

INSTITUTIONAL CAPACITIES OF NORTH MACEDONIA IN COUNTERING ONLINE EXTREMISM

NEEDS ASSESSMENT REPORT

METODI HADZI JANEV
SAMET SHABANI

HORIZON CIVITAS
CILC Center for International Legal Cooperation
Netherlands - North Macedonia Counterterrorism Platform
Kingdom of the Netherlands

COUNTERTERRORISM PLATFORM II

NEEDS ASSESSMENT REPORT

INSTITUTIONAL CAPACITIES OF NORTH MACEDONIA IN COUNTERING ONLINE EXTREMISM

Netherlands - North Macedonia
Counterterrorism Platform

July, 2025

Title: Needs assessment report on institutional capacities of North Macedonia in countering online extremism

Authors: Metodi Hadzi Janev and Samet Shabani

Graphic design and translation: BB Consulting

Format: Electronic only

Circulation: ~20 stakeholders

Access: open to public

The report has been made as part of the project "DELETE: disrupting Extremism Lines Effectively Through Engagement" as an integrated initiative under the project "Netherlands-North Macedonia Counterterrorism Platform II" implemented by the Center for International Legal Cooperation (CILC) in cooperation with Horizon Civitas.

The project is funded by the Ministry of Foreign Affairs of the Netherlands. The opinions and content are the sole responsibility of the authors and do not necessarily reflect the views of the donor or the other implementing partners.

HORIZON CIVITAS

CILC Center for International Legal Cooperation

Netherlands - North Macedonia Counterterrorism Platform

Kingdom of the Netherlands

Table of Contents

Accronyms and abbreviations 5

List of appendicies 6

Introduction and Background 7

Methodology 11

The Challenge of Online Radicalization and Extremism: North Macedonia in Context 13

Overview of the Macedonian policies and legislation to address online radicalization and extremism 19

Overview of the Macedonian institutional capacities in addressing and countering online radicalization and extremism 30

Recommendations 41

Appendices 44

Acronyms and Abbreviations

ACRONYM	DESCRIPTION
AYS	Agency for Youth and Sport
BPPOPOCC	Basic Public Prosecutor's Office for Prosecuting Organised Crime and Corruption
CATs	Community Action Teams
CILC	Center for International Legal Cooperation
CMC	Crisis Management Center
CRCCG	Commission for Relations with Religious Communities and Groups
CT	Counter Terrorism
CVE	Countering Violent Extremism
EU	European Union
FATF	Financial Action Task Force
GCTF	Global Counter Terrorism Forum
IA	Intelligence Agency
ICT	Information and Communication Technology
LCP	Local Council for Prevention
MFA	Ministry of Foreign Affairs
MoE	Ministry of Education
MOI	Ministry of Interior
MoJ	Ministry of Justice
MoU	Memorandum of Understanding
NATO	North Atlantic Treaty Organization

Acronyms and Abbreviations

ACRONYM	DESCRIPTION
NCCVECT	National Committee for Countering Violent Extremism and Counter Terrorism
NSA	National Security Agency
OSCE	Organization for Security and Cooperation in Europe
S-CTVE&R	Sector for Combating Terrorism, Violent Extremism and Radicalism
TCO	Terrorist Content Online
UN	United Nations

List of appendices

	DESCRIPTION	PAGE
Appendix A	Identifying Needs Assessment Stakeholders	44
Appendix B	List of Reviewed Documents	45
Appendix C	Interview Guide	46
Appendix D	Activity Reports	49

Introduction

From December 2024 to May 2025, a six-month needs assessment report was conducted on North Macedonia's institutional framework and capacities for countering online extremism. This in-depth analysis, part of the project, involved various interviews, desktop research and field observations to support the development of strategies against terrorism and online extremism.

The purpose of the needs assessment was to map the current state of play, challenges and recommendations for implementation of this measure in Macedonia. The assessment sought to identify key gaps related to the implementation of the measure in the country, as well as provide a baseline study for a possible implementation in the near future, respectively. As such, the report constitutes a credible source for institutions in drafting policy analysis and implementation of regulations related to addressing the online extremism. These measures are indicated for achieving the specific objective 1.4.4 Establishment of Unit for International Cooperation and searching on the Internet (in order to monitor radicalization to violence and violent extremism on the Internet) in scope of the **Action Plan on CVE (2023-2027)** of the Government of Republic of Macedonia. Accordingly, the report and overall, the scope of the project are a direct intervention to accomplish 1.4.5 Trainings for conducting Internet investigations concerning the publication of violent extremist content on the Internet, i.e. through social media, creating false profiles for monitoring Internet content with appropriate software solutions, from the abovementioned Action Plan, respectively.

This section of the report provides a brief overview about the countering online extremism and project intervention rationale, as well as current state of play in Macedonia for implementation of such measure, respectively. Section 2 details the methodology used in the assessment, presents the framework and key research questions for the assessment and highlights limitations to the research. Section 3 reports the primary findings of the assessment. We have categorized findings by the assessment's research questions including: (1) general setting on online extremism, (2) Institutional applicability or framework and (3) content and implementation by institution. Each is followed by the findings that address the question, set off with separate thematic sections. Each thematic section is followed by a discussion of the data supporting it. The report concludes with Section 4, which offers an articulated set of recommendations from stakeholders followed by summative conclusions. This report also includes the following for appendixes: Appendix A: Identifying Needs Assessment Stakeholders, Appendix B: List of Reviewed Documents, Appendix C: Interview Guide, Appendix D: Activity reports.

Context

According to the Action Plan on CVE (2023-2027) - 1.4.4 Establishment of Unit for International Cooperation and searching on the Internet (in order to monitor radicalization to violence and violent extremism on the Internet), this action is foreseen to be implemented in 2023-2024. The previous NCCVECT office prioritized this action and initial kick-off measures to establish the unit were taken. However, there was not any other significant measure taken afterwards, that would relate their strengthening of institutional measures and capacities.

The "Netherlands - North Macedonia Counterrorism Platform II" and its integrated initiative "DELETE: Disrupting Extremism Lines Through Engagement" aimed to address this gap by offering set of capacity building activities to the relevant public institutions. The project is a direct intervention to accomplish the 1.4.5 Trainings for conducting Internet investigations concerning the publication of violent extremist content on the Internet, i.e. through social media, creating false profiles for monitoring Internet content with appropriate software solutions.

Hereby, the project offered a variety of activities that supported institutional efforts in setting policies on countering online extremism, as follows:



Needs assessment mission

The mission, held in December 2023 aimed to identify priorities for future cooperation between institutions of Netherlands and North Macedonia, as well as to guide the development of the activities included under the project. Key meetings were held with security and justice institutions, including the NCCVECT. Identified needs included enhanced tools and training for online investigations, evidence handling, preparedness for returning foreign terrorist fighters, preventing online radicalisation and stronger international cooperation.

Accordingly, the project team held several coordination meetings throughout the project period to define all related details about upcoming activities.

The project team requested the National Committee for Countering Violent Extremism and Counter Terrorism (NCCVECT) to establish a Working Group on Countering Online Radicalization (WG) that will be the very target group of this project for the upcoming activities. HC and CILC worked closely with this WG in building their capacities and assisting them in actions/measures that are needed to be taken.



Study Visit

Organized study and work visit for the WG in the Hague, Netherlands. The goal of the study visit was to provide the WG with Dutch institutional knowledge and experience in countering online radicalization.

Moreover, it consisted a working meeting with EUROPOL, Eurojust and Dutch institutions to establish international cooperation for sharing the detected online radical content shared in both countries (North Macedonia and Netherlands) but in local languages used in North Macedonia (Albanian, Macedonian and Turkish).

National Forum: Religion and Online Challenges

In cooperation with the Commission for Relations with Religious Communities and Groups (CRRCG), a one-day event brought together religious leaders, young theologians, communication experts, and representatives from public institutions, academia, and civil society. The discussion focused on empowering religious communities to combat online radicalization, hate speech, and discrimination. The event also aimed to foster positive narratives, interfaith cooperation, and societal cohesion in the digital realm.

Expert debate: Online extremism and human rights

This one-day event gathered stakeholders from public institutions, academia, and CSOs specializing in countering violent extremism, terrorism, and human rights. They discussed how North Macedonia's legal framework could be adjusted to limit online terrorist and extremist content while safeguarding human rights like freedom of expression, personal data protection, and privacy.

Workshop on legislative adjustment in countering TCO

The workshop aimed to support the development of legislation in North Macedonia aligned with the EU Regulation (2021/784) on countering terrorist content online (TCO). It sought to mobilize public institutions to propose amendments to the national legal framework to limit the spread of terrorist and extremist content online while protecting human rights, including freedom of expression, data protection, and privacy. The activity focused on fostering a balanced approach to countering online extremism through expert discussions and collaborative drafting of a regulatory framework.

Trainings (2) by Dutch Police Academy

- **Training OSINT and online investigation**
- **Training on Preventing radicalization for first line professionals (multidisciplinary)**

The trainings provided by the Dutch Police Academy aimed to provide members of the National committee for countering violent extremism and counter-terrorism from North Macedonia insights into how the Netherlands and EU member states address counter terrorism and violent extremism, including the early detection of terrorist content online.

The sessions focused on the definition of how to monitor and address terror-related online activity as well as mechanisms that make such monitoring and early detection possible, including the Dutch so-called “soft approach”. Additionally, the sessions facilitated exchanges and supported the strengthening of cooperation among relevant authorities and representatives from local institutions.

with recommendations for countering TCO

Considering this background, a needs assessment of existing needs was deemed necessary to identify best mechanisms for possible applicability of Regulation on countering terrorist content online as a measure in the process of EU legal adjustments in the country. To guide the study, Horizon Civitas initiated a small research team, which developed a needs assessment framework including data collection and analysis activities. The body of the framework includes a set of research questions based on the purpose driving the study.

The research team used the research questions to organize the needs assessment framework and develop data collection questions and measures. The team assembled the measures into the appropriate data collection and analysis instruments, including an analytical coding structure to guide the desk review (and later, analyze the other qualitative data), a printed questionnaire to be used for in-face interviewing, a web-based version of the same questionnaire to be used when in-face interviewing is not possible, and integrated Activity Reports that contains solid recommendations for further policies that regards online extremism.



7 activities
within 6 months period



128 participants
built capacities



1 policy paper
roadmap for EU standards

Methodology

In this section, we describe the methodology used in the assessment, present the framework and key research questions and highlight limitations to the research. The needs assessment involved six primary steps: (1) desk review consisting of collection, coding and analysis of documents identified by Horizon Civitas and supplemented by the research team ; (2) development of a tool for the identification of stakeholders to include in the needs assessment; (3) interviews with identified stakeholders in-person and online ; (4) observation notes and activity reports coming out of the project itself ; (5) analysis and triangulation of all data sources using a structured coding scheme to develop findings and initial recommendations; (6) presentation and correction/validation of study findings and recommendations at a stakeholders workshop.



Desk Review

The desk review includes institutional documents and research about online extremism in Macedonia. The research team identified a set of documents and reports to consider for inclusion in the desk review.
In total, 24 were identified. Of these, the team reviewed, supplemented and ultimately included 17 key study documents (Appendix B: List of Desk Review Documents). The documents provided basic context for further elaboration of the topic.



Stakeholder identification

The research team developed Framework Tool for Identifying Needs Assessment Stakeholders (Appendix A: Identifying Needs Assessment Stakeholders) to support Horizon Civitas in identifying and engaging stakeholders in the needs assessment.
The tool sought to help Horizon Civitas identify a robust, relevant set of stakeholders to involve in the needs assessment. Based on their contextuality with the topic, stakeholders were grouped as primary purpose, affiliation, and funding.



In-depth stakeholder interviews

The views and perspectives of stakeholders constituted the pivotal component of the needs assessment. In order to gain detailed and nuanced insight into the current situation and needs, the research team conducted in-person and online interviews with a range of key stakeholders. The list of informants and respondents was developed by Horizon Civitas staff and research expert. Using the study research questions, the research team developed a set of questions to use as a basis for developing a semi-structured interview guide. In total, 10 interviews with identified stakeholders were conducted. Out of those, 4 were conducted in-person and 6 were responded to online.

Data Analysis

The research team analyzed qualitative study data (documents and interviews) first by developing topic-specific codes based on study research questions. The coding helped the team to determine the most frequent themes, patterns and answers and accordingly develop a set of concrete findings. Finally, this process allowed the team to aggregate across findings to develop a set of recommendations on how to best put online extremism in practice.

Limitations of the needs assessment report

This needs assessment, while informative, faced several limitations, some identified early on. These limitations are important to consider when interpreting the findings:

Data Reliance:

- Stakeholder-centric: The study heavily relied on the perceptions and views of stakeholders, leading to subjective insights into online extremism. While their input was valuable, it doesn't represent an objective analysis of the entire landscape.
- Limited Literature Review: Although external research was considered, it wasn't a comprehensive review, potentially missing broader perspectives.

Sampling and Generalizability:

- Convenience Sampling: Interview participants were readily available individuals, not randomly selected. This limits the findings' applicability to larger populations.
- Varying Data Availability: Both desk review materials and interview informants differed in accessibility across the country, potentially skewing the data.

Recommendation Structure:

- Unsorted Recommendations: Stakeholders largely refrained from categorizing recommendations by immediate, interim, and long-term goals. This makes prioritizing future actions more challenging.

Potential Biases:

- Self-Selection Bias: Participants who volunteered may hold strong opinions about the subject than those who didn't, influencing the data.

Despite these limitations, the study effectively combined qualitative and quantitative data triangulation to generate valuable insights into countering online extremism resources, gaps, and needs. However, interpreting and applying these findings should be done with these limitations in mind.

The Challenge of Online Radicalization and Extremism: North Macedonia in Context

Brief overview of the global trends and Online Radicalization

The digital revolution has transformed the way individuals communicate, access information, and form social networks. While this transformation has brought numerous benefits, it has also created opportunities for extremist groups to exploit online spaces for radicalization, recruitment, and propaganda dissemination. Online violent radicalization refers to the process by which individuals are exposed to extremist ideologies and gradually adopt violent beliefs, often leading to engagement in extremist activities or acts of terrorism.[1]

Extremist groups leverage the internet—particularly social media platforms, encrypted messaging apps, and online forums—to target vulnerable individuals, spread their narratives, and mobilize support. The anonymity of the digital space, coupled with the ability to reach a global audience, makes online radicalization a significant security challenge. Key drivers of this phenomenon include ideological indoctrination, grievances related to social or political conditions, identity crises, and the influence of extremist networks that operate across borders.

Digital dual-use technologies have become instrumental in the spread of disinformation, which in turn fuels online radicalization and extremism. Technologies such as artificial intelligence (AI), deepfake manipulation, and automated bot networks enable malicious actors to manufacture and amplify extremist narratives with unprecedented speed and precision. AI-generated deepfakes allow extremists to fabricate false speeches, doctored videos, and misleading images, making it easier to spread conspiracy theories, diminish certain groups, and incite violence. Automated bots and troll farms systematically disseminate extremist content, flooding social media platforms with propaganda designed to radicalize individuals by exploiting existing grievances, social divisions, and ideological conflicts.

[1] Online radicalisation is a complex and evolving concept, and there isn't a universally agreed-upon definition. However, it generally refers to the process by which individuals are exposed to extremist ideologies and beliefs through online platforms, leading to changes in their cognitive and/or behavioral patterns.
Please see more on this in: Alexander Meleagrou-Hitchens and Nick Kaderbha, (2017), "Research Perspectives On Online Radicalisation A Literature Review, 2006–2016", VOX-Pol Network of Excellence, 2017, available at: DCUJ4985_Lit_Review_020517_web.indd; Also see: Rosie Mutton, James Lewis, Sarah Marsden, (July 2023), CREST newsletter, available at: Online Radicalisation: A Rapid Review of the Literature

The viral nature of disinformation ensures that extremist messages reach wide audiences before fact-checkers or platform moderators can intervene, reinforcing echo chambers that isolate individuals from counter-narratives and alternative viewpoints.

Furthermore, encryption, decentralized communication platforms, and blockchain-based content hosting make it difficult for authorities to trace the origin of radicalizing content and disrupt extremist networks. Encrypted messaging apps like Telegram and WhatsApp serve as safe havens for radical groups to coordinate, recruit, and share extremist materials without exposure to counterterrorism efforts. Additionally, blockchain technology allows extremists to store and distribute propaganda in a tamper-proof and censorship-resistant manner, preventing the removal of radical content even when detected by authorities. These technologies also enable covert fundraising and financial transactions through cryptocurrency, allowing extremist organizations to sustain their operations anonymously. The combination of disinformation, radicalization, and the protective shield of dual-use technologies makes countering online extremism increasingly challenging, requiring adaptive regulatory measures, enhanced digital literacy, and collaborative counter-disinformation efforts to mitigate the risks.

As a result, governments worldwide have struggled to balance security measures with fundamental rights such as freedom of speech and privacy while countering online extremism. Efforts include enhanced cyber monitoring, legal frameworks for online hate speech, content moderation policies, and counter-narrative campaigns to counteract extremist propaganda. However, the rapidly evolving nature of online radicalization, combined with the decentralized structure of extremist movements, continues to pose a complex and persistent threat.

Online Radicalization and Extremism in North Macedonia

North Macedonia is not immune to the global threat of online radicalization. The country has faced challenges related to the spread of extremist ideologies, the recruitment of foreign fighters, and the use of digital platforms to incite violence. While North Macedonia has taken significant steps to counter violent extremism (CVE), the online dimension of radicalization remains a growing concern, particularly among youth and vulnerable communities. Several factors contribute to the online radicalization problem in North Macedonia:

Legacy of regional conflicts and transnational influences amid increased geopolitical competition

The Western Balkans, including North Macedonia, has been a target for radical networks, particularly those affiliated with Islamist extremism and far-right nationalist movements. The return of foreign fighters from conflict zones has raised concerns about online extremist networks operating within the country, using digital platforms to spread radical ideologies. Additionally, regional instability and political polarization create an environment where extremist rhetoric can thrive online.

Moreover, the increasing geopolitical competition between global and regional powers has further exacerbated vulnerabilities to radicalization and online extremism. The strategic positioning of the Balkans has made it a contested space for influence, with major actors—including the European Union, the United States, Russia, China, and Turkey—pursuing competing political, economic, and ideological agendas. This competition is often accompanied by targeted information campaigns, disinformation efforts, and narratives that exploit existing ethnic, religious, and political divisions. External actors, whether state or non-state, have sought to leverage radical discourse to destabilize the region, weaken democratic institutions, and challenge Western integration efforts. These dynamics not only create fertile ground for extremist ideologies to gain traction but also complicate counter-extremism efforts, as different political factions within the country may be influenced by external actors with conflicting interests.

