Edward Anderson, Head of Public Safety and Community Outreach Department, OSCE

Mr. Anderson delivered a compelling presentation on the real-world risks posed by poorly understood or poorly governed AI systems. He described how voice data, facial recognition, search terms, and even syntax patterns are now compiled into predictive profiles—often with insufficient transparency or oversight.

Drawing on his policing and military background, he warned that unverified data can quickly lead to wrongful identification, harassment, or stigmatization. “We’re moving at lightning speed. But unlike authoritarian actors, we’re bound by law and human rights. That slows us down—and that’s exactly why our standards must be higher,” he said.

He concluded with a call for internal training, ethical safeguards, and regional partnerships that reflect local realities and democratic norms.

3. Countering Malign State Exploitation of AI

PhD(c) Gledis Nano, Former General Director of the State Police, Albania

In the final session, Mr. Nano offered a sobering account of Albania’s recent experience with cyberattacks and digital espionage. Reflecting on his own leadership during a national data breach, he described the institutional and personal toll of foreign intrusion—including the public exposure of internal police communications.

Mr. Nano warned that countries like Albania are increasingly targeted by state-sponsored entities using commercial tech platforms as proxies for surveillance and influence. He pointed specifically to the Smart City surveillance proposal, which, according to media reports, is linked to foreign military contractors.

“Even when intentions are good, we must ask: who is building the system? What are their affiliations? And what access are we giving away?” he said.

He urged greater scrutiny of foreign tech partners, stronger data protection laws, and a cultural shift in how digital security is understood within institutions.

“We can no longer afford to be relaxed,” he said. “If we think we’re ready, we are wrong. We must wake up—and do the hard work now.”

Open Discussion and Closing Reflections

Following the presentations, participants engaged in a candid and thought-provoking discussion that brought forward both concern and opportunity. There was widespread recognition that while AI introduces new forms of threat—particularly through disinformation, surveillance, and radicalization—it also demands new forms of cooperation and local adaptation.

One key thread was the **decline in political will** for regional collaboration across the Western Balkans, with tensions between neighboring states often stalling progress. Yet many participants noted that **operational-level ties between law enforcement and defense sectors remain strong** and could serve as a practical foundation for cross-border coordination on AI-related risks.

Key themes raised during the discussion included:

- **The danger of fragmented strategies** in a region where external actors often exploit instability and weak points in coordination.
- **The need to reframe AI risks** beyond military or cybersecurity threats, toward a broader lens that includes youth radicalization, digital literacy, and community trust.
- **The potential to adapt Albania's CVE model**—built on local partnerships, strong state-civil society cooperation, and ethical governance—for a regional prevention architecture.

Several participants also urged governments not to shift focus away from prevention efforts now that the immediate threat of violent extremism has decreased. As one attendee remarked, "we are safest when we are proactive, not when we assume the problem is gone."

Arianit Shehu closed the session by affirming that insights from the summit will feed directly into ACCET's policy briefs for the U.S. Congress, particularly the House and Senate Committees on Intelligence and Foreign Affairs. He stressed the importance of grounding international policy recommendations in local realities, trusted partnerships, and tangible examples of success.

III. Key Outcomes

The summit generated a robust exchange of ideas among security professionals, government officials, civil society leaders, and academics. While the event did not conclude with a formal declaration, several critical themes and consensus points emerged from the presentations and open discussion.

1. Acknowledgment of AI as a Strategic Security Risk

Across sessions, speakers affirmed that artificial intelligence is no longer a future concern—it is a present and evolving threat vector. AI is being leveraged by both state and non-state actors to disrupt democratic processes, manipulate public opinion, and erode institutional trust.

Participants underscored that this is not solely a technological issue. Rather, it is a political and societal challenge that touches on ethics, governance, legal frameworks, and human rights.

“AI is being used to supercharge disinformation, online radicalization, and social division. If we treat this only as a tech issue, we will fail to grasp the deeper risks to democratic cohesion.” — Dr. Dwaine Lee

2. The Importance of Democratic Values and Rule of Law

A recurring theme—especially from OSCE and ACCET speakers—was that democratic actors face a unique dilemma: they must respond quickly and effectively to AI threats, but they must also do so within the constraints of law, transparency, and human rights.

Participants agreed that ethical safeguards must not be seen as weaknesses but as vital sources of legitimacy and resilience. The misuse of AI by authoritarian regimes serves as a reminder of what is at stake when such guardrails are absent.

“Our systems must be faster, yes—but they must also be fair. The rule of law is not an obstacle to security. It is the foundation of it.” — Edward Anderson, OSCE

3. Recognition of Albania as a Regional Leader in Stability and CVE

Multiple speakers commended Albania for its proactive role in countering violent extremism and digital threats. The country's strong political will, coordinated interagency approach, and commitment to human rights were cited as examples that other Western Balkan countries might learn from.

Several participants noted the country's success in the repatriation and reintegration of returnees from conflict zones—emphasizing the importance of civil society partnerships and community-based prevention.

