Deliverable Nº
6.1

MINDb4ACT

Critical Technologies and Social Innovation Schemes Report

WP6 'Society in action: co-design of validated pilot projects'

Deliverable details	
Work package	WP6
Deliverable number	D6.1
Nature	Report
Lead contractor for the document	European Organisation for Security (EOS)
Author(s)	Elodie Reuge (EOS)
Contributing consortium partners	ELCANO, GUCI, CENTRIC, SYNYO
Reviewer(s)	Rosalía Machin Prieto (ENLETS)
Due date:	30/11/2019
Delivered date:	29/11/2019
Dissemination level	Public
Pages	61

DISCLOSURE STATEMENT:

No part of this document may be used, reproduced and/or disclosed in any form or by any means without the prior written permission of the MINDb4ACT Consortium.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 740543.

Abstract

MINDb4ACT stands for Mapping, IdentifyiNg and Developing skills and opportunities in operating environments to co-create innovative, ethical and effective ACTions to tackle radicalisation leading to violent extremism. The consortium is composed of 7 Law Enforcement Agencies, Think-Tanks, Research Centres, Universities, Industry Associations and NGO's. MINDb4ACT is contributing improvements to current counter-violent extremism policies (CVEs) in the countries represented in the consortium, as well as in the new generation that will connect through collaborative ecosystems to co-design interventions. MINDb4ACT will be exclusively focused on "developing policy recommendations and practical solutions for end-users."

Index

Executive Summary

In the deliverable 6.1, MINDb4ACT focused on critical technologies and social innovative solutions. At the end of the report, the list of the critical technologies (Annex 2), the list of Innovative social initiatives (Annex 3), the critical technologies SWOT analysis (Annex 4) and the social innovations SWOT analysis (Annex 5) can be found. The partners who collected the needed information and filled in the excel sheets were the following:

- SYNYO: Austrian enterprise focused on research, innovation and technology,
- ELCANO: Spanish think tank specialized in international and strategic studies conducted from a Spanish, European and global perspective,
- CENTRIC: UK multi-disciplinary and end-user focused center of excellence, located within Sheffield Hallam University,
- GUCI: Spanish Civil Guard, which is the oldest law enforcement agency covering the entire country and
- EOS (leading the Deliverable): European organization for security, representing the voice of the European security industry and research community.

The diversity of the partners expertise, profile and nationalities ensures that the research undertaken covers a wide spectrum. The industrial background of EOS allows the organization to provide a thorough analysis of the data collected.

Document Context

The WP6, ‘Society in action: co-design of validated pilot-projects’, fosters “Knowledge Partnerships” through participation and civic engagement. As per DoW, the WP:

a) builds on assessment of skills and needs (Organizational evaluation tool) of LEAs and agencies involved in each pilot project
b) maps current and future application of technologies and social innovations (like grassroots initiatives)
c) ethnographic study of contexts on which pilot projects are being developed
d) organizes and develops the planning cells for implementation of pilot projects.”

T6.1 develops a list of critical technologies and social innovations that have the potential to be applied as part of counter-radicalisation policies, with the participation of the industry and of social innovation experts. This task is focused on improving the consortiums understanding of the radicalisation process and increasing the potential for identifying the early stages of radicalisation and opportunities for intervention.

Purpose of the document

The document D6.1, the Critical Technologies and Social Innovation Schemes Report, maps the current and future application of technologies and social innovations, and will ultimately contribute to fostering “Knowledge Partnerships” through participation and civic engagement. The key issue of the paper is to analyse the current trends in technology and how they can be adapted to the real needs of the LEAs.

Methodology

According to the description presented in the DoW, the partners involved in Task 6.1 gathered information and created a list of critical technologies[1] and social innovation initiatives directly applicable to CVE (Annexes 2 and 3).

Then, a SWOT analysis was applied to examine the selected technologies in order to identify those **most relevant** to LEAs. The resulting list (Annexes 4 and 5) is considered a “technology push” for future technological and innovative capabilities that match the emerging and future needs of LEAs.