[1] Online radicalisation is a complex and evolving concept, and there isn't a universally agreed-upon definition.
However, it generally refers to the process by which individuals are exposed to extremist ideologies and beliefs through online platforms, leading to changes in their cognitive and/or behavioral patterns.
Please see more on this in: Alexander Meleagrou-Hitchens and Nick Kaderbha, (2017), "Research Perspectives On Online Radicalisation A Literature Review, 2006–2016", VOX-Pol Network of Excellence, 2017, available at: DCUJ4985_Lit_Review_020517_web.indd; Also see: Rosie Mutton, James Lewis, Sarah Marsden, (July 2023), CREST newsletter, available at: Online Radicalisation: A Rapid Review of the Literature

Transitional challenges: Governance, Corruption, and Organized Crime

Beyond the direct drivers of online radicalization, North Macedonia's governance and institutional challenges also play a crucial role in shaping the security landscape. The country faces structural weaknesses that make its institutions vulnerable to exploitation by extremist actors, particularly in the digital space. Governance and institutional weaknesses, corruption and political clientelism, ethnic challenges and politicization of the public sector and the growing nexus between organized crime and extremism are structural illnesses that facilitate transnational extremist practices to target vulnerable individuals and groups in North Macedonia across the religious, ethnic and political/ideological spectrum.

The transition from post-socialist governance to democratic rule has been accompanied by significant challenges in institutional capacity, legal enforcement, and policy implementation. Weak governance structures hinder the effectiveness of counter-radicalization policies, as agencies responsible for addressing extremism often struggle with overlapping mandates, resource constraints, and bureaucratic inefficiencies.

Corruption remains a persistent issue in North Macedonia, undermining public trust in government institutions and security agencies. When citizens perceive state institutions as ineffective or biased, they may turn to alternative networks, including radical groups, for support and a sense of belonging. Political clientelism, where public sector jobs and positions are distributed based on political loyalty rather than merit, weakens institutional independence, leading to inconsistencies in the enforcement of counter-extremism measures. Undermining good governance translates into a lack of institutional capacities to detect and counter online extremism. While North Macedonia has established counterterrorism and CVE frameworks, the ability of institutions to effectively monitor, prevent, and counter online radicalization remains limited. Challenges include a lack of specialized training for law enforcement, gaps in legal frameworks for regulating extremist content online, and insufficient coordination between agencies responsible for cyber monitoring and security.

North Macedonia has long faced ethnic divisions between its Macedonian and Albanian populations, which have at times been exploited by radical actors to deepen societal fractures. Online extremist groups often use ethnic grievances as recruitment tools, portraying their causes as struggles for justice, identity, or political representation. Furthermore, the politicization of the public sector, where institutions are often aligned with specific ethnic or political interests, hampers the development of an impartial and effective counter-radicalization strategy.

Organized crime networks operating in the Western Balkans building on ethnic and religious proximity often intersect with extremist groups, facilitating activities such as illicit arms trafficking, financial crime, and smuggling of radicalized individuals across borders. The use of encrypted online platforms for illegal transactions, money laundering, and recruitment further complicates efforts to tackle radicalization. The absence of a strong, coordinated response between law enforcement, intelligence agencies, and cyber units enables criminal and extremist groups to exploit institutional weaknesses.

Use of social media and encrypted platforms

Extremist groups exploit social media, messaging apps, and online forums to spread their narratives. Platforms such as Facebook, Telegram, YouTube, and TikTok have been identified as primary channels for disseminating extremist content, radical propaganda, and conspiracy theories that fuel grievances and recruitment efforts. Encrypted platforms allow extremists to communicate and organize without immediate detection by law enforcement agencies.

Use of video gaming platforms and centers

The increasing prevalence of online video gaming platforms has introduced new avenues for social interaction, but also presented novel challenges, particularly concerning the potential for online radicalization. Accordingly, research by GNET highlights that "in recent years, online games have also been used to engage users and foster interest in the goals of radical groups with a view to their future recruitment".

Moreover, some reports and observations from the field in the country suggest that there are considerable number of unauthorized video gaming centers used as places to manifest radical preaches targeting youth. Namely, some of country's citizens charged with criminal acts related to violent extremism and terrorism (recruiting, logistical support, participating to foreign wars as members of terrorist organizations) were reported to own or co-own video gaming centers where recruitments and preaches to violence and radicalization were organized.

Misinformation, disinformation, and extremist narratives

Online radicalization in North Macedonia is closely linked to the spread of misinformation and disinformation, often in the form of fake news, conspiracy theories, and extremist propaganda. Some radical narratives exploit existing social divisions—whether ethnic, religious, or political—to sow discord and attract recruits. Disinformation campaigns, sometimes linked to foreign influence operations, further exacerbate these divisions by amplifying extremist content. Unlike state-led foreign influence operations, which tend to be more coordinated and strategic, online radicalization can emerge from both state and non-state actors, including loosely affiliated ideological networks, informal extremist groups, or lone actors. These actors frequently use disinformation as an entry point, exploiting grievances or identity-based tensions to draw individuals into more radical worldviews.

This distinction is important because not all radicalizing content online is the result of deliberate foreign influence. In many cases, it reflects organic but dangerous echo chambers, or ideologically motivated disinformation that is not tied to geopolitical strategy but still contributes to polarization and radicalization in society.[2]

Limited Public Awareness and Digital Resilience

Many individuals, particularly younger populations, lack the digital literacy skills needed to recognize extremist propaganda and resist radicalization efforts. There is a need for structured educational programs, awareness campaigns, and community engagement efforts to build resilience against online extremism. Schools, religious institutions, and civil society organizations play a crucial role in promoting critical thinking, digital responsibility, and counter-narratives to extremist ideologies.

Given the complexities of online radicalization in North Macedonia, a comprehensive needs assessment is necessary to evaluate the existing capacities, gaps, and institutional responses. This report seeks to analyze the public sector's ability to detect, prevent, and respond to online radicalization, identify areas for capacity development, and recommend targeted interventions that enhance the country's resilience against extremist threats in the digital space.

By mapping the current legal, institutional, and technical capacities of North Macedonia's public sector and assessing the skills and competencies of key institutions, this needs assessment aims to provide a foundation for strategic investments, policy improvements, and training programs tailored to counter online radicalization effectively.

[2] In their study paper O'Hara & Stevens, found that Echo chambers fueled by misinformation may radicalize individuals without the need for state involvement. The authors highlight the complexity of attributing online radicalization solely to foreign actors. See in: David O'Hara, Kieron & Stevens, David. (2015). Echo Chambers and Online Radicalisation: Assessing the Internet's Role in Extremism. Policy & Internet, 7(4), 401–422. Similarly, in their research, Amarasingam & Argentino argue that: "Radicalization can begin with conspiracy theories and disinformation before individuals transition to more overtly extremist communities. This often occurs outside of state influence, driven by decentralized networks". see in: Amarasingam, Amarnath, & Argentino, Marc-André. (2020). The QAnon Conspiracy Theory: A Security Threat in the Making? CTC Sentinel, 13(7), 37–44.

Overview of the Macedonian policies and legislation to address online radicalization and extremism

The Republic of North Macedonia has made significant efforts to develop a legal and policy framework to counter violent extremism (CVE) and online radicalization, aligning its approach with international and regional obligations, including those of the United Nations (UN), the European Union (EU), NATO, and the OSCE. The country has adopted strategic documents, legislative measures, and institutional mechanisms to address these threats. However, gaps remain in enforcement, coordination, and technological capacities, particularly regarding the online dimension of radicalization.

The National Strategy for Countering Violent Extremism (CVE) 2023-2027

The 2023-2027 Strategy for Countering Violent Extremism is a continuation of the previous strategy, given the necessity for sustainable solutions and long-term interventions.[3] It represents a comprehensive framework aimed at addressing the challenges posed by violent extremism, including the critical aspect of online radicalization. This analysis evaluates the strategy's capacity to tackle online radicalization by examining its understanding of key concepts, legal and institutional frameworks, public sector competencies, integration of best practices, and the challenges and shortfalls.

Understanding of online radicalization and violent extremism

The strategy demonstrates a clear comprehension of online radicalization, recognizing it as a dynamic process where individuals may come to accept terrorist violence as legitimate, potentially leading to engagement in terrorism. This understanding aligns with definitions provided by organizations such as the OSCE, which describes violent extremism and radicalization leading to terrorism as a process where individuals accept terrorist violence as a possible, perhaps legitimate, course of action.[4]

[3] Government of the Republic of North Macedonia, "The National Strategy for Countering Violent Extremism (CVE) 2023-2027 available at: https://nccvect.gov.mk/?q=mk/node/44 and Action Plan for the implementation of the National Strategy for Countering Violent Extremism 2023-2027, available at: https://vlada.mk/sites/default/files/dokumenti/strategii/eng_action_plan_pcve_strategy_2023-2027.pdf

[4] OSCE, (August 2024), Perceptions, Views And Challenges Of Young People In North Macedonia Research On Youth And Security, available at: https://www.osce.org/files/f/documents/4/2/575137_2.pdf?

The strategy takes a whole-of-society approach, emphasizing prevention, intervention, and reintegration while strengthening institutional coordination among government agencies, civil society, and international partners. It highlights the role of digital platforms in radicalization processes and underscores the need to enhance cyber monitoring, counter-narratives, and interagency cooperation to tackle online extremism effectively.

Key aspects related to online radicalization include:
-Enhancing digital literacy and public awareness campaigns to build resilience against extremist propaganda.
-Strengthening legal frameworks and institutional capabilities for monitoring extremist content online.
-Improving inter-agency cooperation between cybersecurity bodies, law enforcement, and intelligence agencies.
Developing deradicalization and disengagement programs, particularly for individuals exposed to online extremist networks.

Legal, institutional, and technical capacities against online radicalization and extremism

The New Strategy continues to serve as a policy framework that facilitates and guides the national legal framework against violent extremism in general and online extremism in particular. Institutionally, through its action plan,[5] the strategy emphasizes a whole-of-society approach, promoting coordination among national and local governments, civil society organizations, and international partners. This approach is crucial for addressing the multifaceted nature of online radicalization. The strategy also highlights the need for technical capabilities to monitor and counter online extremist content, acknowledging the role of digital platforms in the spread of radical ideologies.(action plan).[6]

Skills and competencies for detection, accountability, and response

The strategy identifies the necessity for specialized training programs to enhance the skills of public sector employees in detecting and responding to online radicalization. This includes developing competencies in monitoring digital spaces, understanding online recruitment tactics, and implementing counter-narratives. The emphasis on capacity-building reflects an awareness of existing gaps and a commitment to empowering institutions to effectively address these threats.

[5] Action Plan for the implementation of the National Strategy for Countering Violent Extremism 2023-2027, available at: https://vlada.mk/sites/default/files/dokumenti/strategii/eng_action_plan_pcve_strategy_2023-2027.pdf

[6]Global Counter terrorism Forum, (2023), National-Local Cooperation (NLC) Toolkit. Available at: https://www.thegctf.org/Portals/1/GCTFNLCToolkit_EN.pdf

Integration of best practices and broader experiences

The strategy attempts to incorporate lessons learned from past challenges, as well as new threats posed by the evolving digital landscape. The strategy incorporates best practices from international experiences, adapting them to the local context. For instance, it references the Global Counterterrorism Forum's (GCTF) toolkit on strengthening national-local cooperation in preventing and countering violent extremism, which provides practical guidance for enhancing collaboration between different levels of government and communities. By aligning with such frameworks, the strategy ensures that interventions are informed by proven methodologies and tailored to North Macedonia's specific needs.[7]

Criminal Code: Anti-Terrorism Legislation and Hate Speech in the Context of Online Extremism

North Macedonia's Criminal Code[8] includes provisions that criminalize acts of terrorism, incitement to violence, recruitment for terrorist purposes, and the use of online platforms for extremist activities. Amendments have been made to address the foreign fighter phenomenon, particularly following the return of Macedonian nationals from conflict zones in Syria and Iraq.

Relevant articles include:

-Article 394-g: Criminalizes participation in foreign military, paramilitary, or terrorist groups, including recruitment and facilitation.

-Article 394-h: Addresses the financing of terrorism, including the use of online platforms to transfer funds for extremist activities.

-Article 394-b: Covers public incitement to terrorism, including the dissemination of extremist content online.

As hate speech online is a critical enabler of radicalization and online extremism in North Macedonia, particularly given the country's ethnopolitical divisions and history of regional conflicts it is important to assess the legislation in the context of online hate speech. Criminal responses to hate speech are most commonly justified on the grounds of public order or national security but can also be found within the framework of offenses protecting the state or in cases of war crimes and crimes against humanity. The Criminal Code of North Macedonia criminalizes hate speech, particularly when it incites violence, hatred, or discrimination against individuals or groups based on ethnicity, religion, or other protected characteristics.

[7] Ibid.

[8] Criminal Code ("Official Gazette of the Republic of North Macedonia" No./1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009, 51/2011, 135/2011, 185/2011, 142/2012, 166/2012, 55/2013, 82/2013, 14/2014, 27/2014, 28/2014, 41/2014, 115/2014, 132/2014, 160/2014, 199/2014, 196/2015, 226/2015, 97/2017, 248/2018 and no. 36/23

Article 319 (Incitement to Hatred, Discord, and Intolerance) criminalizes public incitement to violence or hatred based on national, ethnic, religious, or other forms of identity. It applies to both offline and online speech, including social media and digital platforms.[9]

Article 394-d (Cybercrime-Related Hate Speech) was introduced to address hate speech on digital platforms, this provision criminalizes the use of information and communication technology (ICT) to incite hatred, violence, or discrimination. It strengthens the legal basis for monitoring and prosecuting online extremist propaganda.

Article 407-a Approving or justifying genocide, crimes against humanity, or war crimes. It stipulates that whosoever publicly negates, roughly minimizes, approves and justifies the crimes stipulated in Articles 403 to 407, through information system shall be sentenced to imprisonment of one to five years. If the negation, minimizing, approval, or justification is performed with the intent to instigate hate, discrimination, or violence against a person or a group of persons due to their race, skin color, national, ethnic origin, religion or conviction, mental or bodily disability, sex, gender identity, sexual orientation and political beliefs, the offender shall be sentenced to imprisonment of at least four years.

Article 417 criminalizes racial or other discrimination through hate speech. Accordingly whoever spreads ideas about the superiority of one race over another, or who advocates racial hate, or instigates racial discrimination, shall be sentenced to imprisonment of six months to three years.

While North Macedonia's legal framework criminalizes online extremism and hate speech, enforcement remains a significant challenge due to jurisdictional limitations, technological constraints, and procedural hurdles faced by law enforcement. A major obstacle is that much of the extremist content is hosted on foreign platforms, such as Facebook, X, Telegram, and YouTube, which operate under different legal systems and content moderation policies. Law enforcement agencies often struggle to compel these platforms to remove content or provide user data, especially when companies are based in jurisdictions with stronger privacy protections or lax regulations on hate speech enforcement. Additionally, extremist actors increasingly use encrypted communication channels (such as Telegram, WhatsApp, and Signal), which prevent authorities from monitoring radical networks, tracking recruitment efforts, or obtaining digital evidence.

The formal legal framework for recognizing and sanctioning hate speech is diffuse (spanning across many articles), imprecise, and lacks a clear definition and scope for hate speech.[12] The conceptual ambiguities related to hate speech also affect the development of judicial practice.[13]

These challenges are further compounded by a lack of digital forensic expertise, insufficient cross-border cooperation, and procedural delays in filing accusations. In many cases, prosecutors face difficulties in proving the intent behind online hate speech, especially when content is subtly worded or framed as political expression, leading to low conviction rates and ineffective deterrence.

Strengthening law enforcement's cyber-investigative capacities, enhancing legal cooperation with tech companies, and improving judicial training on digital evidence are crucial steps in addressing these enforcement gaps.

Law on Prevention of Money Laundering and Terrorism Financing [14]

Recognizing the role of digital financial transactions in funding extremist activities, North Macedonia has introduced legal measures to prevent the financing of terrorism. The Law on Prevention of Money Laundering and Terrorism Financing aligns with Financial Action Task Force (FATF) standards and EU directives. It requires financial institutions to monitor transactions and report suspicious activities, including online donations that could be linked to radical groups.

Despite these measures, crypto-based financing and unregulated online transactions remain a loophole that extremist networks can exploit. Strengthening cross-border financial intelligence sharing and technical expertise in tracking online financial flows is a key challenge.

[12] White paper on the situation with hate speech in the Republic of Macedonia, October 13, 2015, Helsinki Committee for Human Rights of the Republic of Macedonia, p.11. available at: https://mhc.org.mk/en/publications-en/white-paper-on-the-situation-with-hate-speech-in-the-republic-of-macedonia/

[13] ECRI Report on "THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA", (fifth monitoring cycle), adopted on 18 March 2016, p.17, available at: https://rm.coe.int/fifth-report-on-the-former-yugoslav-republic-of-macedonia-macedonian-t/16808b590d

[14] The Law on Prevention of Money Laundering and Terrorism Financing, Official Gazette of the Republic of North Macedonia No.151/22

Civil and Administrative Law Provisions Against Online Extremism Through Hate Speech: Anti-Discrimination and Media Laws

The Law on Prevention and Protection Against Discrimination[15] (2020, amended 2022) was adopted after criticism[16] of the previous Law (2010).[17] The new provisions directly address the key shortcomings mentioned earlier, including dealing with hate speech. The new Law expands protection against hate speech in digital spaces and provides mechanisms for victims to file complaints with the Commission for Prevention and Protection Against Discrimination.

The Law on Audio and Audiovisual Media Services was enacted in 2013.[18] It prohibits the broadcasting of media content that encourages or spreads discrimination, intolerance, or hatred. In the initial version of the Law, this prohibition only covered discriminatory grounds such as race, gender, religion, or nationality. It regulates media outlets and broadcasters, ensuring that hate speech and extremist propaganda are not disseminated via TV, radio, or online media.