“We are a modest country in size, but we have shown that political will and coordinated action can make a difference. The risk is low today, but it will only stay low if we remain vigilant.” — Lejdi Dervishi, CVE Coordination Center

r. Edward Anderson
Head of Public Safety and
unity Outreach Department
OSCE
Ms. Lejdi Dervishi
Director of the Coordination Center for
Countering Violent Extremism
Albania
Mr. Arianit Shehu
Executive Director ACCET

4. Civil Society and Academia as Critical Actors

Speakers highlighted the unique value of civil society organizations (CSOs) and academic institutions in addressing AI-related threats. Civil society can access remote communities, build trust with youth and families, and provide early warning of online radicalization. Academia brings analytical rigor, ethical reflection, and long-term visioning.

The inclusion of these sectors was framed not as a formality, but as a strategic necessity—especially when addressing narratives, identity, and community trust.

“Security cannot be built solely from the center. Civil society has eyes, ears, and relationships in places government cannot reach.” — Closing discussion participant

5. The Dual Nature of AI: Risk and Opportunity

While the summit focused largely on the threats posed by AI, several participants emphasized its potential for positive impact. Tools for early detection of extremist content, predictive analysis of emerging risks, and automated verification of disinformation were mentioned as areas worth exploring.

At the same time, concerns were raised about capacity gaps, training needs, and the risk of overreliance on opaque algorithms.

“AI can be a tool for prevention—but only if we know how to use it responsibly, with the right legal and institutional safeguards in place.” — Gledis Nano

IV. Key Recommendations

While the summit was designed as an open exchange rather than a formal decision-making forum, several practical recommendations emerged through the presentations and participant dialogue. These insights are particularly relevant for government agencies, civil society organizations, security professionals, and international partners across Albania and the wider Western Balkans.

1. Build Institutional Awareness of AI-Driven Threats

Speakers stressed that many frontline institutions—including police, education systems, and municipal authorities—remain under-informed about the specific threats posed by AI-powered manipulation, surveillance, and disinformation. Targeted awareness campaigns and scenario-based briefings should be delivered to:

- Law enforcement and military professionals
- Educators and public servants
- Prosecutors, judges, and magistrates

“Our officers are trained for physical evidence, not digital manipulation. But today’s threats may originate thousands of kilometers away.” — Edward Anderson

2. Promote Digital Literacy and Resilience Among Youth

Several participants emphasized that young people—particularly in remote or underserved areas—are highly vulnerable to manipulation through social media, games, and AI-driven content. Countering this requires proactive investment in:

- Digital literacy curricula in schools
- AI-awareness sessions for youth and parents
- Content validation tools and civic education materials

“Young people are not just passive targets—they are active users. We must equip them with critical thinking, not just technical tools.” — Lejdi Dervishi

3. Scrutinize Foreign Technology Partnerships

Gledis Nano and others voiced concern over the growing presence of foreign-linked technology projects in national infrastructure, including AI-powered surveillance platforms. He called for increased scrutiny of:

- The origin and affiliations of vendors and contractors
- Data ownership and cross-border data flow implications
- Whether existing procurement frameworks provide enough protection

“Even well-intentioned projects can introduce unacceptable risks if we don’t ask the right questions early.” — Gledis Nano

4. Invest in Internal Capacity Before Deploying AI Tools

While many agreed on the usefulness of AI for security, multiple speakers warned against premature or unregulated use. Institutions must first invest in:

- Internal training on how AI systems function and fail
- Legal frameworks governing data use and accountability
- Ethics reviews and human rights compliance mechanisms

“Before we apply AI to fight crime or terrorism, we must train our own staff to understand it—and to question it.” — Edward Anderson

5. Continue to Elevate the Role of Civil Society in Prevention

The summit reinforced Albania’s success in mobilizing civil society organizations (CSOs) for early intervention and rehabilitation, particularly around returnees and families at risk. Participants urged continued recognition of CSOs as:

- First-line responders in prevention
- Trust-building actors in affected communities
- Partners in P/CVE policy development and education

“Civil society knows the terrain. They must not be an afterthought—they are a front-line partner.” — Closing participant comment

The American Center For Combating Extremism And Terrorism
Our Vision:
A safer, more secure world for all
The American Cente
ism And Terrorism

V. Conclusion

The Tirana summit underscored a growing consensus: artificial intelligence is not only transforming societies—it is actively reshaping the threat landscape. From disinformation and deepfakes to automated recruitment and foreign-backed surveillance systems, the misuse of AI presents a complex, fast-evolving challenge for democratic societies.

Yet the summit also revealed the strength of Albania and the Western Balkans in facing these risks. Participants highlighted Albania's stability, political will, and multi-sectoral coordination as a model for the region. They called for continued investment in awareness, training, youth engagement, and the ethical use of emerging technologies.

Above all, the event reaffirmed that effective responses must be rooted in democratic values, rule of law, and trust between state and society. Technology alone cannot deliver security. But informed leadership, inclusive partnerships, and regional cooperation can.

As Scott Bates put it:

"We have to stay one step ahead—not only with better technology, but with shared values, clear rules, and real partnerships."

This summit was a step toward action—grounded in dialogue, shared purpose, and a common commitment to protecting the future.