The information that has been analysed includes the application of big data technologies for enhancing the approach that the consortium takes towards the radicalisation process and its potential for identifying the early stages of radicalisation and opportunities for intervention. **The research sources used by the partners involved in D6.1 include academic literature, police interview reports, court proceedings, prison**

[1] With *critical technologies,* the consortium refers to the technologies essential or key for the development of the technologies used in Security, especially those relevant for early detection or prevention of violent extremism. Critical can also be understood as « emerging disruptive » in the sense that they are expected to have a large impact but currently the level of development is still low.

records, intelligence agency reports, government assessments and other open sources to build a richer picture of the radicalisation issues that MINDb4ACT addresses, throughout Member States.

As there are a broad range of security technologies and social innovation projects being run at the EU and global level, the framework for collecting information was limited to the context established by the content and the objectives of the project, which aims to develop new approaches for CVE policies and practices.

Hence, the critical technologies and social innovation schemes collected have a clear impact on CVE (understood as mentioning either CVE, CR, or deradicalisation)[2].

The information has been collected through a pre-structured template sent by EOS (Annex 1). All relevant information for researchers, policymakers and practitioners will be, after the submission of this report, shared through the MINDb4ACT Platform developed by SYNYO and organized through Living Labs.

The excel sheet is structured as follows:

CRITICAL TECHNOLOGIES

- Name of the technology
- Description
- Provider (Manufacturer)
- Location of the Provider
- Technology Field (Social Media Analysis, Big Data Analysis, Virtual Reality)
- Technology Methodology (Web crawling, Decision Support)
- Technology Platform (Windows, Linux, Mac Osx, Android, IOS…)
- Technology License (Open Source, Mixed Source, Closed Source (proprietary))
- Technology Availability (Free, Paid)
- URL of Technology
- Operationalisation in the EU (Is the technology already being used in EU Member States? Where? By Whom ? Impacts? Next steps?)
- SWOT Analysis
  - STRENGTHS
    - Source URLs for Strengths (include links to source of analysis)
  - WEAKNESSES
    - Source URLS for Weaknesses (include links to source of analysis)
  - OPPORTUNITIES
    - Source URLS for Opportunities (include links to sources of analysis)
  - CHALLENGES

As per definition, this includes all forms of extremism.

            - Source URLs for Challenges (include links to source of analysis)
- Entry Added by XX (MINDb4ACT Partner name)

SOCIAL INNOVATION

- Name of social innovation initiative
- Description
- Provider
- Location of the Provider
- Social Innovation Field (Intelligence/information sharing, Education/skills development, Business funding, Counter-narratives, Policy Engagement…)
- Social Innovation Target Audience (Children, Youth, Women, Men, Prisoners, Returning Fighters, All…)
- URL of Social Innovation
- Operationalisation in the EU (Is the social innovation initiative already being implemented in EU Member States ? Where ? By Whom ? Impacts? Next steps?)
- SWOT Analysis
    - STRENGTHS
        - Source URLs for Strengths (include links to source of analysis)
    - WEAKNESSES
        - Source URLs for Weaknesses (include links to source of analysis)
    - OPPORTUNITIES
        - Source URLs for Opportunities (include links to source of analysis)
    - CHALLENGES
        - Source URLs for Challenges (include links to source of analysis)
- Entry added by XX (MINDb4ACT Partner name)

After collecting the required information from the partners, EOS analysed the current trends in technology and how they are adapted to the real needs of LEAs.

The critical technologies presentation

Geographical data

In total, 31 technologies considered as critical by the partners have been listed (Annex 2). 24 of them have been analysed through the SWOT method (Annex 4). From the ones analysed, 13 are from European providers, 9 are from non-European providers and 2 of the providers can be considered as global entities. From the European providers technologies, 2 (developed as part of the COPKIT project) are still under development (with the purpose of being operationalized in the EU) and 11 are listed as operating in the EU. Concerning the technologies developed by non-European providers, 5 can be found in the EU, while for 4 of them the information has not been indicated. As for the technologies coming from the providers with a largest geographical spectrum, 1 is operational in the EU and the information is not available for the second one.