Cybersecurity, Counter-Disinformation and Digital Privacy Protection Policies & Legislation

Cybersecurity and online data protection are increasingly relevant in the fight against online radicalization, particularly in safeguarding children and youth from extremist exploitation.[19] As radical groups utilize digital platforms for recruitment, propaganda, and manipulation, weak cybersecurity measures and insufficient personal data protection leave young individuals vulnerable to online targeting. Extremist networks exploit social media algorithms, encrypted messaging apps, and online gaming platforms to spread radical narratives while leveraging data breaches, phishing attacks, and digital profiling to identify and manipulate susceptible individuals. In this context, strong cybersecurity policies and robust personal data protection regulations are essential to mitigate these risks.

[15] The Law on Prevention and Protection Against Discrimination (2020, amended 2022, available at: The Law

[16] ECRI Report on "THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA" (fifth monitoring cycle), adopted on 18 March 2016, p.11, available at https://rm.coe.int/fifth-report-on-the-former-yugoslav-republic-of-macedonia-macedonian-t/16808b590d

[17] Law on prevention and protection against discrimination (2010), available at: The Law on Prevention of Money Laundering and Terrorism Financing, Official Gazette of the Republic of North Macedonia No.151/22

[18] Law on Audio and Audiovisual Media services (as published in the Official Journal of Republic of Macedonia No.184 26.12.2013), available at: https://avmu.mk/wp-content/uploads/2017/05/Law_on_Audio_and_Audiovisual_Media_Services_as_published_in_Official_Journal.pdf

[19] According to EU The definition of the age at which someone is considered a 'child' varies depending on the underlying data source and policy needs. The maximum age can be up to 17 years. Young people are defined as being between 15 and 29 years old. Consequently, these 2 groups can sometimes overlap. Please see more at; EUROSTAT, available at: https://ec.europa.eu/eurostat/web/children-youth#:~:text=The%20maximum%20age%20can%20be,15%20and%2029%20years%20old

North Macedonia has sought to strengthen cyber resilience, among other things, by protecting user data, enhancing digital literacy, and strengthening online safety mechanisms, including countering false narratives. In this regard, several strategic policy documents and laws must be considered that directly or indirectly provide a policy and legal framework to counter online radicalization and extremism.

The First National Cybersecurity Strategy 2018-2022 and Action Plan 2018-2022 [20] laid the groundwork for institutional cooperation in monitoring digital threats. Nevertheless, for more than three years, the country functioned without a national cyber security strategy leaving a dramatic gap in our preparedness against developing threats. The lack of comprehensive legislation for cyber security will additionally make society vulnerable leaving institutions and citizens at risk.[21] The new 2025-2028 National Cyber Security Strategy provides a framework looking ahead to creating a safe digital future for every citizen, company and institution in the country.[22] Under the main priority (7. Cybersecurity resilient society) there are two specific priorities relevant to counter online extremism and radicalization 7.1. Raising cybersecurity awareness and against disinformation spread via cyberspace and 7.2. protection of children and youth on the internet. The strategy, nevertheless, does not specifically mention online radicalization and foreign influence operations.

National Strategy for Building Resilience and Countering Hybrid Threats 2021-2026. defines six areas of operational activities for countering hybrid threats.[24] Disinformation is mentioned in several of them. The strategy treats disinformation in a broader framework, as part of hybrid threats. This strategy focuses on:

-Enhancing media literacy and critical thinking to prevent susceptibility to extremist content.

-Developing technological solutions to detect and flag radical content online.

-Strengthening cooperation with tech companies to remove extremist content in line with EU regulations.

[20] National Cybersecurity Strategy 2018-2022 and Action Plan 2018-2022, December 2018, available at: https://sherloc.unodc.org/cld/uploads/res//treaties/strategies/macedonia_the_former_yugoslav_republic_of/mkd0002s_html/ap_cybersec_v1.13_eng.pdf

[21] MIA, (January 21, 2025), Cyber security strategy a turning point in country's digital transformation process: minister", available at: ECRI Report on "THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA" (fifth monitoring cycle), adopted on 18 March 2016, p.11, available at https://rm.coe.int/fifth-report-on-the-former-yugoslav-republic-of-macedonia-macedonian-t/16808b590d

[22] Ibid

[23] Ministry of Digital Transformation, January 2025, "National Cyber Security Strategy 2025-2028"

[24] National Strategy for building national resilience and coping with hybrid threats (2021), available at: https://mod.gov.mk/storage/2021/12/Nacionalna-Strategija-za-gradene-otpornost-i-spravuvane-so-hibridni-zakani-april-2021.pdf

The Macedonian legal framework for online privacy is compiled by the set of regulations that cover privacy online, including the Law on Personal Data Protection (aligned with the EU's GDPR)[25], The Law on Criminal Procedure,[26] and The Law on Electronic Communications.[27] A more detailed analysis on the matter is provided in the 2024 study on "Protecting Digital Privacy, Legal and Practice Analysis for North Macedonia and EU".[28]

An important aspect of countering online extremism from the perspectives of good governance and human rights in North Macedonia is the Law on Interception of Communications,[29] which regulates state surveillance and intelligence-gathering practices. While lawful interception is crucial for monitoring and preventing online radicalization, overreach, lack of transparency, or misuse of surveillance powers can fuel extremist narratives that exploit government overreach, perceived oppression, and restrictions on civil liberties. Radical groups often frame state surveillance, harsh counter-extremism measures, and political abuses as evidence of government repression, reinforcing grievances that contribute to online radicalization and recruitment. Ensuring that interception laws are implemented with clear oversight, judicial accountability, and human rights safeguards is essential to balancing security needs with democratic principles, preventing extremists from weaponizing government actions to legitimize their narratives.

[25] Law on Personal Data Protection ("Official Gazette of the Republic of North Macedonia" No. 42/20) and the Law on Amendments to the Law on Protection of Personal Data ("Official Gazette of the Republic of North Macedonia No. 294/21)

[26] Law on Criminal Procedure ("Official Gazette of the Republic of North Macedonia" No. 150/10, 100/12, 142/16 and 198/18)

[27] Law on Electronic Communications ("Official Gazette of the Republic of Macedonia" No. 39/2014), 188/2014, 44/2015, 193/2015, 11/2018 and 21/2018 and "Official Gazette of the Republic of North Macedonia" No. 98/2019 and 153/2019

[28] More on this issue see in - Ljubica Krtsevska & Metodi Hadji-Janev, (2024), "Protecting Digital Privacy, Legal and Practice analysis for North Macedonia and EU", American Bar Association, available at: here

[29] Law on Interception of Communications ("Official Gazette of the Republic of North Macedonia" No. 71/18)

Overview of other Governmental Policies relevant to Prevent and Counter Online Radicalization & Extremism

Since extremist groups use disinformation and propaganda to radicalize individuals online, Prevention of Violent Extremism and Counter-Terrorism (2023-2027) (2023), accompanied by Action Plans (AP) led by the NCCVECT (2024) allocate responsibilities in other governmental institutions.

The National Strategy for Countering Violent Extremism 2023-2027 and its accompanying Action Plan outline 60 sub-objectives, with 12 specifically dedicated to youth-focused interventions. These efforts aim to raise awareness, strengthen community resilience, and prevent online radicalization by engaging young people in proactive initiatives. The Agency for Youth and Sport (AYS) and the Local Council for Prevention (LCP) play a central role in these activities, with responsibilities outlined in the Action Plan.[30]

Their mandate includes the design and implementation of media and promotional campaigns that foster social cohesion and counter violent extremism narratives, as well as facilitating confidence-building dialogues to address underlying grievances that may contribute to radicalization. Additionally, these institutions are tasked with establishing and supporting Community Action Teams (CATs), which serve as grassroots mechanisms for early intervention and youth engagement. They also organize youth debates on topics related to social inclusion and sports, alongside dialogues with sports associations and fan groups to prevent radical influences in community spaces.[31]

Beyond direct outreach, the strategy emphasizes formal and non-formal education as a tool for building resilience against extremist narratives. It includes initiatives to develop online platforms dedicated to counter-narratives, ensuring that young people are exposed to alternative perspectives that challenge radical ideologies. A key component of the strategy is the creation of youth-led community centers, supported by state institutions, civil society organizations, and international partners, providing safe spaces for youth engagement and activism. These initiatives are elaborated further in Section 1.3.6 of the Action Plan, detailing specific programs and mechanisms for sustainable youth empowerment and radicalization prevention.[32]

[30] Action Plan for the implementation of the National Strategy for Countering Violent Extremism 2023-2027, available at: The Law on Prevention and Protection Against Discrimination (2020, amended 2022, available at: The Law and National Youth Strategy 2023 – 2027 and Action Plan 2023 – 2025, available at: The Law on Prevention and Protection Against Discrimination (2020, amended 2022, available at: The Law

[31] More on this see in the Pleiades, (2024), Mapping stakeholders in North Macedonia: Addressing violent extremism at central and local levels, available at: ECRI Report on "THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA" (fifth monitoring cycle), adopted on 18 March 2016, p.11, available at https://rm.coe.int/fifth-report-on-the-former-yugoslav-republic-of-macedonia-macedonian-t/16808b590d

[32] Ibid

The Ministry of Education (MoE) plays a direct role in the prevention process through the education system. Their activities are highlighted in the Action Plan of 2023-2027 with the following task: Developing a programe, training of trainers and trainings for teaching staff in preschool, primary and secondary education for early recognition of signs of radicalization to violence and violent extremism, Implementation of a programe for the legal socialization of Youth at the local and national level, active parenting workshops, implementation of a programme for (non-)formal education and vocational training of convicted persons (2023 – 2027).[33]

Institutional Implementation and Coordination: Operationalizing Policy and Legislation Against Online Extremism and Radicalization in North Macedonia

North Macedonia has established a robust policy and legislative framework to address online radicalization, but implementation remains the key challenge. Strengthening technical capacities, legal enforcement, inter-agency coordination, and international cooperation will be crucial in enhancing the country's resilience against online extremism. Moreover, a more proactive approach to counter-narratives, community engagement, and digital education is needed to address the root causes of radicalization and prevent its spread in the digital space.

Despite a comprehensive strategy, there is a clear gap between policy and enforcement. Bureaucratic inefficiencies, limited coordination, and resource constraints slow down implementation, especially in public sector bodies that lack expertise in digital threats. Legal reforms, including updates to the Criminal Code and counterterrorism laws, have improved the framework, but issues remain in defining extremist content without infringing on free speech and privacy. Public preparedness is another hurdle. Insufficient training programs and fragmented interagency efforts undermine early warning and rapid response systems. Moreover, while the policies and legislation emphasize public-private partnerships, North Macedonia struggles to influence global digital platforms in moderating harmful content.

There is also a lack of clear mechanisms to involve civil society and local communities—key players in countering extremist narratives. Additionally, the strategy does not fully account for the rapidly evolving nature of online extremism, leaving it vulnerable to emerging technologies and encrypted communication channels.

[33] Ibid

Macedonian legislation only vaguely addresses the implementation and regulation of transformative and dual-use digital technologies, despite their growing relevance in online radicalization and extremism. Technologies such as artificial intelligence (AI), deepfake manipulation, blockchain, and encrypted communication platforms can be exploited by extremist groups for propaganda dissemination, recruitment, and operational security. While laws on cybersecurity, personal data protection, and counterterrorism provide a general framework, they lack specific provisions for regulating AI-driven radicalization, the misuse of encrypted digital tools, or the risks posed by emerging technologies in extremist ecosystems. Without clear policies on dual-use digital technologies, North Macedonia faces challenges in effectively countering online extremism while ensuring responsible innovation and technological development.

In summary, while North Macedonia's policies set an important groundwork to combat online radicalization, bridging the gap between legislation and practice will require bolstered technical capabilities, better-trained personnel, enhanced interagency cooperation, and more dynamic, inclusive engagement with both civil society and global tech partners.

Overview of the Macedonian institutional capacities in addressing and countering online radicalization and extremism

General overview of the Macedonian institutional approach to prevent and counter online extremism

Given that violent extremism is no longer associated only with individual terrorist attacks, but also with conflicts that have caused tens of thousands of deaths and injuries, including those caused by right-wing extremists, the concept of CVE fosters closer cooperation and exchange between the security services and actors in the fields of conflict management and prevention relying heavily on the support of the local communities and civil society organizations. Abusing the internet and modern communication platforms by the malicious actors to violently radicalize vulnerable members of society has become a serious concern in the worldwide CVE efforts. The initial focus on internet abuse by non-state actors for political purposes was on how violent extremists have used the Internet and social media to plan and carry out their attacks. In recent years, however, growing attention has been given to how these spaces and platforms are used to inspire, radicalize and issue a 'call to action' to those vulnerable to extremist messages and narratives.

Although many forums (sponsored by UN, EU, OSCE, NATO, or through bilateral programs of cooperation) dedicated to online radicalization and CVE (in general) in North Macedonia recognized the need for a comprehensive CVE approach the practical institutionalization and operationalization of these recognition seems to be lagging. In fact, the first institutional effort of coherent CVE came only after The National Committee for Countering Violent Extremism and Counter-Terrorism (NCCVET) was established in 2017.[34] The Government's decision from 2017 stipulates that NCCVET will serve as a national coordinative body to monitor and analyze the situation pertaining to CVE and CT and coordinate activities of the relevant institutions working on addressing the phenomenon of violent extremism and acts of terrorism.[35]

[34] Government Decision on Establishment of NCCVET (Official Gazette of the Republic of North Macedonia No. 98/2017)

[35] Ibid

The late institutionalization of the concept of CVE in general and online radicalization, in particular, stems from two main reasons. First, speaking in the general CVE context, the discourse is a result of a sporadic, inadequate and neglected approach to the issue. Second, when it comes to online radicalization, the discourse rests on the general administration's bias i.e., that the internet and relevant information and communication technologies (ICT) are usually attributed as the IT personnel only area.[36]

Though narrative understanding among the political elites and relevant authorities has long recognized the importance of the comprehensive approach (a whole of the government and whole of society) for an effective CVE concept in reality there was no practical implementation of such an understanding. One reason for this could be that the process of CVE was mainly led by the security and intelligence sector personnel whose capacities in dealing with CVE were inherited by the old-school CT approaches. These approaches were predominantly based on punishment mechanisms and not on prevention. A deeper look into the personnel's skills and knowledge will confirm that most of the personnel developed their knowledge and skills about CT in the former system that was coined on a different government's role in society.[37]

On the other hand, the centralized government's mechanisms to control and lead the society (under which this personnel was trained) from a local to a federal level organized on top-down principles evaporated during the ill-managed transition. At the same time, the new democratically elected leadership grew up through the NGO sector as the only leading force in democracy capacity building lacked sufficient security (including wider geopolitical) awareness. As a result, the only functional part that could fit in and take the lead to CVE was personnel from the security and intelligence services.

The new concept introduced with the establishment of the NCCVET seems to be trying to change this. Accordingly, the NCCVET consists of the Ministry of the Interior; Ministry of Defense; Ministry of Justice; Directorate for Execution of Sanctions; Ministry of Foreign Affairs; Ministry of Local Self-Government; Ministry of Labor and Social Policy; Ministry of Education and Science; Ministry of Health; Ministry of Information Society and Administration; Ministry of Transport and Communications; Directorate for Financial Intelligence; Directorate for Financial Police; Customs Administration; The Intelligence Agency; The Basic Public Prosecutor's Office for Prosecuting Organized Crime and Corruption; Center for Crisis Management; Directorate for Protection and Rescue; Agency for Electronic Communications; Agency for Youth and Sports and the Commission for Relations with Religious Communities and Religious Groups.

[36] For example, with the establishment of sector for computer and electronic crime in the Ministry of interior digital forensic was separated from the general well developed and certified forensic unit, which reflects the thesis that IT community is seen as a "different package". Moreover, very similar conclusions were made by the team from Global Cyber Secirity Capacity Center led by professor Michael Goldsmith, in the Cybersecurity Capacity Review FYR Macedonia 2018, sponsored by the World Bank. See: Global Cyber Secirity Capacity Center, (2018), "the Cybersecurity Capacity Review FYR Macedonia 2018", World Bank, available at: https://mioa.gov.mk/sites/default/files/pbl_files/documents/reports/cmm_fyrom_report_final_13_august2018_2.pdf

[37] For example, the former national coordinator for CT Toni Jakimovski was a long term law enforcement officer coming from the intelligence sector (who actually worked at UBK- Directorate for Security and Counterintelligence sector. The previous two coordinators of NCCVECT were also with the law-enforcement intelligence background coming from the same sector.

Although theoretically well designed, in practice things seem to be different. For example, in the latest official plan to implement the "Program on national security against Terrorism", one of the success criteria for the program indicates "Raising citizens' awareness about CVE". Given that this is a rare institutional regulatory measure tackling this important avenue in CVE, where instead of enhancing CSO's capacities to take the lead, the measure reminds one to believe that this is inherited from the old-school top-down approach to the issue.[38] Therefore, the analysis of the institutional capacitates to CVE will take the top-down approach.

The challenge of insufficient capacities to address online radicalization echoes the general challenges associated with the institutional capacities for e-governance. For example, an independent evaluation of the cybersecurity capacities of the country, run by the World Bank and the Global Cyber Security Capacity Centre in 2018, asserted that "It was not possible to obtain a clear picture regarding crisis management…" in the course of cyber threats.[39] The Crisis Management Center (CMC) according to the Crisis Management Law is responsible for preventing risks and threats (where radicalization, extremism and terrorism are underlined as such) and managing the crisis from such threats.[40] Moreover, the evaluation found that "*The extent to which organizations consider cyber threats as part of crisis situations is uncertain. It is understood that general crisis management is necessary for national security, however, cybersecurity is not yet considered as a component*"….; "The cybersecurity culture is generally not very advanced and often users are not aware of the risks associated with the use of the Internet, the cybersecurity strategy overall awareness and readiness.[41]

The NCCVECT's capacities

According to the above-mentioned Government decision, the NCCVET is managed and represented by the National Coordinator for CVE, CT, and the two deputies. The vision with the establishment of the NCCVET was to enhance the whole of the government approach and the whole of the society approach (through coordination of the local government efforts as well as the role of civil society). Therefore, the NCCVET's role was to launch strategic coordination of the cross-sectoral cooperation, including cooperative planning and activities required to prevent, prosecute and respond to threats of radicalization that can lead to violent extremism and terrorism with the relevant stakeholders from the society. [42]

[38] National Committee for Countering Violent Extremism and Countering Terrorism (February 2018), "National Counterterrorism Strategy Of The Republic Of Macedonia (2018-2022)", Government of the Republic of Macedonia, Skopje, p. 30 and p.33, available at: https://wb-iisg.com/wp-content/uploads/bp-attachments/6135/ct_national_strategy_eng_translation_sbu.pdf

[39] Global Cyber Security Capacity Centre, (2018), "Cybersecurity Capacity Review, Former Yugoslav Republic of Macedonia (FYR Macedonia)", Wordl Bank, p.9 available at: https://mioa.gov.mk/sites/default/files/pbl_files/documents/reports/cmm_fyrom_report_final_13_august2018_2.pdf

[40] Article 3, p.2 and 5. From the Law on Crisis Management, Official gazette No.25, from May 4, 2005.

