Addressing terrorist and other violent extremist actors' misuse of social media for the achievement of strategic purposes in the COVID-19 era

The project will help monitor, detect, investigate and raise awareness of violent extremist actors' misuse of the Internet and social media for strategic purposes, including by analysing the impact that COVID-19 has had on their overall propaganda, recruitment and fundraising techniques.

Description of the Project

The project aims to identify, explore and raise awareness of ways in which terrorists and other violent extremist actors are exploiting social media platforms to achieve their strategic purposes and to assess the impact COVID-19 has had on their overall propaganda, incitement, recruitment and fundraising techniques. It also seeks to enhance the capacity of law enforcement and prosecutorial agencies in 5 selected countries of Western Balkans (Albania, Bosnia & Herzegovina, Montenegro, North Macedonia, and Serbia) to investigate and subsequently prosecute, acts of propaganda and incitement to violence via social media and to identify COVID-19 disinformation and misrepresentation campaigns.

More specifically, the project foresees three main work streams of engagement and implementation: (a) monitoring misuse of social media by terrorist and other violent extremist actors and evaluating new potential threats, emerging trends, synergies and complementarity in the strategic approach; (b) awareness raising initiatives to increase knowledge and understanding of violent non-state actors' propaganda, incitement and fundraising techniques as well as measures to avoid detection; (c) training law enforcement and prosecutorial agencies to detect, investigate and subsequently prosecute, acts of propaganda and incitement to violence through social media and to identify disinformation and misrepresentation campaigns aimed at jeopardizing the efficacy and credibility of governments' response measures during the COVID-19 crisis. While the first two work streams will have a global dimension, the third one on capacity-building will have a regional focus.

Rationale

Member States continue to face a significant threat from the abuse of information and communications technology (ICT) by violent non-state actors, particularly terrorist and other violent extremist entities, such as 'white supremacist', 'far-right', 'extreme right-wing', or 'racially and ethnically motivated' movements. The exploitation of the Internet and social media platforms has enabled ISIL, Al-Qaida, their affiliates, sympathizers and supporters all over the world to spread propaganda, share training materials, engage in the illicit trade in weapons, identify potential recruits, generate funds and carry out attacks. Messages are conveyed through not only mainstream social media applications but also encrypted channels and the dark web. In numerous resolutions, and, notably, resolutions 2354 (2017) and 2396 (2017), the Security Council has expressed concern over the misuse of ICT-related technology by terrorists to achieve their strategic purposes. Although not new, the COVID-19 crisis has further increased terrorist radicalization, recruitment and fundraising-related phenomena through social media platforms and encrypted messaging apps.

UNICRI's preliminary analysis and monitoring results contained in the report "Stop the Virus of Disinformation" shed light on how terrorist, violent extremist and organized criminal groups have been trying to take advantage of the pandemic and related side effects such as, social isolation, generalized sense of anxiety and uncertainty and lack of opportunities to undermine trust in governments and, at the same time, to reinforce extremist narratives and strategic purposes. According to the Analytical Support and Sanctions Monitoring Team, ISIL has had a captive audience during the lockdown and, if it has successfully used this for planning and recruitment purposes, it is possible that the easing of restrictions in non-conflict zone will see a spike in attacks once targets become available again.

Through this project and UNICRI's overall strategy, Member States will have an enhanced understanding of the phenomenon and of the measures to successfully address the related threat. The 5 selected Member States – in which the Train-the-Trainer work stream will be piloted – will have improved capabilities to effectively monitor, detect and prosecute violent non-state actors' misuse of the Internet and social media and will be able to pass on such skills to their peers by training them systematically. This project will be able to address technical assistance needs identified in CTC/CTED assessments of both Bosnia & Herzegovina and Serbia.

Outcomes

The project seeks to achieve the following outcomes:

Outcome 1: Improved understanding of the misuse of social media by terrorist and other violent extremist actors and of the impact of COVID-19 in that regard.

