

Project
**“Enhancing resilience in Albanian cyber ecosystem
against Violent Extremism”**

**Legislative framework for countering
Violent Extremism in cyberspace in Albania**

December 2019

Funded by



U.S. EMBASSY
Tirana, Albania

Authors:

Edlira Gjollëshi

Eda Buci

Consultant: Erjon Tase



U.S. EMBASSY
Tirana, Albania

This publication is part of the project “**Enhancing resilience in Albanian cyber ecosystem against Violent Extremism**”, supported financially by the Public Affairs Office of the US Embassy in Tirana.

Opinions, findings, conclusions and recommendations expressed are of the author/s, and do not necessarily represent those of the State Department.

INTRODUCTION

The Academy of Political Studies (APS) is implementing the project “**Enhancing resilience in Albanian cyber ecosystem against Violent Extremism**”, aiming to build well-defined mechanisms for counting online radicalization of vulnerable groups of users. This goal it is expected to be addressed through both high quality research on the current situation on electronic publishing services in Albania and advocacy actions to tackle the illegal content in internet.

The recommendations and assessments produced by a pool of local experts intend to ensure the involvement and greater understanding of decision-makers towards addressing the gaps in legal framework in view of establishing this mechanism against the contaminating elements circulating on the internet and affecting cyber security.

To achieve the objective set, it was undertaken a desk research starting by a thorough analysis of the current situation as regards the institutional and legal framework, resources as well as capacities of local actors to implement the mechanism for counting online radicalization.

The conclusions highlighted in this report will be presented and discussed with decision-makers and relevant stakeholders, aiming to further investigate on the challenges of implementation of existing recommendations.

I. BACKGROUND

Online platforms are important drivers of innovation and growth in the digital economy. They have enabled an unprecedented access to information and exchanges as well as new market opportunities, notably for small and medium-sized enterprises (SMEs). Online platforms also provide the main access point to information and other content for most people on the internet today, be it through search engines, social networks, micro-blogging sites, or video-sharing platforms. The business models of platforms have also evolved recently towards closer links between users and content – notably for targeted advertisement. These platforms connect billions of users with vast quantities of content and information¹ and provide innovative services to citizens and business.

However, the important spread of illegal content that can be uploaded and therefore accessed online raises serious concerns that need forceful and effective replies. Incitement to terrorism, xenophobic and racist speech that publicly incites hatred and violence, as well as child sexual abuse material are present online and more than never accessible by users. The increasing availability of terrorist material online and the spreading of such content is a serious threat to security and safety, as well as to the dignity of victims. Many governments has responded to these concerns through a certain number of measures. However, addressing the detection and removal of illegal content online represents an urgent challenge for the digital society today.

Concerned by series of terrorist attacks in the EU and proliferation of online terrorist propaganda, the European Council of 22-23 June 2017 stated that it "expects industry to ... develop new technology and tools to improve the automatic detection and removal of content that incites to terrorist acts. This should be complemented by the relevant legislative measures

at EU level, if necessary". Similarly, the European Parliament, in its resolution on Online Platforms of June 2017 urged these platforms "to strengthen measures to tackle illegal and harmful content", while calling on the Commission to present proposals to address these issues.

On the same vein, the Government of Albania has been increasingly focused on developing more effective strategies to reduce the appeal of terrorism and limit the pool of potential recruits in both offline and online space. The National Strategy and respective Action Plan against the Violent Extremism in Albania (2015) consider the fight against violent extremism one of its fundamental priorities.

II. LEGAL FRAMEWORK DEVELOPMENT

The national policies towards countering the online violent extremism in Albania are guided by the following **fundamental documents**:

National Security Strategy (2014) - (drafting the new strategy 2020-2024)

The National Security Strategy reflects the development of state policies for the security of citizens, the society and Albanian democratic state against external and internal risks and threats. The terrorism is set in this strategic document as one the real transnational danger for the Albanian Republic security (Point 29.3, page 12). "The geo-strategic position of Albania is one more element that leads towards our country being used as a logistics and communication route. Militant and extremist groups, which use violence as a way of realizing their political objectives, are a serious danger in the security of people's lives and functioning of the state in the Albanian Republic".

National Strategy on Countering Violent Extremism (2015)

The National Strategy on Countering Violent Extremism and the National Action Plan, address the phenomenon in the approach of preventing the driving and attracting factors that nurture and empower concrete action to be taken like committing violent acts, accessing strategic communication and disseminating extremist propaganda using the Internet, and reintegrating citizens who have joined such extremist groups.

National Strategy on Cyber Security 2020-2025 (drafted, under the consultation process)

One of the main policy measures of this strategy (Policy 1, Objective 4) seeks to improve information infrastructures to combat cybercrime, radicalization and violent extremism. To accomplish the above, the aim will be to establish two mechanisms to:

- Continues identification of contaminant elements circulating on the Internet that violate cyber security in the country.
- Establish mechanisms for regulating secure Internet in public areas, certified by the cyber security regulatory authority.