[41] World Bank & Global Cyber Security Capacity Centre, (2018)

[42] National Committee for Countering Violent Extremism and Countering Terrorism, 2018, "National Strategy Of The Republic Of Macedonia For Countering Violent Extremism (2018-2022)", Skopje, available at: Government of the Republic of Macedonia

Among others, the Committee drafts national strategies for CVE and CT, with appropriate action plans; coordinates and directs the activities of all entities involved in the implementation of plans arising from national strategies in this area; builds relations with representatives of civil society, local self-government, religious communities, experts and the academic community in order to define and implement appropriate measures for CVE and CT; monitors regional and global trends and communicates with relevant institutions and partners on a regional and international level; coordinates the process of conducting evaluations, analyses and research on the causes and emerging forms, but also new trends in recruiting terrorists; and coordinates the activities related to the implementation of national campaigns for preventing of violent extremism and radicalization that can lead to terrorism, and supposed to participate in organizing inclusive public debates, forums and seminars.

The National Coordinator and Deputy Coordinators of the NCCVET lack executive power and operate with limited budgets and resources. While such arrangements might be standard in more mature democracies, in the context of North Macedonia, this often results in the effectiveness of the NCCVET being contingent upon the personal relationship between the Coordinator and the Prime Minister. Consequently, implementation of decisions may depend more on political dynamics than institutional mandates. Since its establishment in 2017, many members of the NCCVET have remained under-resourced—both in terms of human capacity and operational tools—hindering their ability to effectively monitor, analyze, and coordinate sustainable efforts to prevent violent extremism.

A further structural challenge lies within the justice system. The judiciary and public prosecution, which represent critical components in addressing vulnerabilities that may lead to frustration and radicalization, remain largely disconnected from the overall framework of countering violent extremism (CVE), and even more so from the nuances of online radicalization and extremism. Their limited exposure and experience in these areas increase the likelihood of procedural missteps and missed opportunities for early intervention.[43] Moreover, to date, there is no centralized database or system for the geographical or typological mapping of identified extremists or potential radicalization hotspots—let alone any mechanism for tracking related online activities. Likewise, there is no publicly available evidence of structured capacity-building initiatives aimed at addressing this critical gap or supporting the development of early warning systems at the national level.An additional challenge is that there is no relevant evaluation mechanism, including independent studies that will analyze the overall CVE concept, measure the effectiveness of the NCCVET and the performance of relevant stakeholders in the North Macedonian strategic concept of CVE, including online radicalization.

[43] See for example an observation of the US State Department on the issue: Academic (July 20, 2017), "Стејт департмент: Во Македонија не постои посебна национална стратегија за спречување на насилниот екстремизам", available at: https://akademik.mk/stejt-department-vo-makedonija-ne-postoi-posebna-natsionalna-strategija-za-sprechuvane-na-nasilniot-ekstremizam/

Ministry of Interior

The Ministry of Interior is responsible for public security and state security as a part of national security.[44] Addressing modern security threats including, terrorism and violent extremism as implied tasks from the public and state security responsibilities were first prescribed with the Strategic Plan of the Ministry of Interior 2018-2020.[45] However, The Sector for Combating Terrorism, Violent Extremism and Radicalism (S-CTVE&R) within the Department for Suppression of Organized and Serious Crime specializes in CVE. Today the MOI is responsible for monitoring extremist activities, online investigations, and law enforcement interventions. While the general CVE approach in recent years has marked some progress, there are no publicly available protocols for a systematic approach to online radicalization and extremism.[46] For example, according to the official MOI strategic plan (2019-2021), 3000 law enforcement officers accomplished training on radicalization (not specifically mentioning online radicalization) as an important segment of the CVE.[47] The same document also provides general evidence about capacity-building measures among law enforcement officers throughout different forms of cooperation dedicated to strengthening CVE without mentioning online radicalization and extremism specifically.[48] The same document indicates that one of the strategic priorities in CVE (without specifying online radicalization) would be "Prevention, profiling, processing, protection and suppression of terrorism, extremism detection of all unconstitutional activities related to terrorism and extremism as well as strengthening the measures against financing related with these negative trends.[49] In this line the Ministry also works on establishing local prevention councils, units for international cooperation, and online monitoring to counter radicalization, while enhancing inter-agency collaboration to prevent radicalization in public and correctional facilities.

From the publicly available evidence, it seems that enhancing capacities for preventing/countering online radicalization and extremism has not received the required parallel attention as in the physical general CVE measures.[50]

[44] Law on internal affairs (Official Gazette No. 42/2014, 116/2014, 33/2015), available at: http://www.mvr.gov.mk/Upload/Documents/ZVR%20nov%20precisten%20 05.03.15.pdf

[45] Strategic plan of the Ministry of Interior 2018-2020, available online: https:// mvr.gov.mk/Upload/Editor_Upload/%D0%A1%D0%9F-2018-2020-%D0%B7%D0%B0%D1%81%D0%B0%D1%98%D1%82(1).pdf

[46] According to internal administrative structural description of jobs (systematization of working positions) in the sector for internal affairs, as well as in the police stations and units, provides the basis for carrying out preventive activities related to violent extremism by the police officers at the local level. Each police station at the level of sector has three inspectors for prevention: for public order and peace, for traffic and for criminal matters. Moreover, the project "Community Policing in the Function of Prevention of Radicalization and Violent Extremism" with the support of the OSCE Mission to Skopje. See in: Bornarova Suzana and Bogoevska Natasha (2018), Report on mapping of the institutional capacities for prevention of violent extremism, IOM

[47] Ministry of Internal Affairs, (February 2019), "Strategic Plan" (Original: Стратешки план), p. 20, available at: https://mvr.gov.mk/Upload/Editor_Upload/STRATESKI%20PLAN%202020-2022(1).pdf

[48] Ibid, see at p. 41 for example

[49] Ibid, Strategic priorities under 3 at p. 41

[50] During 2018 the Ministry of Interior started the implementation of the project on introduction of neighborhood constable or police officer in Kumanovo, as a part of the community policing. See more at: Bornarova Suzana and Bogoevska Natasha (2018), Report on mapping of the institutional capacities for prevention of violent extremism, IOM

The only information related to building capacities for online extremism available is that Under the Action Plan, the MOI focuses on training police officers and cadets, strengthening private security agencies, and promoting initiatives like the "Red Button".[51] Instead of addressing online radicalization and extremism is a split work between the (S-CTVE&R) within the Department for Suppression of Organized and Serious Crime and the Sector for Computer Crime.

Intelligence Agency and National Security Agency

According to the law of intelligence agency, IA is responsible for collecting, processing, analyzing, and safeguarding data pertinent to the security, defense, foreign policy, and economic interests of North Macedonia, including issues related to terrorism and violent extremism from political, ethnic, and religious perspectives.[52] From its publicly available activities, it seems that IA does not specialize in online extremism & radicalization. Instead, the Agency is focusing on “terrorism and violent extremism from a political, ethnic and religious aspect”, and “cyber threats”.[53]

According to the Law on National Security Agency – NSA is responsible for collecting, process, analyzing, evaluating, exchanging, storing and protecting data and information in order to detect and prevent activities related to security threats and risks to the national security of the state among others from terrorism & financing of terrorism, violent extremism.[54] There is no specific provision that allocates responsibilities for online extremism and radicalization.

According to the IA Action Plan for 2024, the IA and ANS are engaged only under one task, continuous specialized training for its personnel to strengthen their capacity to respond to violent extremism and radicalization leading to terrorism.[55]

[51] “Red Buton” is an app which is intended for reporting any knowledge or information in the field of child abuse https://www.mvr.gov.mk/Upload/Editor_Upload/Godisen%20MVR%20javna%20verzija1.pdf

[52] Law on the Intelligence Agency Official Gazette of the Republic of Macedonia, No. 21 of 27.1.2021

[53] IA, The Agency conducts intelligence activities in order to identify external threats , available at: https://ia.gov.mk/index_en.html

[54] The Law on National Security Agency, Official Gazette of the Republic of North Macedonia, 2019, art.4

[55] IA. (2024). Activities. Retrieved from Intelligence Agency: https://ia.gov.mk/index_en.html

Ministry of Justice - MOJ

The Ministry of Justice plays an important role in the overall CVE and online radicalization. National Criminal Courts and Basic Public Prosecutor's Office For Prosecuting Organized Crime And Corruption are two directly involved crucial institutions for the overall CVE and online radicalization success. There is no section, or sector inside of the national justice system designated to address extremism, terrorism, or online radicalization and extremism-related issues-cases.[56] Inside the national criminal court's system, there are no specially designated sections to decide on legal cases related to violent extremism, terrorism and online radicalization& extremism.[57] However, the Basic Public Prosecutor's Office for Prosecuting Organised Crime and Corruption (BPPOPOCC), from a department for prosecuting organized crime and corruption, is responsible forfiling cases whenever there is reasonable doubt about: Terrorists endangering the constitution and security (Art 313); Participation in the foreign military police, paramilitary and para-police formation (Art 322-a); Assembling for enemy purposes against the state (Art 324); Terrorist organization (Art 394-a); Terrorism (Art 394 – b); and Financing of terrorism (Art. 394-v-Cyrillic).[58]

MOJ has addressed several high-profile cases related to CVE (not to online radicalization). The most prominent case, in which 11 persons were sent to jail in 2016, codenamed "Cell", concerned a group found guilty of recruiting people to fight in Iraq and Syria and of participation in foreign paramilitary forces. The BPPOPOCC has also filed charges against another eight persons "for participation in foreign paramilitary structures". This was the first such case after the criminal code updates in 2014 (to include jail sentences for participation in foreign military conflicts). Apart from dealing with returnees from armed conflicts, several domestic high-profile cases have also turned attention.

One of these cases is the Kumanovo shootout – known as the "Kumanovo case". The BPPOPOCC filed charges for terrorism against 37 suspected involved in the shoot against the police. The court found 33 of the 37 defendants guilty for terrorism and sentenced them to a total of 736 years in prison. Four suspects were acquitted. Seven of the defendants got life sentences.

[56] See Ministry Of Justice of the R. of N. Macedonia, available at: https://www.pravda.gov.mk/sudovi

[57] Ibid

[58] All of the articles are from the National Criminal Law (Official Gazette of the Republic of North Macedonia, No 42, from 16.2.2020 (Originally: "Службен весник на РСМ, бр. 42 од 16.2.2020 година")

Another high-profile case for the mass murdering near Lake Smilkovo in 2012 has been highly politicized[59] and has caused up some grievances and ethnic tensions and according to some provoked the rise of right-wing extremism.[60] Similarly, the case of the infamous mob attack on parliament in 2017, resulted in terrorist charges and has also been highly politicized [61] which unequivocally raises serious concerns about the MOJ's impartiality.[62]

Up to date, there are no publicly available documents by the criminal courts, BPPOPOCC, or the MOJ to specifically address online CVE and radicalization. Though there are well-developed strategic documents addressing relevant sectors that need improvement aligned with appropriate programs, there is nothing that mentions radicalization, extremism or terrorism.[63] Moreover, the MOJ rightfully recognized the necessity to introduce ICT in the judiciary system and public prosecution offices. However, there is nothing that addresses online extremism and radicalization.[64]

The Academy for Prosecutors and Jurists operates under the MOJ. Although according to the website of the Academy, it looks like there is a developed program tailored to build proper human capacities for the judiciary system there are no specific documents dedicated to CVE and online radicalization.[65] Hence, except for sporadic foreign-sponsored activities (forums, workshops conferences, training and etc.), it seems that there are no specifically tailored-based programs for capacity building in terms of CVE and online radicalization. Therefore, the thesis that the MOJ is disconnected from the overall CVE concept seems to be correct.

[56] See Ministry Of Justice of the R. of N. Macedonia, available at: https://www.pravda.gov.mk/sudovi

[57] Ibid

[58] All of the articles are from the National Criminal Law (Official Gazette of the Republic of North Macedonia, No 42, from 16.2.2020 (Originally: "Службен весник на РСМ, бр. 42 од 16.2.2020 година")

[59] Makfaks, (April 19, 2018), "Nacev: The "Monstrum" case is a living example of Zaev's morbid campaign., originally: "Нацев: Случајот „Монструм" е жив пример за морбидната кампања на Заев", available at: https://shorturl.at/hHvS4

[60] MMS, (February 21, 2020), "Ahmeti on the "Monstrum" case: We feared that it could lead to clashes and an escalation of the situation", Original: Ахмети за „Монструм": Стравувавме да не дојде до судири и ескалација на состојбата", available at: https://shorturl.at/A0d3L

[61] Alsat, (March 23, 2018), "„April 27": Charges of terrorism brought against 30 individuals. Originally: "27 април", обвинениј против 30 лица за тероризам", available at: https://shorturl.at/MC5e6

[62] See foe example critics Republica, (August 12, 2019), "Swedish court refuses to extradite Dejan Davidovski because it considers that it is a political persecution", available at: which unequivocally raises serious concerns about the MOJ's impartiality.

[63] Please see Ministry Of Justice of the R. of N. Macedonia, Strategic Plan of the Ministry of Justice" "Original: Република Северна Македонија, (Јули, 2019), „Стратешки план на Министерството за Правда, available at https://www.pravda.gov.mk/Upload/Documents/STRATESKI%20PLAN%202020-2022%20god.pdf

[64] The Republic of North Macedonia Government of the Republic of North Macedonia Ministry of Justice, (2019), "Strategy For Information Communication Technology Of Justice Sector", available at: https://www.pravda.gov.mk/Upload/Documents/Strategy-ICT-2019-2024%20.pdf

[65] Please see: https://jpacademy.gov.mk/en/publications/

Ministry of Education - Schools

Ministry of Education and with that the school system plays an important part in the overall CVE and online extremism and radicalization. Nevertheless, there is a lack of awareness not to speak about capacities among the school workers about their role in the CVE and online radicalization. Though NCCVET recognizes the importance of the schools in overall CVE, until 2024 there were no coherent programs that would enhance raising awareness and capacity-building efforts among the school workers as viable members of the CVE concept in the country. While the above-mentioned Action Plan of 2023-2027 remains valuable progress, it is not clear if and how effective the implementation would be. A general conclusion is that the school system is not prepared for preventing and countering online extremism. The existing protocols are pro form, there is no systematic approach to training the school workers, and there are no independent evaluations (except in some sporadic cases of self-evaluation).[66]

A closer look into the counseling school systems leads one to believe that there is a counseling framework system that could be improved and upgraded for CVE and online radicalization. Besides methodological (to relax existing formality) there is an urgent need for substantial context-based interventions in the counseling system including tangible monitoring procedures (with developed early warning indicators) and the existing curriculums that will upgrade these procedures and overall awareness to be suitable for CVE and online radicalization. Moreover, the current counseling services are too formalized, inflexible and not tailored to the needs and specifics of the living situation of each student and his/ her family.[67]

Local government - Municipalities

The National Strategy for CVE mandates the municipalities to be an important stakeholder in the overall institutional response to CVE and online radicalization. Municipal authorities are required to prepare local action plans and together with local action teams to contribute to the implementation of the National Strategy for CVE and online radicalization. In any community-based approach for the prevention of radicalization that can lead to violent extremism, the municipality is a central institution where the prevention model is supposed to be anchored.

[66] Metodi Hadji-Janev, (2024), Research On The Causes And Factors That Influence The Online Radicalization Of Macedonian Youth At The Local Level, Double Hope-Shtip, *The research was conducted within the framework of the project Click Smart – Say No to Extremism, by the organizations Double Hope-Stip and the Institute for Cooperation and Democratic Development from Skopje, with financial support from the European Union and implemented by Open Gate La Strada*

[67] Ibid

Nevertheless, a closer look at the municipalities' capacities to effectively CVE and prevent online radicalization echoes the challenges that the central government faces. This perception is also supported by several studies that tackle municipalities' capacities to CVE and the prevention of online radicalization.[68] Precisely, extremely low levels of awareness, and almost no capacities (institutional, human and resources) to CVE and prevent online radicalization depict a brief summary of the assessment of the municipalities' capacities to CVE and prevent online radicalization. Similarly, any preventive measures (early warning mechanisms, or mapping hot spots for online radicalization, etc.) may only be discussed on sporadic forums that some members (without continuity) have participated in, on the "only because they were told so", basis. There is no systematic approach or any administrative-led mapping mechanism of indicators that will help the municipalities and if necessary, to require central authorities' support, to better prepare and develop tangible mechanisms in CVE and prevention of online radicalization.

[68] See for example, Filip Stojkovski & Natasia Kalajdziovski (2018), Community Perspectives on the Prevention of National Extremism in Macedonia, Democracy Lab and Bergof Foundation; Also see: Filip Stojkovski, Ivan Stefanoski, Kristijan Aleksovski (2019), Baseline study: Perceptions of front-line school workers and community officials from Skopje, Kumanovo, Tetovo and Gostivar on radicalization leading to violent extremism, CRPM

Summative analysis of the Macedonian institutional capacities to prevent/counter online extremism and radicalization

While Macedonian institutions predicted and involved in the national policy and legislation are set to provide a structured response to online radicalization and extremism, challenges remain in institutional capacities (in human resources and technologies), data sharing, inter-agency coordination, and the integration of cyber expertise into law enforcement, intelligence and security sector, judiciary and educational efforts.

In particular, there are the following institutional challenges:

1. **Limited Digital Forensic Capabilities**
   - Law enforcement, intelligence and security agencies, including judicial institutions lack advanced digital forensic tools to track online radicalization processes, analyze extremist networks, and monitor encrypted communication.
   - There is a need for enhanced collaboration with tech companies and international cybercrime units to address cross-border extremist activities.

2. **Weak Content Moderation and Online Regulation**
   - North Macedonia relies on social media platforms to remove extremist content, but these platforms often operate under foreign jurisdiction with varying levels of cooperation.
   - The country lacks a legal framework and strategic approach to compel tech companies to act against online extremist content swiftly.

3. **Judicial Challenges and Legal Enforcement**
   - Prosecution of online radicalization cases is difficult due to the lack of clear evidentiary standards for digital content.
   - Judicial institutions require more training in handling cyber-related extremism cases, especially regarding international legal cooperation and digital evidence processing.