Technological data

The technological data has been divided into five main layers: technology field, technology methodology, technology platform, technology license and technology availability.

From the wide range of **technology fields** noted here, *Data Visualization and processing* and *Big Data analysis* are most frequently encountered. Most of the technologies listed indicate more than one technology field:

- Data visualization and processing (6 technologies)
- Big data analysis (5 technologies)
- Social Media analysis (3 technologies)
- OSINT analysis (2 technologies)
- Threat intelligence (2 technologies)
- Cyber Threat Intelligence (2 technologies)
- Cyber Threat intelligence (1 technology)
- Advanced Persistent Threat (1 technology)
- Graph mining (1 technology)
- Information retrieval (1 technology)
- Machine learning (1 technology)
- Surveillance, Detection, Investigation (1 technology)
- Surface web and dark web monitoring (1 technology)
- Individual identification (1 technology)
- Counter advanced, known and new cyber-attack (1 technology)
- Human intelligence operations (1 technology)
- Data matching (1 technology)
- Cyber Intelligence/security-Satellite monitoring (1 technology)
- GSM and Wi-Fi monitoring (1 technology)
- Lawful interpretation (1 technology)
- Effectiveness Evaluation (1 technology)

A long and diversified list of **Technology methodologies** has also been indicated here. *Decision support* (2 technologies), *surface web and darknet through avatar* (2 technologies) and *Process information into actionable intelligence* (6 technologies - linked to the Data visualization and processing field) are the most common methodologies in the table. The other listed are only linked to one technology field:

- Web crawling
- Shoring Platform, web server database, PHP support with a couple of modules
- OSINT data collection
- Structured database, processing, visualization
- Audio and Video surveillance, GPS and GIS tracking, Data Crawling
- Advanced crawling engine
- Platform
- Automated biometric identification
- Emulation, simulation, serious gaming and visualization capabilities
- CTTP model
- Receive and analyze passenger data
- Network traffic analysis
- Network forensics
- Analytical engine powered by machine learning algorithms
- Big data storage platform
- APIs
- Decision support
- Software platform
- Shared hash database

Concerning the **platforms** presented in the scheme, the list is less diversified. Most of the platforms are used by several technologies and a technology can be used by several platforms at the same time:

- Linux (7 technologies)
- Windows application (2 technologies) / Windows (13 technologies)
- Mac (2 technologies)
- Web browser (Safari, IE, Firefox and Chrome) (2 technologies)
- IOS and Android mobiles platforms (2 technologies)
- Web App (1 technology)

In terms of **license** and **availability of the technologies**, several options are showed:

- Proprietary (without any indication of the availability of the technology) (2 technologies)
- Closed source with paid access (17 technologies)
- Closed source with free access (2 technologies)
- Open source with free access (3 technologies)

The Critical Technologies SWOT analysis

While the weaknesses, opportunities and challenges are not always described in the table, the strengths of the technologies are all (except one) indicated here:

1- *Knowledge Extraction Components* and *Components for intelligence discovery and decision support*:
- Strength: Possible adaptability of the technology with the Mindb4act requirements (no weakness, no opportunity, no challenge indicated yet).

2- *MISP (the Malware Information Sharing Platform):*
- Strengths: Full control of what happens with the data due to the storage of the data within the premises and under the control of the user
- Opportunities: Different MISP instances can be connected to each other, giving the possibility to receive information from other instances and store it locally (ensuring confidentiality). (no weakness nor challenge indicated)

3- *SAIL LABS Media Mining System:*
- Strength: Real-time information analysis from various media sources
- Weakness: Strong reliability on OSINT data which might be fake or incorrect and focus on surface web
- Opportunity: Collection of data from various sources. Production of a more holistic pictures of threats
- Challenge: Need to assess which personal information can be included in the output (GDPR issue)

4- *Electronic surveillance:*
- Strength: Data accessible through a central command and control center / Correlation and synchronization of data from heterogeneous sources.
- Weakness: No inclusion of open or big data → important sources might be overlooked
- Opportunity: Combination with open source intelligence or social media gives a holistic approach for monitoring and surveillance of offenders
- Challenge: Data protection is crucial to avoid any misuse of sensitive data.