International Conventions ratified

The Republic of Albania has signed and ratified the United Nations Conventions and Protocols on Terrorism and is, in addition, a co-sponsor of United Nations Security Council Resolution 2178 (2014), as well as the **Council of Europe Convention on the Prevention of Terrorism** (CETS No.196).

Albania has also adopted **UN Security Council Resolutions 1267 and 1373**, which set out procedures for seizing property for terrorist activities. Albania was one of the sponsors of **UN Resolution 2178** (2014) "Condemning violent extremism, underlining the need to prevent travel and support for foreign terrorist fighters" adopted by the Security Council in September 2014.

In the cybercrime sector, Albania has harmonized its legislation with the **Council of Europe Convention on Cyber Crime** (ETS No.185). The **Budapest Convention on Cybercrime** was incorporated into national law in Albania in 2008. Albania intends for the Budapest Convention to be used as a global framework for measures against information network crimes. In 2004, Albania ratified the "Additional Protocol of the Cyber Crime Convention, for the penalization of racial and xenophobic natured acts carried out via computer systems" (ETS No. 189).

For the implementation of these strategic approach a number of important laws and regulation have been adopted and drafted, such as:

- **Law no. 7895, dated 27.1.1995** "Criminal Code of the Republic of Albania"
- **Law no. 7905 dated 21.03.1995** "Code of Criminal Procedure of the Republic of Albania";
- **Law no. 9918, dated 19.05.2008** "On electronic communications in the Republic of Albania", as amended by Law no. 102/2012 in line with the latest developments in the EU acquis;
- **Law no. 9887, dated 10.3.2010** "On the protection of personal data", as amended by Law no. 48/2012 and Law no. 120/2014;
- **Law no. 10325, dated 23.9.2010** "On State Databases";
- **Law No. 72, dated 28.6.2012** "On the Organization and Functioning of the National Geospatial Information Infrastructure in the Republic of Albania";
- **Law no. 2/2017** "On cyber security" (Cyber Security Law);

The legal mechanisms designed to combat terrorism and violent extremism are currently present in the Criminal Code of the Republic of Albania. According to Article 28/2 of the Code: *"A terrorist organization is a special form of criminal organization, consisting of two or more persons, who have a consistent cooperation in time, with the intent to commit acts of terrorist*

intent." Chapter VII of the Criminal Code contains 17 other articles, which define the types of terrorist violence, the creation and financing of terrorist organizations, the recruitment and training of individuals for the purpose of committing acts of terrorism.

Article 230 of the Criminal Code has been amended to include terrorist crimes in order to spread panic among the population or to compel state, Albanian or foreign bodies to commit or not to perform a particular act, or to destroy or destabilize, in serious, essential political, constitutional, economic or social structures of the Albanian state, of another state, institution or international organization including:

- i) abduction of individuals;
- ii) serious damage to public property, infrastructure, transport systems; hijacking of aircraft, ships, other means of transport or fixed platforms;
- iii) production, holding, purchase, transport or marketing of explosives, firearms, biological, chemical or nuclear, as well as scientific research for the production of weapons of mass destruction and so on.

Article 230 / a is intended to impede the financing of terrorism by punishing such conduct with 15 years of imprisonment, while Article 230 imposes sanctions on individuals concealing funds used to finance terrorist activities.

Many amendments to the Criminal Code were adopted in 2007, specifically in conjunction with Article 231 of the Code, in order to incorporate into national law the obligations undertaken by Albania with regard to the ratification of the **European Convention on the Prevention of Terrorism by condemning "Recruiting individuals for the purpose of committing terrorist acts or financing terrorist activities"**, even where such acts are directed to another state, an international institution or organization. In October 2013, the Assembly also adopted Law No. 157 "On Measures against the Financing of Terrorist Activities".

In recent years, changes have been made to Article 265 / a, b, c of the Criminal Code. These Articles set out the security measures applicable to **individuals fighting in a foreign country** (Article 256 / a); Organization for participation in fighting in a foreign country (Article 256 / b); Call for participation in violent acts in a foreign country (Article 265 / c). These articles complement an already broad legal framework regulating terrorist activities, violent extremism and financing of terrorist activities in Albania.

In line with the Stabilization and Association Agreement commitments there is the need to transpose the following EU directives and regulations in the national legislation:

- **Directive (EU) 2017/541/EU** of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA
- **Regulation (EU) 2016/679** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal

data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

- **Directive (EU) 2016/680** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
- **Commission Recommendation (EU) 2018/334** of 1 March 2018 ‘on measures to effectively tackle illegal content online’.

III. INSTITUTIONAL FRAMEWORK

Efforts are made to establish and make functional of several structures that ensure and guarantee the implementation of the legal framework in view of ensuring a safer cyberspace from illegal content:

Coordination Center against Violent Extremism was established by DCM no. 737, dated 13.12.2017. The CVE Center serves as a catalyst for capacity building, identifying needs, and functioning mechanisms with reference to the National Strategy for Combating Violent Extremism and the Action Plan. The concepts and measures drawn up in these two documents above have given certain obligations to all Line Ministries, institutions, and other relevant actors such as civil society, religious communities, the media and international partners. Through this Strategy the CVE Center has the opportunity to develop guiding principles, policies and actions to confront radicalism and violent extremism on the territory of Albania but also to coordinate with the region or wider to undertake joint prevention initiatives.