4. **Geopolitical and Foreign Influence Factors**
   - External actors, including Russia, Turkey, and Middle Eastern influences, have amplified extremist rhetoric in North Macedonia through disinformation campaigns and ideological outreach.
   - Foreign funding of religious institutions, NGOs, and media outlets has sometimes contributed to the spread of radical narratives, which requires greater transparency in foreign funding regulations.

5. **Public Awareness and Digital Literacy Deficits**
   - While some media literacy programs exist, public awareness campaigns on online radicalization are not systematically implemented.
   - Many educational initiatives remain donor-driven, rather than institutionalized within the national education curriculum.

Recommendations

1. Legislative Reforms

- **Define Terrorist Content Online (TCO):** Amend the Criminal Code to include a precise definition of TCO, aligning with EU Regulation (2021/784). Specify content that incites violence, promotes terrorism, or facilitates terrorist acts, excluding educational, journalistic, or counter-terrorism content. Establish a one-hour removal deadline for Hosting Service Providers (HSPs) with clear procedures for compliance.
- **Introduce Proactive HSP Obligations:** Enact regulations requiring HSPs to proactively monitor and remove TCO, with penalties for non-compliance (e.g., fines up to 4% of global revenue for systematic violations) and incentives (e.g., liability exemptions for timely removal).
- **Strengthen Hate Speech Provisions:** Clarify and consolidate Articles 319, 394-d, and 417 of the Criminal Code to address online hate speech explicitly, ensuring precise definitions and judicial guidance to improve enforcement consistency.
- **Enhance Cybercrime Legislation:** Introduce a new criminal offense, "Digital Dissemination of Terrorist Content," to address gaps in prosecuting subtle extremist content that avoids explicit calls to violence.
- **Incorporate Human Rights Safeguards:** Embed principles of proportionality, necessity, and non-discrimination in TCO regulations. Mandate judicial oversight for content removal and data access, with transparent appeal mechanisms for users.

2. Institutional Capacity Building

- **Establish a Dedicated TCO Monitoring Unit:** Create a specialized unit within the Ministry of Interior's (MoI) Sector for Combating Terrorism, Violent Extremism, and Radicalism, tasked with monitoring TCO. Ensure coordination with the National Committee for Countering Violent Extremism and Counterterrorism (NCCVECT), National Security Agency (NSA), and Agency for Audio and Audiovisual Media Services (AVMU).
- **Enhance Inter-Agency Coordination:** Develop a situation center under the MoI for real-time information exchange among the MoI, NSA, Intelligence Agency, Ministry of Justice (MoJ), and Public Prosecutor's Office. Regular inter-agency drills and joint protocols should be established.
- **Invest in Technical Infrastructure:** Deploy AI-based tools, hash-matching technologies, and big data analytics to monitor encrypted platforms (e.g., Telegram, WhatsApp) and detect subtle extremist content. Partner with tech companies for interoperable data-sharing platforms.
- **Specialized Training Programs:** Provide ongoing training for security personnel, prosecutors, and judges on digital forensics, Open-Source Intelligence (OSINT), and cultural sensitivities. Training should cover emerging trends like extremist content on gaming platforms and encrypted chat applications.

Recommendations

3. Human Rights Protections

- **Implement Judicial Oversight:** Require judicial warrants for monitoring private communications or removing content. Establish specialized judicial panels to oversee TCO cases, ensuring accountability and preventing overreach.
- **Create Independent Oversight Bodies:** Form an independent commission, including civil society representatives, to monitor TCO implementation, conduct periodic audits, and publish transparency reports on content removal and data access.
- **Strengthen Appeal Mechanisms:** Ensure citizens have access to clear, accessible complaint processes for unlawful monitoring or content removal, with expedited judicial review.
- **Promote Civil Society Engagement:** Involve civil society organizations in policy development, monitoring, and public education to enhance transparency and advocate for human rights protections.

4. Public-Private Partnerships (PPPs)

- **Develop Regulated PPP Frameworks:** Leverage private sector expertise in AI, real-time monitoring, and media analysis through PPPs. Ensure strict oversight, transparency, and compliance with human rights standards to prevent abuses.
- **Support Smaller HSPs:** Provide technical and financial assistance to small and medium-sized HSPs to meet TCO regulation requirements, including access to shared AI tools and training on content moderation.
- **Foster Tech Company Collaboration:** Establish formal cooperation mechanisms with major platforms (e.g., Facebook, YouTube, Telegram) for rapid content removal and data sharing, aligning with Europol's EU Internet Referral Unit (IRU) and PERCI system.

5. Public Awareness and Community Resilience

- **Launch Digital Literacy Campaigns:** Implement nationwide campaigns, led by the Agency for Youth and Sport (AYS) and Local Councils for Prevention (LCP), to enhance digital literacy, critical thinking, and resilience against extremist propaganda, targeting youth and vulnerable communities.
- **Promote Counter-Narratives:** Develop online platforms and media campaigns to disseminate counter-narratives, in collaboration with civil society, religious leaders, and community influencers. Focus on social cohesion and interfaith dialogue to counter divisive extremist rhetoric.
- **Strengthen Educational Initiatives:** Integrate digital responsibility and media literacy into school curricula, supported by the Ministry of Education (MoE). Train teachers to recognize early signs of radicalization and engage students in critical thinking exercises.

Recommendations

6. International and Regional Cooperation

- **Enhance EU Collaboration:** Strengthen cooperation with Europol, Eurojust, and the Global Counterterrorism Forum (GCTF) to share intelligence, best practices, and technical expertise. Establish a North Macedonia chapter in the ICCT's Foreign Terrorist Fighters (FTF) Knowledge Hub.
- **Foster Bilateral Partnerships:** Deepen collaboration with the Netherlands and other EU countries to adopt best practices in online monitoring, legal frameworks, and prevention strategies, building on the Netherlands-North Macedonia Counterterrorism Platform.
- **Align with EU Acquis:** Accelerate legislative alignment with EU Regulation (2021/784) and other EU directives to enhance cross-border cooperation and access to EU funding for counter-extremism initiatives.

7. Addressing Emerging Threats

- **Monitor New Digital Platforms:** Develop strategies to monitor extremist content on emerging platforms, such as online gaming environments and niche forums, where youth are increasingly targeted.
- **Counter Disinformation and Hybrid Threats:** Integrate counter-disinformation measures into the National Strategy for Countering Hybrid Threats (2021-2026), focusing on detecting and mitigating foreign influence operations that amplify extremist narratives.
- **Address Anti-Government Extremism:** Proactively monitor the rise of anti-government movements, such as sovereign citizen ideologies, to prevent their emergence in North Macedonia, drawing lessons from Dutch experiences.

8. Financial and Resource Allocation

- **Secure Sustainable Funding:** Allocate dedicated budgets for TCO monitoring, training, and public awareness campaigns, leveraging national funds and international support from the EU and the Netherlands Ministry of Foreign Affairs.
- **Invest in Digital Forensics:** Establish a national digital forensics institute or partner with private entities to enhance capabilities for investigating TCO, addressing the current lack of private forensic expertise.
- **Support Local Governments:** Provide resources to municipalities to implement local prevention programs, including training for community leaders and funding for youth-led community centers.

Appendix A - Identifying Needs Assessment Stakeholders

NAME OF STAKEHOLDER	**STAKEHOLDER DESCRIPTION** (PRIMARY PURPOSE, AFFILIATION, FUNDING)
Assembly of North Macedonia	Affiliation
Ministry of Interior Affairs	Primary purpose
Ministry of Defense	Primary purpose
Ministry of Justice	Affiliation
Ministry of Digital Transformation and Technology	Affiliation
Ministry for European Affairs	Affiliation
National Committee for Countering Violent Extremism and Countering Terrorism	Primary purpose
Commission for Relations with Religious Communities and Groups of Macedonia	Affiliation
National Security Agency	Primary purpose
Intelligence Agency	Primary purpose
Agency for audio and audiovisual services	Affiliation
Human rights organisations	Primary purpose
International civil society organizations	Affiliation
Republic of North Macedonia Ombudsman	Primary purpose
Public opinion analysts	Affiliation
Security experts	Affiliation

Appendix B - References and list of documents

1. National Strategy for countering violent extremism
2. Action plan for implementing the strategy for countering violent extremism
3. Criminal Code of North Macedonia
4. Law on Prevention of Money Laundering and Terrorism Financing
5. Law on Prevention and Protection Against Discrimination
6. Law on Audio and Audiovisual Services
7. National Cybersecurity Strategy
8. National Strategy for Building Resilience and Countering Hybrid Threats
9. Law on Data Protection
10. Law on Criminal Procedure
11. Law on Electronic Communications
12. Law on Interception of Communications
13. Strategic Plan of the Ministry of Interior 2018-2020
14. Strategic Plan of the Ministry of Interior 2019-2021
15. Global Counterterrorism Forum (GCTF) Toolkit on Strengthening National-Local Cooperation in Preventing and Countering Violent Extremism
16. World Bank and Global Cyber Security Capacity Centre, Cybersecurity Capacity Evaluation (2018)
17. 2024 Study on “Protecting Digital Privacy, Legal and Practice Analysis for North Macedonia and EU”

Appendix C - Interview guide

Needs assessment report on institutional capacities of North Macedonia in countering online extremism

Date: _____

Questionnaire Objective: To collect information on the current capacities, experiences, and needs of the public sector in addressing online radicalization and violent extremism. Following the introduction about the questionnaire, its purpose, scope of interest, and what it will serve to, the researcher makes sure whether everything is clear, by asking:
-Do you understand the parameters of our conversation?
-Do you have any questions at this time?

I. General information about the interviewee and the institution

1. **Name and surname of the interviewee:**
2. **Institution:**
3. **Position/Role in the institution:**
4. **Duration of work engagement in this position:**
5. **Brief description of your institution's role in addressing radicalization and violent extremism:**

II. Understanding online radicalization and violent extremism

6. How do you define online radicalization and its impact on security in Macedonia?
7. Do you think online radicalization is a growing problem in your area of work? If so, what are the main indicators?
8. What are the main platforms, tools, or channels used by radical groups in the online space?

Appendix C - Interview guide

III. Institutional capacities

9. Does your institution have formalized policies or strategies for addressing online radicalization and violent extremism?
    - If so, what are the key components?
    - If not, what are the biggest challenges to establishing them?

10. What resources (human, technical, financial) does your institution have to deal with online radicalization?

11.Does your institution collaborate with other institutions or organizations on this topic?

- If so, which ones and what is the nature of the cooperation?
- If not, why?

IV. Challenges and gaps

12. What are the biggest challenges you face in identifying and addressing online radicalization?

13. Does your institution have access to relevant data and tools for monitoring online radicalization?

- If not, what would be needed for improvement?

14. Do you think there are gaps in the legal and institutional framework that make it difficult to combat online radicalization?

- If so, which ones specifically?

15. What aspects of your institutional structure or resources should be strengthened to more effectively address this threat?

V. Training and capacity development

16. Do employees in your institution have access to regular training on dealing with online radicalization and violent extremism?

- If so, what trainings have you attended so far and what was their impact?
- If not, what training do you think would be most relevant?

17. What topics or training areas would be most important to strengthen the capacities of your institution?

- Technical skills (monitoring, data analysis, etc.)
- Legal framework and legal aspects
- Communication strategies and public awareness
- Partnerships and multi-sectoral cooperation

Appendix C - Interview guide

VI. Recommendations and next steps

18. In your experience, what measures or activities could have the greatest impact in addressing online radicalization?

19. What support do you expect from national authorities, international partners or the civil society sector to address this threat?

20. Is there anything else you would like to share related to this topic?

VII. Final questions

21. Would you like to receive feedback on the findings of this research?

22. Would you like to suggest additional relevant individuals or institutions for interview?

Note to interviewers:

- Stick to the questions, but be flexible if the interviewee shares significant information outside the scope of the questionnaire.
- Remain neutral and professional in asking questions and leading the discussion.
- Make sure the answers are detailed and clear, asking follow-up questions if necessary.

List of appendicies

Appendix D - Activity Reports

ACTIVITY REPORTS	PAGE
National Forum: Religion and Online Challenges	50
Training on multidisciplinary approach on P/CVE	60
Study visit to Netherlands	70
Expert debate: Online extremism and human rights	80
Workshop on Legislative Adjustment for Countering Terrorist Content Online	96

Activity Report

National Forum: Religion and Online Challenges



February 2025

Prepared by
Samet Shabani

HORIZON CIVITAS

CILC Center for International Legal Cooperation

Netherlands - North Macedonia Counterterrorism Platform

Kingdom of the Netherlands

ACTIVITY REPORT

OVERVIEW

Project	Netherlands – North-Macedonia Counterterrorism Platform II (MK23081) *Activity implemented in scope of the DELETE project
Activity	National Forum: Religion and Online Challenges
Date	12.02.2025
Location	Skopje, North Macedonia
Panelists	Ali Pajaziti, Aneta Jovkovska, Marjan Gjurovski, Sead Dzigal
Moderator	Mersiha Smailovikj
Facilitator	Natasha Nikoforovikj, Elena Stojanova, Ognen Kocevski

DESCRIPTION OF ACTIVITY

Objective

This activity aimed to engage religious stakeholders, including religious leaders, young theologians, and communication experts, alongside representatives from public institutions, academia, and civil society organizations, to discuss strategies for enhancing the capacities of religious communities to counter deviant phenomena online, such as radicalization, hate speech, and discrimination, while promoting positive narratives, interfaith cooperation, and societal cohesion in the digital space.

Methodology and means of delivery

The activity was consisted of three main sessions:

1. Moderated discussion with presentation: Experts provided insights into the challenges of online deviant phenomena, the role of religious communities in countering them, and the importance of strategic communication in online spaces.

2. World Café: proposals and recommendations from and for the religious stakeholders about preventing deviant phenomena: Participants provided inputs and rotated three thematic tables: (1) Religion, youth and online space; (2) Theology and security issues; (3) Religion and media literacy

3. Plenary session: presentation of thematic table conclusions, formulating list of recommendations: Facilitators from each World Café table presented their group's discussion points and recommendations, fostering a collective dialogue on actionable strategies.

Narrative description of activity

The activity commenced with opening remarks by Samet Shabani from Horizon Civitas, who emphasized the importance of empowering religious communities to address online challenges as part of the broader objectives of the Netherlands – North-Macedonia Counterterrorism Platform II.

The Director of the Commission for relations with religious communities and groups (CRRCG) Mrs Olivera Trajkovska emphasized that the very founding idea of the Commission is to engage religious communities in prevention of phenomena that regards countries and communities' security and resilience, as well as fostering the sense of dialogue in a multi-faith and multi-ethnic setting of the country.

The National Coordinator for CVE and CT Mr Pavle Trajanov pointed out that the religious stakeholders are one of the main actors in the 'whole-of-society' approach of institutions to countering extremism (online and offline).

The activity continued with the session moderated discussion in moderation of Mersiha Smailovikj, national expert on religious freedom. The experts of the session and their remarks were as follows:

1. Marjan Gjurovski, security expert: Marjan Gjurovski delivered a speech titled "The Role of Religious Stakeholders in Enhancing Online Security." He outlined how religious actors—such as theologians, religious figures, and communities—can contribute to security issues through various mechanisms. Gjurovski emphasized the potential of religious leaders providing councils and training to security institutions on specific religious matters to prevent online phenomena like hate speech and radical narratives. He advocated for integrating online security topics, including cybersecurity and the spread of radical content, into theological studies and religious rituals, such as sermons and community advice in places of worship. Additionally, he highlighted the importance of fostering a spirit of collaboration between religious communities and related institutions, drawing on practices from EU countries to address contemporary online challenges effectively.

2. Ali Pajaziti, expert on sociology of religions: Ali Pajaziti presented a speech titled "The Impact of Online Deviant Phenomena on Society and Religion." He explored how contemporary deviant phenomena in online spaces—such as religiophobia, religion-based discrimination, and radical religio-political narratives—shape societal dynamics, influence the understanding of modernization, and affect perceptions of religion, particularly through extreme approaches to these values. Pajaziti assessed the existing capacities of religious stakeholders in North Macedonia to address these online challenges, noting both strengths and limitations in their current efforts. He offered recommendations for improvement, including enhancing training programs, fostering interfaith dialogue, and developing targeted strategies to counter radical narratives, thereby strengthening the role of religious communities in promoting societal cohesion and addressing modern online threats.

3. Aneta Jovkovksa, expert on religious pedagogy: Aneta Jovkovska delivered a presentation titled "The Role of Religious Pedagogy in Addressing Online Challenges." She discussed how religious pedagogy can contribute to tackling online challenges in society by integrating ethical teachings and moral guidance into digital education. Jovkovska emphasized the need to train future religious figures with digital skills to effectively respond to deviant phenomena in online spaces, such as radicalization and hate speech, through targeted programs that enhance their technological proficiency. She also advocated for synchronizing religious ontology with modern tools to prevent online threats, proposing the development of curricula that blend traditional religious values with contemporary digital strategies to foster a proactive approach among religious communities.

4. Sead Dzigal, expert on communication sciences: Sead Dzigal presented a speech titled "Leveraging Religious Influencers and Counter-Narratives in Online Spaces." He explored how the trend of "religious influencers" can contribute to preventing online deviant phenomena by using their platforms to promote positive religious messages and counter radical content.

HORIZON CIVITAS
CILC Center for International Legal Cooperation
Netherlands - North Macedonia Counterterrorism Platform
Kingdom of the Netherlands

Dzigal assessed the existing capacities of religious institutions in communicating security challenges, highlighting strengths in strategic communication and digital tools, while identifying gaps that need addressing through enhanced training and technology adoption. He further discussed the development of counter-narratives and alternative narratives to challenge radical interpretations of faith online, offering examples such as interfaith campaigns and recommendations for creating engaging, faith-based content to foster tolerance and understanding.

Following the moderated discussions, the World Café session focused on three key questions designed as thematic tables.

Table 1: Religion, youth and online space:

Discussion and recommendations:

- Establish Councils within Religious Communities to monitor and counter fake news, hate speech, and extremist content, with young theologians leading public responses to promote peace and coexistence.
- Train young theologians as influencers to share spiritual values and positive narratives online, with oversight to ensure ethical conduct.
- Develop podcasts (Theocasts) featuring theologians to engage youth with content promoting peace and understanding.
- Launch interfaith campaigns, inspired by Albania's "Not in My Name!", involving religious leaders, public figures, and cultural influencers to counter radicalization.
- Foster collaboration between religious communities and institutions, drawing on EU practices, to address online challenges affecting youth.
- Assess the impact of online deviant phenomena like religiophobia and radical religio-political narratives on youth, recommending enhanced training and interfaith dialogue.
- Synchronize religious ontology with modern tools to prevent online threats, creating relevant content for young people.
- Discuss the role of religious influencers in countering radical content and engaging youth with positive messages.
- Develop counter-narratives and alternative narratives to challenge radical faith interpretations, using examples like interfaith campaigns to engage young audiences.