5- *SOCMINT*:
- Strength: Harvesting information from both the surface web and the dark web
- Opportunity: Deep web analysis allowing the tracking of terrorist and extremist from the social media, the surface web and the dark web.
- Challenge: Strong security and privacy implications coming from the surface and the dark web (weakness not listed).

6- *Medusa*:
- Strength: Artificial intelligence algorithms that can handle a large amount of data disseminated through heterogeneous sources quickly.
- Opportunity: Real time trend analysis, multisource, public sentiment and opinion awareness
- Challenge: Integration and compatibility (no weakness listed)

7- *Mantis (Model-based Analysis of threat intelligence sources*):
- Strength: Analysis platform enabled the aggregation and correlation of threat data into a unified representation based on attributed graphs.
- Opportunity: Platform providing a unified representation of threat data constructs from different standards (no weakness nor challenge listed)

8- *MBSIS Suite*:
- Strength: Combination of a set of technologies for biometric investigations

- Opportunity: Modular and scalable system to be integrated into existing security IP infrastructures
- Challenge: Compatibility and database connection issues in the integration into existing system (no weakness listed)

9- *COSAIN*:

- Strength: Real Time Access to multiple internet data streams, intelligent location filtering, evolving machine learning capability / ability to be run on public sentiment analysis events and evaluating threats from community disorder
- Opportunity: Ability to monitor police reputations, community tensions and potential public disorder events
- Challenge: Better for proactive analysis than investigating individuals

10- *Repknight*:

- Strength: Ability to crawl and monitor dark web content, as well as detect and notify users of data breaches and user custom search monitoring of dark web sources.
- Weakness: Focus on Dark web monitoring which incurs a limitation on looking at other forms of deep web.
- Opportunity: Ability to put data and custom databases/taxonomies into the system allowing crawl for key words matching these repositories online and notify in real time if they have been discovered.
- Challenge: Main focus on dark web crawling

11- *X1 Discovery:*

- Strength: Collection and Indexing of data from social media streams, linked content and websites through APIs, webmail connectors and direct web navigation. Aggregation of data from multiple sources in real time in a highly scalable and case-centric manner.
- Weakness: Main reliance on APIs
- Opportunity: Collection of data from multiple social media feeds as well as documenting and hashing it as the crawling proceeds.
- Challenge: APIs may become more expensive and more difficult to acquire in the future.

12- *Threat arrest:*

- Opportunity: Validation of the effectiveness by a prototype implementation interconnected with real cyber systems pilots in the areas of smart energy, healthcare and shipping and from technical, legal and business perspectives. (no strength, weakness nor challenge indicated)

13- *I2*:

- Strength: Flexible analytical toolkit with modular add ins available for a variety of analyst need
- Weakness: expensive and lack of modern features
- Opportunity: Modular aspect
- Challenge: Requirement of trainings to use it

14- *Virtual Humint:*

- Strength: Management of multiple avatars / Can be integrated in existing intelligence systems

- Weakness: Might not correspond with EU regulations for information security and police investigations
- Opportunity: Support investigation of terrorist attacks and radicalisation planned through the infiltration of closed forums with the avatar
- Challenge: GDPR issues (as well as ethics and privacy compliance)

15- *Gotravel:*

- Strength: Monitoring system operating on a national level and connecting databases of passenger information
- Weakness: limited to air travels
- Opportunity: enhancement of the platform
- Challenge: possible extension of the scope

16- *Palanthir Gotham:*

- Strength: Advanced platform for data analytics, big data processing, live monitoring, taxonomy building, and intelligence documenting
- Weakness: Expensive and trainings required
- Opportunity: Ability to integrate live situational awareness data into historic and bottom up datasets
- Challenge: trainings and cost

17- *Vehere*:

- Strength: Speech recognition, natural language processing and behavioural analytics
- Opportunity: Harnessing data from multiple sensors (no weakness nor challenge listed)