National Authority for Electronic Certification and Cyber Security (NAECCS) is a public body, which operate under the Prime Minister's authority, pursuant to Law No. 9880/2018 “On Electronic Signature”, Law No. 107/2015, dated 1.1.2015 “On Electronic Identification and Trusted Services”, Law No. 2 / 2017 "On cyber security". The Authority aims to ensure reliability and security in electronic transactions between citizens, businesses and public authorities, enhancing the effectiveness of public and private services and electronic commerce; sets minimum technical standards for data security and information society networks / systems in accordance with international standards in this field, with a view to creating a secure electronic environment.

The Albanian State Police is the institution in charge of prevention, detection and investigation of the criminal offences, among which are included also the criminal offences in the area of ICT, which are dealt with by the Computer Crime Section.

The General Prosecution Office exercises criminal prosecution against criminal offences in the area of cybernetics through the Cyber Crime Section. This structure checks the activity of the special units that deal with cyber crimes, which are set up at District Prosecution Offices.

The State Intelligence Service (SIS/SHISH) via the Cyber Crime Section is in charge to search, detect and analyse cyber crimes that threaten the national security.

IV. CONCLUSIONS AND NEXT STEPS

The Albanian institutions has been focused during the last decade on developing the necessary legal and institutional framework in order to provide a suitable environment for business communication, building and maintaining advanced electronic communication infrastructures for the needs of public administration and e-government. Currently there is a rich legal framework that directly and indirectly regulates ICT and information society. However, the completion and improvement of ICT legislation is needed to respond to the rapid and dynamic development of this sector.

When it comes to the violent extremism threat, Albanian legislation must be harmonized as soon as possible with the EU Acquis Communautaire, creating a complete and clearly codified mechanism to correctly address such issue. The analyses of the current legal framework demonstrates the lack of legal acts to regulate relationships and clearly define the duties and rights of online platform providers in order to timely block or delete material with violent extremist content.

The guidance document “Communication from the EU Commission to the European Parliament - Tackling Illegal Content Online¹”, underlines the responsibility should be taken by the online platforms for the increased illegal content hosted by them. *“Even if such content is created and uploaded by third parties, the constantly rising influence of online platforms in society, which flows from their role as gatekeepers to content and information, increases their responsibilities towards their users and society at large. They should therefore be proactive in weeding out illegal content, preventing its reappearance, put effective notice-and-action procedures in place, and establish well-functioning interfaces with third parties (such as trusted flaggers) and give a particular priority to notices from national law enforcement authorities”*, is stressed in the document. Following this new approach of the European Union, the member countries members has developed more regulations for the online platforms operators towards illegal content.

In the same line the Albanian Government has foreseen in the draft “National Strategy on Cyber Security 2020-2025”, the establishment of two new mechanisms to regulate the relationship between the public bodies and online platforms providers to detect and prevent illegal content from cyberspace.

The proposed mechanisms should clearly define the duties of online platforms providers to prevent that their infrastructure and business is used to commit crimes. Online platforms should decisively step up their actions to address this problem, as part of the responsibility which flows from their central role in society. They must have a responsibility to protect their users and prevent illegal content on their platform, and be typically in possession of technical means to identify and remove such content.

¹ Tackling Illegal Content Online – European Commision, 28.9.2017
<https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-555-F1-EN-MAIN-PART-1.PDF>

V. REFERENCES

Council of Europe Convention on Cyber Crime (ETS No.185) -

<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>

Council of Europe Convention on the Prevention of Terrorism (CETS No.196) -

<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196>

UN Security Council Resolutions 1373 (2001) on Threats to international peace and security caused by terrorist acts – [https://undocs.org/S/RES/1373\(2001\)](https://undocs.org/S/RES/1373(2001))

United Nations Security Council Resolution 2178 (2014) -

<https://www.un.org/securitycouncil/s/res/2178-%282014%29>

Albanian National Security Strategy (2014) -

<http://www.mod.gov.al/eng/index.php/security-policies/strategic-documents/100-national-security-strategy>

National Strategy on Countering Violent Extremism (2015) - <https://cve.gov.al/wp-content/uploads/2018/11/strategjia-2018-me-ndryshime.pdf>

Draft National Strategy on Cyber Security 2020-2025 -

<http://www.konsultimipublik.gov.al/Konsultime/Detaje/248>

Directive (EU) 2017/541/EU of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA -

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017L0541>

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data - <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680>

Terrorism Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JH – <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017L0541>

Commission Recommendation (EU) 2018/334 of 1 March 2018 ‘on measures to effectively tackle illegal content online’ - <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32018H0334>