Table 2: Theology in security issues

Discussion and recommendations:

- Establish a Council of Theologians for Countering Online Extremism that will assist security institutions in addressing religiously motivated extremist content in online spaces.
- Training to security institutions on religious matters to prevent online threats.
- Integrate online security topics like cybersecurity and radical narratives into theological studies and religious rituals, such as sermons, to reach broader audiences.
- Use religious influencers to counter radical content, evaluating institutional communication capacities.

Table 3: Religion and media literacy

Discussion and recommendations:

- Promote assertive communication through education on self-control, fact-checking, and tolerance in online spaces to engage theologians effectively.
- Evaluate existing institutional communication capacities, identifying gaps in strategic communication and digital tools for youth outreach.
- Enhance awareness training for religious leaders to recognize and address hate speech and misinformation targeting all religious communities, fostering mutual respect and societal protection.
- Train future religious figures with digital skills to respond to deviant phenomena in online spaces, targeting youth engagement.

EVALUATION OF ACTIVITY

Feedback and impact

The National Forum was well-received, with participants appreciating the opportunity to engage religious stakeholders in addressing online challenges. The discussions highlighted the critical role of religious communities in countering deviant phenomena while promoting positive narratives. The event strengthened collaboration between religious communities, public institutions, and civil society, laying the groundwork for sustained interfaith cooperation. Recommendations, such as establishing councils within religious communities and launching online campaigns, were seen as practical steps toward aligning North Macedonia's efforts with international best practices for countering online extremism.

Problems encountered

Challenges included limited representation from smaller religious communities, which restricted the diversity of perspectives. The short duration of the event constrained in-depth discussions on complex issues, such as monitoring encrypted platforms and addressing subtle extremist narratives. Some participants noted the need for more technical expertise to discuss advanced tools for online content moderation.

New/updated information

The forum revealed emerging trends in online deviant behaviors among youth, including religiophobia, digital addiction, and the role of unqualified religious influencers. Participants highlighted the growing use of encrypted platforms and gaming spaces for spreading extremist content, underscoring the need for enhanced digital monitoring capabilities. The discussions also emphasized the potential of interfaith campaigns, such as "Not in My Name!", as a model for North Macedonia. Updates from the Ministry of Interior (to be confirmed) indicated ongoing efforts to improve digital forensics and inter-agency coordination to address online threats.

CONCLUSIONS AND RECOMMENDATIONS

The National Forum successfully facilitated a multi-stakeholder dialogue on the role of religious communities in countering online deviant phenomena, including radicalization, hate speech, and discrimination. The discussions underscored the need for enhanced capacities within religious communities, strategic online initiatives, and interfaith cooperation to promote societal cohesion. While North Macedonia has a foundation for addressing these challenges through its national strategies, gaps remain in technical capacities, specific regulations for online content, and engagement with youth in digital spaces. The forum highlighted the importance of civil society and religious stakeholders in advocating for transparency and human rights protections in online environments.

Recommendations

1. Capacity Building:

- Establish Councils within Religious Communities to monitor and counter fake news, hate speech, and extremist content, with young theologians leading public responses.
- Train young theologians as influencers to promote spiritual values and positive narratives online, with oversight to ensure ethical conduct.
- Enhance awareness training for religious leaders to recognize and address hate speech and misinformation targeting all religious communities.

2. Online initiatives:

- Promote assertive communication through education on self-control, fact-checking, and tolerance in online spaces.
- Develop podcasts (Theocasts) featuring theologians to engage youth with religious content promoting peace and understanding.
- Launch interfaith campaigns, inspired by Albania's "Not in My Name!", involving religious leaders, public figures, and cultural influencers to counter radicalization.

3. Educational reforms:

- Introduce digital ethics courses at theological faculties to address online challenges.
- Promote media literacy programs to encourage responsible media consumption among youth.

4. Interfaith and Institutional Capacities:

- Foster interfaith dialogue between religious leaders and youth to combat deviant phenomena.
- Encourage joint interfaith efforts to address hate speech and radicalization collaboratively.
- Strengthen coordination between religious communities, the Ministry of Interior, and the National Committee for Countering Violent Extremism and Terrorism to align efforts with national strategies.

HORIZON CIVITAS
CILC Center for International Legal Cooperation
Netherlands - North Macedonia Counterterrorism Platform
Kingdom of the Netherlands

Activity Report

Trainings by Dutch Police Academy



March 2025

Prepared by
Diana Navarrete

HORIZON CIVITAS
CILC Center for International Legal Cooperation
Netherlands - North Macedonia Counterterrorism Platform
Kingdom of the Netherlands

ACTIVITY REPORT

OVERVIEW

Project	Netherlands – North-Macedonia Counterterrorism Platform II (MK23081)
Activity	Training provided by the Police Academy • Training OSINT and online investigation • Training on Preventing radicalization for first line professionals (multidisciplinary)
Date	10.03.2025 - 14.03.2025
Location	Demir Kapija, North Macedonia
Presenters	Bart Collard, Coordinator in Counter Terrorism (CT) and Prevention of Violent Extremism (PVE), Dutch Police Academy Franklin Renfrum, Trainer at the Dutch Police Academy Patrick van de Bunte, Trainer at the Dutch Police Academy Sanne Cator, Trainer at the Dutch Police Academy
Coordination	Emily van Rheenen, Senior Project Manager, CILC Diana Navarrete, Project Manager, CILC Aleksandra Krzalovska, Local expert and interpreter
Interpreters	Filip Koviloski , Vesna Andonovska

DESCRIPTION OF ACTIVITY

Objective

The trainings provided by the Dutch Police Academy aimed to provide members of the National committee for countering violent extremism and counter-terrorism from North Macedonia insights into how the Netherlands and EU member states address counter terrorism and violent extremism, including the early detection of terrorist content online (TCO). The sessions focused on the definition of how to monitor and address terror-related online activity as well as mechanisms that make such monitoring and early detection possible, including the Dutch so-called “soft approach”. Additionally, the sessions facilitated exchanges and supported the strengthening of cooperation among relevant authorities and representatives from local institutions.Simultaneous interpretation was provided during all the sessions in the program to ensure the smooth implementation of the sessions.

Methodology and means of delivery

To ensure preparations for the training sessions went smoothly and were responsive to participants’ needs, the project team held regular coordination meetings with representatives from the National Committee for countering violent extremism and counter-terrorism, representatives from Horizon Civitas and with the representatives from the Dutch Police Academy.

The training on OSINT and online investigation targeted high-level representatives from key counter-terrorism entities in North Macedonia, including the Intelligence Agency, the Financial Intelligence Unit, Ministry of Interior, Agency for National Security, the National Committee for Countering Violent Extremism and Counterterrorism, and the Terrorism Investigation Department from the Basic Public Prosecution Office. A total of 20 participants attended this training session.

HORIZON CIVITAS
CILC Center for International Legal Cooperation
Netherlands - North Macedonia Counterterrorism Platform
Kingdom of the Netherlands

The training on preventing radicalization for first line professionals targeted representatives from the National Committee for Countering Violent Extremism and Counterterrorism, diverse municipalities in the country, the Ministry of Interior, Ministry of Sports, religious leaders, social workers, and civil society organizations. This allowed to have a multidisciplinary approach and to promote coordination among the different organizations and sectors relevant at the local and national level. A total of 17 participants joined this session.

To ensure a comprehensive understanding of the topic, both training sessions began with an overview of the main types of radicalization, including key definitions and indicators for early detection. Participants were also introduced to emerging trends in radicalization across Europe and globally, providing valuable context for the evolving nature of the threat landscape. Participants were also presented with relevant tools for online monitoring and detection.
To bridge theory with practice, the sessions incorporated hands-on exercises that allowed participants to apply the concepts discussed. These practical components were designed to simulate real-world scenarios, helping participants better understand the operational challenges and responses required for an effective counterterrorism approach.

HORIZON CIVITAS
CILC Center for International Legal Cooperation
Netherlands - North Macedonia Counterterrorism Platform
Kingdom of the Netherlands

Narrative description of activity

Training OSINT and online investigation

The training on OSINT and online investigation opened with welcoming remarks from Ms. Emily van Rheenen, Senior Project Manager at CILC, Mr. Pavle Trajanov, National for Countering Violent Extremism and Counterterrorism, and Ms. Nona de Jong, representative from the Embassy of the Netherlands in Sarajevo. The training sessions were delivered by counterterrorism and preventing violent extremism (CT/PVE) experts from the Dutch Police Academy, with a strong focus on Open Source Intelligence (OSINT), online investigations, and principles for early detection.

Over the course of two and a half days, participants engaged in in-depth discussions on key definitions in the field, including extremism, violent extremism, and terrorism. These sessions provided an opportunity to compare the terminology and frameworks currently used in North Macedonia with those applied in the Netherlands and internationally. Participants recognized the importance of updating and harmonizing national definitions to align with international standards. This alignment was seen as a critical step toward developing specific regulations and operational guidelines for effective online monitoring of extremist content.

The sessions also featured an in-depth exploration of the various forms of radicalization, focusing on their distinct characteristics and indicators for early detection. Key types discussed included right-wing extremism, left-wing extremism, and jihadist-inspired radicalization. Each form was examined in terms of its ideological foundations, recruitment strategies, and the sociopolitical contexts in which it tends to emerge.

Participants learned to identify the specific signs and behavioral patterns associated with each type of radicalization, as well as the primary channels used for dissemination—ranging from mainstream social media platforms to niche forums, gaming communities, and encrypted messaging apps. Special attention was given to how these groups tailor their messaging to appeal to different demographics, particularly vulnerable youth and how to use open source resources to track and monitor these messages.

To reinforce theoretical knowledge with practical application, participants were presented with real-life case studies. These case studies allowed them to analyse actual incidents, trace the radicalization pathways involved, and apply the detection frameworks discussed during the sessions. This hands-on approach helped bridge the gap between conceptual understanding and operational readiness.

In addition to the core ideological frameworks discussed, trainers also highlighted the emergence of new and increasingly complex forms of radicalization that do not neatly align with traditional categories. This phenomenon, often referred to as the "mixed-salad" or "salad bar" approach, involves the blending of disparate ideological elements into a single, often incoherent worldview. This trend has become particularly pronounced in the aftermath of the COVID-19 pandemic, which created fertile ground for misinformation, distrust in institutions, and social fragmentation—conditions that extremist actors have exploited to recruit and radicalize individuals.

A notable example is the rise of the sovereign citizens movement in the Netherlands, a subset of anti-government extremism. This movement rejects the legitimacy of state institutions and promotes self-governance, often leading to confrontational or unlawful behaviour. Although participants did not report the presence of such movements in North Macedonia at this time, they acknowledged the potential for similar trends to emerge in the near future.

To help participants contextualize this evolution, the sessions included an analysis of Professor David Rapoport's "Wave Theory" of modern terrorism. This theoretical framework, which outlines the historical progression of terrorist movements in ideological waves, served as a basis for reflecting on how radicalization may continue to evolve in North Macedonia and across Europe. Participants were encouraged to consider whether a new, fifth wave is emerging, and what implications this may have for future prevention and response strategies.

To conclude the training, participants had the opportunity to network with the Dutch Ambassador to the Netherlands, H.E. Özlem Canel. A group picture was also taken, including participants from both training sessions.

HORIZON CIVITAS
CILC Center for International Legal Cooperation
Netherlands - North Macedonia Counterterrorism Platform
Kingdom of the Netherlands

Training on preventing radicalization for first line professionals

The training on preventing radicalization for first line professionals opened with welcoming remarks from Diana Navarrete, Project Manager at CILC. Similarly to the previous training sessions, counterterrorism and preventing violent extremism (CT/PVE) experts from the Dutch Police Academy provided an in-depth overview of the main definitions in the field.

The sessions also allowed for participants to learn about the various forms of radicalization, including their distinct characteristics, ideological foundations, recruitment strategies, and the sociopolitical contexts in which it tends to emerge. During this training, the main focus on the sessions was put on prevention. Trainers introduced the so-called “soft approach” to prevention, which emphasizes early, non-punitive intervention with individuals showing signs of radicalization. This approach is grounded in dialogue, trust-building, and support rather than enforcement or prosecution.

Local law enforcement officers and community leaders often serve as the first point of contact in cases involving individuals showing signs of radicalization. They play a critical role in identifying early warning indicators and initiating initial engagement with the individual. However, their efforts are most effective when embedded within a broader, multi-agency framework.

To ensure a multidisciplinary and sustained response, these officers collaborate closely with a network of local and regional stakeholders —including social services, mental health professionals, educational institutions, and community-based organizations. This coordinated approach allows for comprehensive monitoring, timely intervention, and the provision of tailored support to individuals at risk.

In this context, inter-agency cooperation was emphasized as a cornerstone of successful prevention strategies. Participants recognized that building strong communication channels and trust among local actors is essential for ensuring that no warning signs are overlooked and that interventions are both timely and effective.

Participants also benefited from real-life, case-based scenarios that enabled them to apply the concepts learned during the training. These practical exercises helped them identify key indicators for the early detection of radicalization and violent extremism, reinforcing their analytical skills and enhancing their ability to respond effectively in real-world situations.

EVALUATION OF ACTIVITY

Feedback and impact

The training sessions were well received by participants, who valued the opportunity to exchange best practices and share lessons learned. The event also served to strengthen collaboration between public institutions and multidisciplinary local bodies, fostering mutual understanding and trust. This engagement laid a solid foundation for continued cooperation and joint efforts in the prevention of radicalization and violent extremism.

Problems encountered

There were no problems encountered during the implementation of this activity

New/updated information

During the training sessions, participants shared valuable insights into the evolving landscape of extremism in North Macedonia, drawing attention to the emergence of anti-government movements. These developments reflect a broader shift toward ideologically fluid and decentralized forms of radicalization, often fueled by distrust in institutions and amplified through online platforms.

Participants also reported a noticeable increase in extremist content circulating on gaming platforms and encrypted messaging applications, particularly among younger audiences. This trend underscores the urgent need for more sophisticated monitoring tools and strategies tailored to the digital environments where radicalization is increasingly taking place.

These observations highlight the importance of proactive, tech-savvy approaches to prevention, as well as the need for continuous training and inter-agency collaboration to stay ahead of emerging threats.

CONCLUSIONS AND RECOMMENDATIONS

The training sessions effectively equipped participants with a comprehensive understanding of the key elements necessary to identify the specific signs and behavioural patterns associated with various forms of radicalization. Participants also gained insight into the primary channels used for the dissemination of extremist content, including social media platforms, encrypted messaging apps, and online forums.

A significant component of the training focused on Open Source Intelligence (OSINT) techniques. Participants were introduced to practical tools and methodologies for conducting online investigations and were given the opportunity to apply these skills through case-based scenarios.

Participants expressed strong interest in continuing this capacity-building process, emphasizing the need for follow-up trainings. They also highlighted the importance of expanding these sessions to include local law enforcement officers, particularly frontline police, who are often the first to encounter early signs of radicalization.

Moreover, this activity laid the groundwork for future project initiatives—most notably, the upcoming study visit to the Netherlands. This visit will offer participants an in-depth look at the Dutch model for coordinating efforts to prevent violent extremism and terrorism. It will also provide a platform to examine the legal frameworks governing online monitoring and to explore opportunities for enhanced bilateral cooperation.

Activity Report

Study visit on countering online extremism in the Netherlands



March 2025

Prepared by
Diana Navarrete

HORIZON CIVITAS

CILC Center for International Legal Cooperation

Netherlands - North Macedonia Counterterrorism Platform

Kingdom of the Netherlands

OVERVIEW

Project	Netherlands – North-Macedonia Counterterrorism Platform II (MK23081) *Activity implemented in scope of the DELETE project
Activity	Study visit on countering online extremism in the NL
Date	17.03.2025 - 20.03.2025
Locations	The Hague, The Netherlands
Presenters	Azra Ikovic, Eurojust Barbara Molas, Research Fellow, Center for Counter-Terrorism (ICCT) Bart Collard, Coordinator in Counter Terrorism (CT) and Prevention of Violent Extremism (PVE), Dutch Police Academy Dorien Kardol, Prosecutor, National Coordinating Public Prosecutor Counterterrorism, Dutch National Public Prosecutor's Office Ivo Arsovski, Europol Liaison Officer, Head of LB North Macedonia, Europol Lili-Anne de Jongh, Policy Advisor, Care and Security Team of the Municipality of Delft Maria Laura Ferioli, Eurojust Merlina Herbach, Research Fellow, International Center for Counter-Terrorism (ICCT) Tanya Mehra, Senior Research Fellow, International Center for Counter Terrorism (ICCT) Wies van Dipten, Process Coordinator, Care and Security Team of theMunicipality of Delft
Coordination	Diana Navarrete, Project Manager, CILC Samet Shabani, Horizon Civitas Wikje Trimbos, Intern, CILC
Interpreters	Vesna Andonovska, Jane Bozhinovski

DESCRIPTION OF ACTIVITY

Objective

The study visit aimed to provide members of the National committee for countering violent extremism and counter-terrorism from North Macedonia, including representatives from the Ministry of Defence, Ministry of Interior, Agency for National Security, relevant national committees, and judicial institutions, with insights into how the Netherlands and international partners seek to counter terrorism and violent extremism. The visit focused on how to monitor and address terror-related online activity as well as the accompanying legal framework and mechanisms that make such monitoring possible. Additionally, the study visit facilitated exchanges with peers from Dutch justice entities, law enforcement institutions, and local municipalities as well as international agencies including Eurojust, Europol, and the International Centre for Counter-Terrorism.