18- *HART*:

- Strength: Supports at least 7 types of biometric identifiers
- Weakness: highly inaccurate data can be included
- Challenge: Hart will be shared with federal agencies as well as state, local LEAs and foreign governments. (no opportunity listed)

19- *Security Trail:*

- Strength: Give access to IP, DNS, WHOIS and company related information available in the SecurityTrails Web platform and beyond it.
- Opportunity: Available for security companies, Researchers and teams (no weakness, challenge listed)

20- *Maltego CE:*

- Strength: Maltego community includes most of the same functionality as the commercial version
- Weakness: Community version cannot be used for commercial purposes
- Opportunity: Free and convenient ability to analyse SOC MINT data
- Challenge: limited capacities

21- *MASAR*

- Strength: Monitoring, measuring and evaluating P/CVE programs
- Weakness: Not under European laws
- Opportunity: MASAR assists practitioners and policy makers in drafting a plan P/CVE programs and projects (no challenge listed)

22- *Cross channel and multi-sensor analytic (NICE*) (no SWOT analysis at all)

23- *Hash Sharing consortium*

- Strength: More than 200 000 hashes
- Weakness: Still no request from LEAs or governments to gain access to the hash sharing consortium database.
- Opportunity: Could be the seed to eradicate terrorism and extremism files from internet
- Challenge: add more stakeholders

The social innovation initiatives presentation

Geographical data

In total, 18 social innovation initiatives have been listed by the partners (Annex 3). 16 of them have been analysed thorough the SWOT method (Annex 5). From the ones analysed 9 initiatives are from European providers and 7 from non-European providers. None here are considered as worldwide. The initiatives provided by European providers are all operationalized in the EU. Concerning those conceived by non-European providers, 3 of them can certainly be found in the EU, out of the 4 remaining, 3 are only operationalized in Canada and in Saudi Arabia. For one Social Innovation, the information is not available.

Social Innovation field

From the wide range of fields listed here, the predominance of social initiatives focusing on *Guidelines* and *Education* has to be underlined, both inside and outside of the EU. The other fields covered can be seen as clearly linked to the concept of *awareness:*

- Guidelines (6 social innovations)
- Guidelines and Statutory responsibility (1 social innovation)
- Education (7 social innovations)
- Training program (1 social innovation)
- Curriculum (1 social innovation)
- Prevention and Intervention toolkit (1 social innovation)
- Community building, prevention (1 social innovation)
- Countering Violent Extremism Toolkits (1 social innovation)

Social Innovation Target

The audiences targeted by the initiatives listed can be divided into 10 main groups. Most of the social innovations indicates more than one target:

- Educationists (7 social innovations)
- Academics (5 social innovations)
- Practitioners (10 social innovations)
- LEAs (2 social innovation)
- Policy makers (6 social innovations)
- Local communities (3 social innovations)
- Young people (1 social innovation)
- Students (1 social innovation)
- Social media users (2 social innovations)

- Industry (1 social innovation)

The Social Innovation SWOT analysis

Like the technology analysis, the weaknesses, opportunities and challenges are not always described in the table. However, the strengths of the social innovations described in the analysis are all indicated here:

Strengths:

1- *The prevent duty:*
- Strength: Operating in 3 key stages of channel (identification of individuals at risk being drawn into terrorism, assessment of the nature and extent of that risk, development of the most appropriate support plan for the individuals concerned
- Weakness: No adequate training provided to the teachers
- Opportunity: Common understanding and mechanism to operationalize similar activities
- Challenge: Program does not sufficiently consider general factors

2- *Handbook for structural quality standards in deradicalisation work*
- Strength: First-ever guide for implementing and monitoring quality standards in deradicalisation work.
- Weakness: German focus
- Opportunity: Handbook that could be used as a framework to develop tailored criteria for other contexts
- Challenge: Lack of funding could be an issue