Outcome 2: Counter-terrorism, law enforcement, intelligence and prosecutorial agencies and, to a certain extent, Internet/social media providers, civil society and international organizations possess an improved understanding of techniques used by violent non-state actors to achieve their strategic purposes and to avoid detection and integrate such knowledge in their daily operations and/or mandate.

Outcome 3: Key national stakeholders in the beneficiary countries involved (Albania, Bosnia & Herzegovina, Montenegro, North Macedonia, and Serbia) – in different capacity – in the investigation, detection and prosecution of violent non-state actors' misuse of the Internet and social media deploy the analytical and investigative skills acquired through the training in their daily operations and contribute to enhance the capacity of other peers by training them.

Outputs/Indicative Activities

The project seeks to achieve the following outputs through implementing the indicative activities below:

Output 1: A trend alert report based on the analysis of concrete case studies collected through the monitoring of terrorist and extremist content/activity online to identify and explore: (i) their strategic purposes, emerging threats and developments as well as synergies, similarities and differences in their approach; and (ii) the impact COVID-19 has had on their overall propaganda, incitement, recruitment and fundraising techniques.

- Monitor misuse of social media by terrorists and other violent extremist actors;
- Carry-out desk-based research and analysis and collect case studies;
- Gather data and information on techniques used to create echo-chambers, spread disinformation and avoid detection;
- Identify and evaluate new potential threats, emerging trends, synergies and complementarity in the strategic approach adopted by both terrorist and other extremist actors;
- Assess the impact of the pandemic on their narratives, recruitment and fundraising strategies;
- liaise with key stakeholders in law enforcement, counter-terrorism agencies, security services in Member States, International Organizations, Internet and social media providers and academia to complement desk-based activities; and
- Draft a trend alert report to highlight the main results of the monitoring, research, data collection and analysis.

Output 2: National and regional awareness raising events; dissemination of the main results of the trend alert report

- Organize regional and national awareness raising events with key stakeholders from the government, private sector, international organizations and academia.

Output 3: Tailored and context-specific training material based on the different technical assistance needs of trends and threats in each State; delivery of train-the-trainer courses to law enforcement and prosecutorial agencies.

- Collect and analyse case studies related to investigation and prosecution of on-line crime, highlighting innovative investigative techniques or prosecution strategies;
- Develop and deliver train-the-trainer courses on evidence collection, preparation of case files, application of relevant legislation without violating freedom of expression, evidence before sentencing.

Human Rights Mainstreaming

The design and implementation of the project is in line with recommendations and guidelines provided by international tools and good practices that promote the protection of human rights, gender equality and the rule of law, as a fundamental basis for the fight against terrorism. As such, the project would incorporate several elements designed to assist Member States and other interested stakeholders to, inter alia, use social media content relating to terrorism as digital evidence for investigation and prosecution, in compliance with human rights and fundamental freedoms and consistent with their obligations under domestic and applicable international law; and to ensure respect for the data subjects' right to freedom from arbitrary or unlawful interference with privacy as well as freedom of expression.

Gender Mainstreaming

The project will assess and pay special attention to the gendered dimensions of the problem, including by identifying issues that may hinder equal participation of both men and women in the different contexts. A balanced ratio of male to females will be encouraged and all-male panels in conferences and workshops will not take place within the project. Gender-based indicators will be developed and included in the logical framework and gender-related data will be continuously monitored throughout implementation, supporting a gender analysis as part of the project's overall evaluation.

Budget
$1,123,446.00

Pillar
Pillar I -Addressing the Conditions Conducive to the Spread of Terrorism, Pillar II -Measures to prevent and Combat Terrorism

Project Status
Concept

Implementation Period
2021-2024

UN Org
UNICRI

UN Global CT Compact Partners
CTED, INTERPOL

Countries
Albania, Bosnia & Herzegovina, Montenegro, North Macedonia, Serbia

Current Donors
This project is currently unfunded.