Methodology and means of delivery

The study visit targeted high-level representatives from key counter-terrorism entities in North Macedonia, including the Financial Intelligence Unit, Ministry of Defense, Ministry of Interior, National Security Agency, the National Committee for Countering Violent Extremism and Counterterrorism, criminal courts, and civil society organisations. A total of 12 participants were able to attend the visit.
Based on requests from participants and to ensure a comprehensive overview of the Dutch (and international) approach to online counterterrorism, the CILC team scheduled visits to institutions including the Municipality of Delft, the International Centre for Counter-Terrorism, Eurojust, and Europol. To address the practical realities needed for a proper counterterrorism approach, there were also sessions on the legal framework and legislation for online monitoring in the context of counterterrorism.
To ensure preparations for the visit went smoothly and were responsive to participants' needs, the project team held regular coordination meetings with representatives from the National Committee for countering violent extremism and counter-terrorism, representatives from Horizon Civitas and with relevant Dutch institutions. Participants from North Macedonia also prepared a list of questions, which were communicated in advance to all participating agencies and addressed during the sessions.

Narrative description of activity

Welcome remarks and introduction to online monitoring

The study visit opened with welcoming remarks from the CILC team as well as an introduction to online monitoring in the context of countering terrorism and violent extremism (CT/PVE) in the Netherlands.

The introduction was provided by expert Bart Collard, Coordinator in Counter Terrorism (CT) and Prevention of Violent Extremism (PVE) at the Dutch Police Academy. The session was a continuation of the trainings provided by the Dutch Police Academy in early March 2025. The session covered open□source intelligence, OSINT mechanisms, the difference between monitoring and searching, how both monitoring and searching are done in the Netherlands, and legal considerations for all of the above, including a human rights perspective. This provided participants with a better understanding of the roles and responsibilities of the different institutions in the Netherlands and prepared them for the next sessions included in the agenda of the visit.

Visit to the National Coordinator for Counterterrorism and Security (NCTV)

The National Coordinator for Counterterrorism and Security is an office within the Dutch Ministry of Justice and Security, and it coordinates the efforts of all parties in the Netherlands which have a role in counterterrorism. As part of this it maintains the Terrorist Threat Assessment Netherlands, the Counterterrorism Alert System, and cooperates with other governments and international partnerships such as the EU and the UN.

The visit focused on providing an overview of the role and functioning of the NCTV, including the detection, collection and processing of signs of radicalization and relevant information and the division of roles and responsibilities for conducting online investigations among all relevant government and enforcement agencies. This allowed participants to exchange best practices and learn relevant information to support the implementation of an online monitoring unit in North Macedonia.

HORIZON CIVITAS
CILC Center for International Legal Cooperation
Netherlands - North Macedonia Counterterrorism Platform
Kingdom of the Netherlands

Additionally, the session involved a discussion on how the internet and social media are often used by extremists and terrorists to form movements and disseminate their political and ideological stances. The NCTV representatives also described the Enhanced Approach Online which the office is seeking to use to reign in extremist content. The Enhanced Approach Online includes four main pillars: 1) dialogue with the internet sector, 2) tightening up statutory instruments, 3) strengthening the local approach, and 4) international cooperation.

Legal framework and legislation for online monitoring in counterterrorism

Prosecutor Dorien Kardol from the National Coordinating Public Prosecutor Counterterrorism Department at the Dutch National Public Prosecutor's Office provided an overview of the Dutch legal framework and legislation for online monitoring. This session aimed to provide a practical and legal understanding of the grounds for online monitoring while discussing the intersections of Dutch and EU legislation.

The discussion began with an overview of the Public Prosecutor's Office, its jurisdiction and mandate, and the division of responsibilities in terrorism cases at the national level. The presentation then moved to relevant Dutch legislation for counterterrorism, including sections of the Dutch Criminal Code covering training, incitement, evidence collection, and more.

International Centre for Counter-Terrorism (ICCT)

The second day started with a presentation from representatives of to the International Centre for Counter Terrorism (ICCT). The ICCT is an independent think tank which seeks to shape effective and evidence-based policies against terrorism and violent extremism. The discussion with the delegation focused on presenting the Foreign Terrorist Fighters (FTF) Knowledge Hub, an independent database that offers quantitative and qualitative data on FTFs who have joined terrorist or violent extremist groups in Syria and Iraq. Participants had the opportunity to understand how to use this tool, explore relevant country-specific data and discuss the impact of FTFs in North Macedonia.

Following the session, CILC facilitated discussions between the National committee for countering violent extremism and counter-terrorism from North Macedonia to initiate cooperation with the ICCT, aiming to establish a North Macedonia country chapter within the FTF Knowledge Hub.

Moreover, during this session, representatives from the ICCT presented the main outcomes of the project "Evaluation of Regulation (EU) 2021/784 addressing the dissemination of terrorist content online (TCO)" and the project "feasibility study on the development of an assessment framework for terrorist and borderline content online". Both projects examine the existing legal frameworks for online monitoring at the European level, equipping participants with a clearer understanding of how to align North Macedonia's legislation with the EU acquis.

Visit to Eurojust

Eurojust (the European Union Agency for Criminal Justice Cooperation) is responsible for coordinating the work of national authorities in investigating and prosecuting transnational crime. As part of their work, Eurojust also seeks to develop regulations and best practices regarding digital information exchange in terrorism cases. The discussion centered on the legal mechanisms available for detecting and monitoring terrorism and violent extremism and the role that Eurojust plays in supporting EU MS. It also provided an opportunity to learn more about the cooperation frameworks in place among EU MS and with non-EU countries. Representatives from Eurojust encouraged their counterparts from North Macedonia to make full use of the tools available to them and to strengthen their cooperation with Eurojust.

HORIZON CIVITAS
CILC Center for International Legal Cooperation
Netherlands - North Macedonia Counterterrorism Platform
Kingdom of the Netherlands

Visit to Europol

The visit to Europol focused on providing the delegation with an overview of the EU Internet Referral Unit (IRU). The EU IRU's mandate includes flagging content online and sharing these flags with relevant partners; supporting authorities with strategic and operational analysis; and acting as a European Centre of Excellence. Within the EU IRU, there are departments dedicated to Terrorist Propaganda Analysis & Referrals; Operations, Internet Investigations, and Technical Support; and Cross-border Access to e-Evidence & Knowledge Sharing. The presentation included discussions on online terrorism content, moderation, investigation, and referrals, forensic analysis, and how evidence gathered can be presented in court. Additionally, the representatives from the EU IRU's provided an overview of the PERCI system, a single system to connect all EU Member States and service providers for the facilitation of referrals and removal orders of content online.

The session finalized with the discussion on how to increase cooperation between Europol and North Macedonia and with a visit to the office of the Europol Liaison Officer for North Macedonia.

Delft municipality on local approach

Lili-Anne de Jongh, Policy Advisor, Care and Security Team of the Municipality of Delft, and Wies van Dipten, Process Coordinator, Care and Security Team of the Municipality of Delft, gave a presentation to the delegation on preventing and countering radicalisation from a local perspective. Incorporating the local perspective from the Netherlands was a key element of this study visit, as municipalities are often the first to detect early signs of radicalisation or extremist behavior and play a crucial role in implementing preventive measures. The municipality of the city of Delft in the Netherlands is an example of success at the local level.

As part of this session, representatives from the municipality discussed radicalisation and jihadism within Delft and how their office focuses on prevention, identification, and intervention. This included prevention classification models, methods to identify signs of radicalisation, educational, cultural, and training activities used to reduce chances of radicalisation, online youth work, possible interventions, and other tactics to build resilience within the community. A key takeaway was the importance of working together via a person-centred approach.

EVALUATION OF ACTIVITY

Feedback and impact

The study visit was organized to ensure continuation of the learning outcomes achieved during previous project activities, including the Trainings provided by the Dutch Police. The visit was well received by participants, who appreciated the opportunity to exchange best practices, discuss relevant information and to establish cooperation with relevant Dutch and European representatives. However, participants recommended extending the duration of future study visits to allow for more in-depth discussions with institutional representatives.

The North Macedonian National Coordinator for countering violent extremism and counter-terrorism expressed that the presentations provided were insightful and relevant to the context in North Macedonia as well as relevant for the implementation of a new unit/body for online monitoring in the country.

Problems encountered

On the first day of the study visit, the city of The Hague experienced a partial blackout, affecting the area where several public institutions are located, including the NCTV and The Hague Humanity Hub—the venue for the session on the legal framework and legislation for online monitoring in counterterrorism. As a result of the disruption, the scheduled dinner for that evening was cancelled. To accommodate participants, the project team provided an additional partial per diem to cover dinner expenses.

New/updated information

During the study visit, participants highlighted a concerning rise in violent radicalization among younger citizens. This trend appears to be significantly driven by the influence of digital platforms, including social media networks, online gaming environments, and encrypted messaging applications.

The Netherlands is facing similar challenges, with an increasing number of young individuals being exposed to and influenced by extremist content online. This shared concern presents a valuable opportunity for enhanced bilateral cooperation between North Macedonia and the Netherlands. Joint efforts could focus on developing early detection mechanisms, sharing intelligence and best practices, and designing targeted prevention strategies tailored to the digital behaviors of younger populations.

Such collaboration could also extend to capacity-building initiatives, including training for law enforcement and educators, the development of digital literacy programs, and the creation of counter-narrative campaigns aimed at building resilience among youth against online radicalization.

CONCLUSIONS AND RECOMMENDATIONS

The study visit successfully created a platform for participants to exchange experiences and best practices, compare their national approaches and legal frameworks for online monitoring of terrorist content (TCO) with those implemented in the Netherlands, and establish cooperation with relevant Dutch and EU agencies.

The visit also enabled participants to identify legislative gaps in North Macedonia's current framework for addressing TCO and explore potential tools and cooperation mechanisms that could enhance the country's efforts in combating terrorism and violent extremism online.

Following this visit, it is recommended to continue supporting North Macedonian authorities in establishing a dedicated unit or body focused specifically on online monitoring. As part of this ongoing support, the project team will organize two additional activities to further assist in this effort and set the basis for drafting a new regulation in the area:

- Expert Debate "investigating online extremism and human rights"
- Workshop on legislative adjustment of countering terrorist content online (TCO)

HORIZON CIVITAS
CILC Center for International Legal Cooperation
Netherlands - North Macedonia Counterterrorism Platform
Kingdom of the Netherlands

Activity Report

Expert debate: Investigating online extremism and human rights



April 2025

Prepared by
Samet Shabani

HORIZON CIVITAS
CILC Center for International Legal Cooperation
Netherlands - North Macedonia Counterterrorism Platform
Kingdom of the Netherlands

ACTIVITY REPORT

OVERVIEW

Project	Netherlands – North-Macedonia Counterterrorism Platform II (MK23081) *Activity implemented in scope of the DELETE project
Activity	Expert Debate: Investigating online extremism and human rights
Date	17.04.2025
Location	Skopje, North Macedonia
Panelists	Merlina Herbach, ICCT Besa Arifi, expert on criminal law Metodi Hadzi Janev, expert on security policies
Moderator	Samet Shabani

DESCRIPTION OF ACTIVITY

Objective

This activity aimed to bring stakeholders from public institutions, academia, CSOs with expertise on countering violent extremism, countering terrorism as well as human rights to discuss together about how should the current legal framework of North Macedonia be adjusted in order to limit the dissemination of terrorist and extremist content in the online sphere, meanwhile protecting human rights such as freedom of expression, personal data protection, and privacy.

Methodology and means of delivery

The activity was consisted of three main sessions:

1. Moderated discussion with presentation: Expert analysis about current legal frameworks of North Macedonia and the one of EU. The experts will offer comparisons, adjustments and recommendations.

2. World Café: proposals and recommendations from and for the religious stakeholders about preventing deviant phenomena: following the analysis, the participants provide their expert proposals and recommendation in three working tables (World Café method), each table consisting different thematic focus.

3. Plenary session: proposals and recommendations for the legal framework for online investigations of extremism: Facilitator of each working table present their discussion and recommendation points.

Narrative description of activity

The activity started with opening remarks by Samet Shabani, Horizon Civitas and Pavle Trajanov, National Committee for CVE and CT of North Macedonia. In his opening speech, Shabani stressed out that this activity and overall, the project is a concrete support to institutional capacities in countering online extremism. Mr Trajanov noted that the expectations from this activity and project are very high since it is addressing the interventions foreseen in the National Strategy for CVE and the Action Plan.

The activity continued with the session moderated discussion with presentations by Merlina Herbach, research fellow at International Center for Counter Terrorism (ICCT), Besa Arifi, expert on criminal law, and Metodi Hadzi Janev, expert on security policies.

Merlina Herbach, LLM, Research Fellow at the International Center for Counter-Terrorism, delivered a presentation titled "Regulating Terrorist Content Online," assessing Regulation (EU) 2021/794, adopted on 29 April 2021, which addresses the dissemination of terrorist content online (TCO Regulation). The presentation outlined the regulation's framework, implementation challenges, and recommendations for effective enforcement while safeguarding fundamental rights.

Key Points of the Presentation

1. Framework and Responsibilities:

- The TCO Regulation empowers competent EU authorities to issue removal orders (Art. 3), scrutinize them (Art. 4), oversee specific measures (Art. 5), and impose penalties (Art. 18).
- Hosting Service Providers (HSPs) are required to comply with removal orders, implement specific measures, retain data, ensure transparency, and provide user-information and appeal mechanisms.
- Users and civil society play active roles in flagging and moderating content and passive roles in protecting fundamental rights.
- Europol supports coordination through tools like the EU Internet Referral Unit (EU IRU) and the PERCI platform for processing removal orders.

2. Cross-Border Cooperation:

- Member States are encouraged to exchange information and coordinate to avoid duplicating removal orders and interfering with ongoing investigations.
- Europol facilitates swift information exchange and supports coordination with HSPs to minimize duplication and enhance efficiency.

3. Cross-Border Cooperation:

- Terrorists use online platforms for recruitment, networking, operational planning, and financing, necessitating robust regulation due to offline implications and the accessibility of terrorist content.
- Challenges include the failure of voluntary moderation, difficulties in enforcement by national authorities alone, user migration to less-regulated platforms, and the impact of new technologies.
- Small HSPs face unique challenges in implementation due to limited resources.

4. Side Effects:

- The regulation places a disproportionate burden on small and medium-sized HSPs.
- Certain services are excluded, leading to uneven implementation and enforcement across platforms.

5. Protection of Fundamental Rights:

- The regulatory framework emphasizes clearly defined content categories, alternative moderation actions, judicial oversight, transparency, and public accountability.
- Implementation requires outreach, cooperation, support for small platforms, non-discrimination, and procedural safeguards, including human oversight and appeal mechanisms.

6. Key Takeaways:

- Narrowly define terrorist content categories to ensure clarity.
- Establish centralized national authorities with clear mandates.
- Balance the scope of HSPs to ensure both quantity and quality of enforcement.
- Provide judicial review, transparency, and support for smaller HSPs.
- Foster outreach and cooperation to enhance implementation.

Besa Arifi's presentation addressed the significance of TCO, its impact on human rights, the national legal and strategic framework, institutional roles, strengths and weaknesses, and recommendations for improvement.

Key Points of the Presentation

1. Significance of Online Terrorist Content (TCO):

- TCO encompasses materials that incite, promote, or provide instructions for terrorist acts, as defined by EU Directive (2017/541). It excludes content for educational, journalistic, artistic, or counter-terrorism purposes.
- A study from 1 January 2019 to 15 July 2021 identified 2% of 1.29 million collected messages (20,670) as polarizing, hateful, or extremist, with political polarization (18,371 messages), ethnic hatred (2,299 messages, mainly between Macedonians and Albanians), and religiously motivated extremism (notably Salafi-jihadist content in Albanian on platforms like Facebook and Telegram) being prominent.
- Challenges include monitoring encrypted platforms like Telegram and subtle extremist messages that avoid explicit calls to violence.

2. EU Regulation (2021/784):

- Applies to Hosting Service Providers (HSPs) offering services in the EU, requiring non-EU providers to appoint an EU legal representative.
- Measures include:

- Removal Orders: Competent authorities can issue orders to remove TCO within one hour, specifying reasons, URLs, and remedies (Art. 3, 17).

- Specific Measures: HSPs must implement technical tools, user reporting mechanisms, and human oversight to prevent misuse

- Data Retention: Removed TCO and related data must be preserved for at least six months (Art. 6).

- Cooperation: HSPs must designate 24/7 contact points and collaborate with authorities, including Europol (Art. 14, 16, 17).

- Penalties: Fines up to 4% of global revenue for systematic non-compliance (Art. 18).

- Human rights protections include necessity, proportionality, non-discrimination, human oversight, complaint mechanisms, and judicial review to prevent excessive removal of legitimate content (Art. 1, 5, 9, 10, 23).

3. TCO in North Macedonia:

o Legal Framework:

- The Criminal Code addresses TCO indirectly through provisions like Art. 394-a (terrorist organization, 4-10 years imprisonment), Art. 394-b (terrorism, including electronic means, 4 years to life), Art. 394-g (spreading racist/xenophobic material online, 1-10 years), and Art. 322-a (participation in foreign wars, minimum 4 years, explicitly mentioning social media).
- The Law on Prevention of Money Laundering and Terrorism Financing supports efforts against online terrorist financing.

o National Strategies (2023-2027):

- The National Strategy for Countering Terrorism recognizes the internet as a key channel for terrorist propaganda and promotes a comprehensive approach, including counter-narratives, civil society collaboration, and rapid TCO removal (Goal 4.5).
- The Strategy for Preventing Violent Extremism identifies the internet as a "virtual arena for radicalization," focusing on capacity building, media literacy, social cohesion campaigns, and countering hate speech (Goal 1.4).
- Both emphasize human rights, proportionality, and transparency.

o Institutions:

- Key bodies include the National Committee for Countering Terrorism and Violent Extremism, Ministry of Interior (MoI) Computer Crime Sector, National Security Agency, Intelligence Agency, Ministry of Defense, and Agency for Audio and Audiovisual Media Services.
- A coordinated action led by the Public Prosecutor's Office for Organized Crime and Corruption, involving the MoI and National Security Agency, targeted Telegram groups sharing extremist content, leveraging digital forensics.

4. Strengths and weaknesses:

o Strengths:

- Existing legal provisions indirectly address TCO, with efforts to align with EU Regulation (2021/784).
- National strategies explicitly recognize TCO and promote human rights protections, counter-narratives, and cooperation with Europol and EU action plans for the Western Balkans.
- Institutional frameworks and planned capacity building within the MoI and National Committee.

o Weaknesses:

- Lack of a specific TCO definition and legal deadlines (e.g., one-hour removal requirement).
- No proactive obligations for HSPs to remove TCO.
- Insufficient human rights protections during content removal.
- Absence of a dedicated TCO unit, leading to fragmented coordination.
- Limited technical capacity for monitoring encrypted platforms and insufficient specialized training for online investigations.

5. Recommendations:

- Legislation: Amend the Criminal Code to define TCO explicitly, aligning with EU Regulation (2021/784), and establish a one-hour removal deadline with clear procedures.
- HSP Obligations: Introduce regulations requiring HSPs to proactively remove TCO, enhancing platform accountability.
- Human Rights: Develop mechanisms for complaints, judicial review, and transparency to protect freedom of expression and prevent excessive content removal.
- Institutional Capacity: Establish a dedicated TCO unit, enhance inter-agency coordination, and invest in technical tools for monitoring encrypted platforms.
- Training: Provide specialized training for security personnel on online investigations and digital evidence.

6. Conclusion:

- North Macedonia has a foundational framework for addressing TCO, with relevant laws, strategies, and institutions. However, gaps in specific TCO regulations, institutional coordination, and technical capacity hinder effectiveness. Implementing the proposed recommendations would align RNM with EU standards, enhance public security, and safeguard human rights.

HORIZON CIVITAS
CILC Center for International Legal Cooperation
Netherlands - North Macedonia Counterterrorism Platform
Kingdom of the Netherlands

Prof. Metodi Hadzi-Janev had a speech focusing on some existing challenges in national level about proceeding with penalizing terrorist content online (TCO). His remarks include:

- The challenge of 'cultural relativism' when it comes to terrorism (the perception on terrorism in certain society might be different at another society), or subjective interpretation of the definition of terrorism by the state actors. It is crucial to firstly have a clear set of institutional definition of what terrorism.
- With the new digital facilities, conditions in place, terrorism is evolving to a more sophisticated question. It is very important to raise institutional capacities accordingly.
- Focusing only in usual media (traditional and social media) online may not be enough to complete 'the puzzle' when investigating terrorist content.
- The young generation of terrorists create new trends of connections in internet (video games used for encrypted messaging, special online chatting spaces). It is of utmost important that institutions know those new trends, and accordingly address them.
- The lack of private forensic institute in the country in case the person being charged for terrorist content online request further investigation of proves by Prosecution.

Following the moderated discussions, participants provided their proposals and recommendations for legislation adjustments. The summary of the discussions and presented work is as follows:

Criteria for Categorizing Extremist Content as "Terrorist"

- Incitement to Violence: Calls for violent acts to achieve political, ethnic, religious, or ideological goals
- Ideological Motivation: Promotion of extremist ideologies like jihadism, neo-Nazism, or ethnic hatred to undermine state institutions or create fear.
- Radicalization and Recruitment: Content that radicalizes individuals or recruits for terrorist organizations
- Threats and Propaganda: Public threats, spreading fear, or propaganda linked to recognized terrorist groups
- Operational Support: Providing instructions for attacks, explosives, or guerrilla tactics.
- EU Regulation Reference: EU's TCO Regulation, defining terrorist content as enabling, supporting, or threatening terrorist acts.

Keywords to Flag Terrorist Content

- Violence and Militancy: "Attack," "bomb," "explosion," "liquidation," "massacre," "jihad," "martyr," "shahid"
- Weapons and Explosives: "Bomb," "C4," "IED," "AK-47," "explosive belt"
- Ideological Terms: "Caliphate," "kafir," "takfir," "holy war," "Islamic state"
- Terrorist Groups/Symbols: "ISIS," "Al-Qaeda," "Taliban," "black flag".
- Coordination Terms: "Operation," "target," "coordinates," "mission".
- Context Caution: One participant warned that keywords alone are insufficient without context, as terrorists adapt language to evade detection.

Role of Civil Society and Human Rights Advocates

- Monitoring and Reporting: Track law implementation, document abuses, and report to national/international bodies
- Advocacy and Legal Aid: Provide legal support for those unfairly targeted and challenge discriminatory practices.
- Public Education: Raise awareness about rights, distinguish extremism from dissent, and promote transparency.
- Policy Involvement: Participate in law-making and advocate for human rights protections
- Collaboration: Work with media, international NGOs, and institutions to ensure accountability.

Security Sector Needs for Monitoring Terrorist Content

- Technology: AI/ML tools for detecting content, big data analytics, and monitoring encrypted platforms.
- Trained Personnel: IT experts, analysts trained in radicalization, and culturally sensitive staff
- Legal Frameworks: Clear laws aligned with human rights to regulate monitoring and data use
- Coordination: Collaboration between police, intelligence, judiciary, and media regulators
- Tech Company Partnerships: Mechanisms for content removal and information sharing with platforms.
- Specific Needs: Emphasized proactive monitoring to prevent radicalization, collect evidence, and disrupt terrorist communications.

HORIZON CIVITAS
CILC Center for International Legal Cooperation
Netherlands - North Macedonia Counterterrorism Platform
Kingdom of the Netherlands

Institution to House a Terrorist Content Monitoring Unit

- MOI (Ministry of Interior): Preferred by majority of participants for its resources, cybercrime expertise, and investigative authority. Three suggests coordination with the National Committee for Countering Violent Extremism and Terrorism.
- NSA (National Security Agency): One suggested NSA, citing their security expertise.
- AVMU (Agency for Audio and Audiovisual Media Services): One suggested proposes AVMU for its media expertise, but AVMU representative notes it lacks investigative capacity.
- Multi-Sector Body: One participant suggested a joint body with representatives from MVR, AVMU, and the National Committee for balanced oversight.
- Rationale: MOI's resources, legal authority, and public accountability make it suitable, while the National Committee ensures multi-sector coordination. AVMU and JO (Public Prosecutor's Office) are seen as secondary due to limited operational roles.

Private Sector Role via Public-Private Partnership (PPP)

- Feasibility: Almost all participants support PPP model for monitoring TCO, citing private companies' advanced AI, real-time monitoring, and expertise in media analysis.
- Examples: One participant noted platforms are developed by private companies, while another highlights their role in detecting hate speech and disinformation.
- Concerns: One participant emphasized risks requiring careful regulation. Another one opposes PPPs locally, citing inefficiencies and risks to neutrality, though he acknowledges EU projects like "Technology Against Terrorism."
- Conditions: Transparency, democratic oversight, and human rights compliance are critical.

Judicial Oversight to Prevent Abuse

- Court Approval: Require judicial warrants for monitoring private communications or removing content.
- Periodic Audits: Courts or independent bodies should review monitoring practices to ensure compliance.
- Right to Appeal: Citizens must have access to judicial review for unlawful monitoring
- Transparency: Public reporting on monitoring activities and legal frameworks to prevent censorship.
- Ombudsman Role: One participant suggests the Ombudsman can enhance democratic oversight and human rights protection.
- Specific Measures: One participant proposes judicial approval for sensitive actions like account blocking or data access.

Key Observations

Consensus: Content must incite violence or support terrorism to be "terrorist." Keywords are useful but require contextual analysis. Civil society plays a critical role in oversight and advocacy. The security sector needs advanced tech and trained staff. MOI is the preferred institution for a monitoring unit, with private sector involvement viable under strict regulation. Judicial oversight is non-negotiable to prevent abuses.

EVALUATION OF ACTIVITY

Feedback and impact

The expert debate was well-received by participants, who appreciated the opportunity to engage in a multi-stakeholder dialogue on countering online extremism while safeguarding human rights. The national coordinator expressed that the presentations were insightful and relevant to North Macedonia's context.

The event strengthened collaboration between public institutions, academia, and civil society, laying the groundwork for future cooperation on legal and institutional reforms. Participants highlighted the practical recommendations, such as amending the Criminal Code and establishing a dedicated TCO unit, as actionable steps toward aligning North Macedonia's framework with EU standards. The activity also raised awareness about the need for judicial oversight and human rights protections, influencing ongoing policy discussions within the National Committee for Countering Violent Extremism and Terrorism.

Problems encountered

Despite the overall success, several challenges were noted. Limited representation from smaller Hosting Service Providers (HSPs) hindered discussions on their specific implementation challenges under EU Regulation (2021/784).

Additionally, some participants expressed concerns about the short duration of the event, which constrained in-depth exploration of complex issues like monitoring encrypted platforms. Divergent views on the lead institution for a TCO monitoring unit (e.g., Ministry of Interior vs. multi-sector body) led to unresolved debates, requiring further consultation.

New/updated information

The activity revealed new insights into the evolving nature of online extremism in North Macedonia. Participants shared recent data indicating a rise in extremist content on gaming platforms and encrypted chat applications, underscoring the need for advanced monitoring tools. Discussions also highlighted the emergence of subtle extremist narratives that avoid explicit violence, complicating detection efforts. The event updated stakeholders on North Macedonia's progress toward aligning with EU Regulation (2021/784), with the Ministry of Interior reporting ongoing efforts to enhance digital forensics capabilities. Additionally, a pilot project involving public-private partnerships for AI-based content monitoring was mentioned as a potential model, though it remains in early stages. These updates emphasized the urgency of addressing technological and legal gaps to counter evolving threats effectively.

HORIZON CIVITAS
CILC Center for International Legal Cooperation
Netherlands - North Macedonia Counterterrorism Platform
Kingdom of the Netherlands

CONCLUSIONS AND RECOMMENDATIONS

The expert debate successfully facilitated a comprehensive dialogue on balancing the fight against online extremism with human rights protections in North Macedonia. The presentations and discussions underscored that while North Macedonia has a foundational legal and strategic framework, significant gaps remain in defining terrorist content online (TCO), establishing proactive obligations for Hosting Service Providers (HSPs), and ensuring robust human rights safeguards. The evolving nature of online extremism, including the use of encrypted platforms and gaming spaces, demands enhanced technical and institutional capacities. Consensus emerged on the need for clear TCO definitions, judicial oversight, and inter-agency coordination, with the Ministry of Interior identified as the most suitable lead for a TCO monitoring unit. However, the debate also highlighted challenges, such as resource constraints for smaller HSPs and the need for careful regulation of public-private partnerships to prevent abuses. The activity reinforced the importance of civil society's role in advocacy and oversight to ensure transparency and accountability.

Recommendations

1. Legislative Reforms:

- Amend the Criminal Code to explicitly define TCO, aligning with EU Regulation (2021/784), and include a one-hour removal deadline for HSPs.
- Introduce proactive obligations for HSPs to monitor and remove TCO, with clear penalties for non-compliance.
- Develop legal mechanisms for complaints, judicial review, and transparency to protect freedom of expression and prevent excessive content removal.

2. Institutional Capacity Building:

- Establish a dedicated TCO monitoring unit within the Ministry of Interior, with coordination mechanisms involving the National Committee for Countering Violent Extremism and Terrorism.
- Invest in AI-based tools and big data analytics to monitor encrypted platforms and detect subtle extremist content.
- Provide specialized training for security personnel on online investigations, digital forensics, and cultural sensitivities.

3. Human Rights Protections:

- Implement judicial oversight mechanisms, including warrants for monitoring and periodic audits by courts or independent bodies.
- Ensure citizens have access to appeal processes for unlawful monitoring or content removal.
- Engage civil society in policy-making and monitoring to enhance transparency and accountability.

4. Public-Private Partnerships:

- Develop regulated PPP frameworks to leverage private sector expertise in AI and real-time monitoring, ensuring compliance with human rights standards.
- Support smaller HSPs with resources and training to meet TCO regulation requirements.

5.Public Awareness and Collaboration:

- Launch public education campaigns to raise awareness about online extremism and distinguish it from legitimate dissent.
- Foster cross-border cooperation with EU bodies like Europol and regional partners to share intelligence and best practices.
- Encourage multi-stakeholder forums to sustain dialogue between institutions, civil society, and the private sector.

Activity Report

Workshop on Legislative Adjustment for Countering Terrorist Content Online (TCO)



May 2025

Prepared by
Samet Shabani

HORIZON CIVITAS
CILC Center for International Legal Cooperation
Netherlands - North Macedonia Counterterrorism Platform
Kingdom of the Netherlands

ACTIVITY REPORT

OVERVIEW

Project	Netherlands – North-Macedonia Counterterrorism Platform II (MK23081) *Activity implemented in scope of the DELETE project
Activity	Workshop on Legislative Adjustment for Countering Terrorist Content Online (TCO)
Date	15.05.2025 - 16.05.2025
Location	Popova Sapka, North Macedonia
Panelists	Pavle Trajanov, NCCVECT Diana Navarrete, CILC Metodi Hadzi Janev, expert on security policies
Facilitator	Samet Shabani, Horizon Civitas
Assistants	Necla Uludag and Jetmir Ziba

DESCRIPTION OF ACTIVITY

Objective

The workshop aimed to support the development of legislation in North Macedonia aligned with the EU Regulation (2021/784) on countering terrorist content online (TCO). It sought to mobilize public institutions, academia, civil society, and the business sector to propose amendments to the national legal framework to limit the spread of terrorist and extremist content online while protecting human rights, including freedom of expression, data protection, and privacy. The activity focused on fostering a balanced approach to countering online extremism through expert discussions and collaborative drafting of a regulatory framework.

Methodology and means of delivery

The workshop consisted of two main components delivered over two days:

1. Expert sessions: Three thematic sessions were held:

- Institutional Framework for Countering Online Extremism: Focused on the National Strategy for Countering Violent Extremism (CVE) and Counterterrorism (CT).
- Presentation of draft Needs Assessment Report (NAR): Expert findings and recommendations shared with stakeholders.
- Sharing Practices from EU countries: Highlighted best practices in legislative alignment with EU standards.

2. Recommendations for Draft Regulation: Included small group work and plenary sessions to prepare a draft Regulation on Countering Terrorist Content Online, incorporating inputs from diverse stakeholders.

Narrative description of activity

The workshop began with a welcome coffee and check-in, followed by opening remarks from Diana Navarrete (Center for International Legal Cooperation), Samet Shabani (Horizon Civitas), and Pavle Trajanov (National Committee for CVE and CT). They emphasized the importance of aligning North Macedonia's legal framework with EU standards while safeguarding human rights.

Session 1: Institutional Framework for Countering Terrorist Content Online:

Pavle Trajanov presented the National Strategy for CVE and CT, outlining institutional roles in combating online extremism, including coordination challenges and the need for updated legal provisions to address technological advancements.

Session 2: Global Legislative Map:

Participants were introduced with the Global Legislative Map, a tool proffered by Global Internet Forum to Counter Terrorism, containing legislative framework and practices of mostly EU countries in addressing the countering of terrorist content online (TCO).

Session 3: Presentation of draft needs assessment report (NAR):

Experts Metodi Hadzi Janev and Samet Shabani presented the draft finding and recommendations coming out from the previously implemented activities (National Forum: Religion and Online Challenges, as well as Expert Debate on TCO in North Macedonia), and overall the needs assessment report (NAR).

The day concluded with a summary of key points and preparations for the drafting sessions.

The second day started with a recap of Day 1. Participants then engaged in small group work to draft the Regulation on Countering Terrorist Content Online, focusing on three thematic areas: human rights, security policies, and legislative aspects. Groups addressed questions on balancing freedom of expression, protecting privacy, aligning with EU regulations, and preventing abuse of authority.

A plenary session consolidated the group outputs into a draft regulation, followed by discussions on next steps, including institutional coordination and public consultations. The workshop concluded with agreement on actionable recommendations to advance the legislative process.

EVALUATION OF ACTIVITY

Feedback and impact

The workshop was well-received, with participants valuing the multi-stakeholder approach that included public institutions, civil society, and academia. The discussions highlighted the need for precise legal definitions, independent oversight, and technological tools to counter online extremism effectively. The event strengthened coordination between stakeholders and provided a foundation for aligning North Macedonia's legal framework with EU standards. Recommendations, such as establishing independent oversight bodies and training programs, were seen as practical steps toward enhancing national capacities.

Problems encountered

Challenges included limited technical expertise among some participants to address advanced technological issues, such as encrypted platforms and algorithmic monitoring. The short duration of the workshop constrained in-depth discussions on complex topics like digital forensics. Representation from smaller online platforms was limited, reducing perspectives from the business sector.

New/updated information

The workshop revealed emerging challenges, including the use of encrypted platforms and social media for terrorist recruitment, particularly among marginalized groups. Participants noted an increase in cyberattacks on state institutions and critical infrastructure, underscoring the need for enhanced digital forensics and inter-agency coordination. The discussions also highlighted the importance of international cooperation, particularly with EU agencies like Europol, to bolster North Macedonia's investigative capacities.

CONCLUSIONS AND RECOMMENDATIONS

The workshop successfully facilitated a collaborative dialogue on developing a legal framework to counter terrorist content online while protecting human rights. It underscored the need for clear definitions, independent oversight, and technological advancements to address online extremism effectively. Gaps in technical capacity, inter-agency coordination, and engagement with online platforms were identified as areas for improvement.

Recommendations

1. Human rights:

- Ensure the legal framework includes precise definitions for "extremism," "radicalization," and "terrorist content" to avoid overreach.
- Incorporate principles of proportionality and necessity, with judicial oversight to protect freedom of expression and prevent censorship based on ideological or political views.
- Establish independent oversight bodies to monitor data collection and content removal, ensuring transparency through public reports.
- Provide human rights training for security agencies and promote data minimization principles to protect privacy.
- Involve civil society and human rights advocates in monitoring implementation through a dedicated oversight commission.

2. Security Policies:

- Address technological challenges (e.g., encrypted platforms) by adopting automated detection systems, hash-matching technologies, and interoperable data-sharing platforms.
- Enhance inter-agency coordination through a situation center under the Ministry of Interior (MoI) for regular information exchange.
- Strengthen international cooperation with EU agencies like Europol for intelligence sharing, training, and technical support.
- Develop clear criteria for proactive monitoring of online platforms, ensuring judicial control to avoid mass surveillance.

3. Legislative Aspects:

- Establish a dedicated unit under the MoI's Terrorism Sector for monitoring terrorist content online, with defined roles for cooperation with digital platforms and other agencies
- Introduce a new criminal offense in the Criminal Code, such as "Digital Dissemination of Terrorist Content," to address legal gaps without requiring a separate regulation.
- Ensure judicial oversight through specialized judges or trained judicial panels to balance executive actions with legal accountability.
- Introduce penalties (e.g., fines, up to 3 years imprisonment) and incentives (e.g., liability exemptions for timely content removal) for online platforms to encourage compliance without excessive regulatory burdens.



> **Recommending the good and preventing from the evil in digital space is a must for modern societies and governments.**

Contact Details:

Emails: **hadzijanev@gmail.com**
samet.sh@horizon.mk

Website: **www.horizon.mk**

HORIZON CIVITAS

CILC Center for International Legal Cooperation

Netherlands - North Macedonia Counterterrorism Platform

Kingdom of the Netherlands