3- *Mother schools:*
- Strength: Link between women at the community level where radicalism is propagated and decision-making levels where counter violent extremism strategies are shaped
- Weakness: Strong engagement at the local level
- Opportunity: Program tested in several countries and continues to grow
- Challenge: Difficult to reach parents of right-wing extremists

4- *Counter narratives for countering violent extremism:*
- Strength: Comprehensive overview of the concept and implementation of counter narratives in the CVE practice
- Weakness: Lack of materials in the toolkit
- Opportunity: Possible extension of the framework with practical information and material
- Challenge: Page is static (no updates or follow-ups)

5- *Lifecycle initiative toolkit:*
- Strength: Basic and in-depth Knowledge hub for practitioners from different field (prevention, detection/intervention and rehabilitation/reintegration)
- Weakness: few of the resources provided are practical guidelines
- Opportunity: Production of more practical tools
- Challenge:

6- *UNESCO Guide to stopping violence in Schools*

- Strength: Guideline covering a wide range of issues leading to violence including radicalisation
- Weakness: document outdated with no particular focus on radicalisation leading to terrorism
- Opportunity: Guideline covering the basic factors of radicalisation which could be used as building blocks for future similar activities (no challenge listed)

7- *Asia Europe countering Dialogue:*

- Strength: Analysis of recent development concerning Daesh extremism and their implications on societies in Asia and Europe (no weakness, opportunity nor challenge listed)

8- *Extreme dialogue:*

- Strength: Building of Long term, sustainable relationships with schools to ensure the highest levels of impact for students and teachers
- Opportunity: Could run an open dialogue session in schools or communities (no Weakness nor challenge listed)

9- *Police Type education as antiradical prophylaxis:*

- Strength: Knowledge sharing
- Weakness: not EU specific
- Opportunity: Introduction of police type uniformed high school classes in educational systems of other EU countries
- Challenge: EU MS regulatory measures

10- *Teacher's guide on the prevention of violent extremism:*

- Strength: Combination of global knowledge and practices from the field of radicalisation prevention in schools
- Weakness: guide too generic
- Opportunity: guide could be adapted by the EU or MS to their particular challenges
- Challenge: Parallel Development of national and European similar guides

11- *Redirect*:

- Strength: Program has a variety of strategies that can be applied to help young people who are vulnerable to being radicalized (strategies range from simply educating people of the dangers of radicalisation all the way up to helping people exit radical groups)
- Weakness: Canadian perspective of the program limits its extent to other geographical scopes
- Opportunity: Possible duplication in the EU
- Challenge: No specific reference made as to whether and how the program could be sustained or extended to other areas

12- *Tech against terrorism:*

- Strength: Knowledge sharing: best practice, platform, practical and operational support
- Weakness: Not EU specific
- Opportunity:
- Challenge:

13- *Antiterrorism assistance Program:*

- Strength: Program serving as a primary provider of US government antiterrorism training and equipment to 53 active partner nations, building capacity to investigate, detect, deter and disrupt terrorist activities while bolstering foreign civilian law enforcement counterterrorism skills
- Weakness: Potential compromising of some features of educational activities in favour of political understanding of and approaches to counter-radicalisation
- Opportunity: Could be duplicated as-is.
- Challenge: Lack of necessary cultural underpinnings that are dominant in radicalisation and deradicalisation narratives processes.

14- *Canadian practitioners network for prevention of radicalisation and Extremist violence*:

- Strength: Best practice guidelines related to assessment prevention and intervention/ identification of existing assets and level of collaboration through a mapping of existing initiatives.
- Weakness: US driven (Opportunity and challenge not listed)

15- Canadian practitioners network for prevention of radicalisation and Extremist violence:

- Strength: Capacity building for knowledge mobilization and transfer of the existing materials on a national and international scale
- Weakness: Not EU specific
- Opportunity: Cooperation with EU internet forum
- Challenge: Share of experience with EU MS.

16- Project Someone:

- Strength: Capacity building for knowledge mobilization and transfer of the existing materials.
- Weakness: Not under European laws (no opportunity nor challenge listed)

Conclusion

A wide range of Critical Technologies and Social innovations have been listed in this deliverable. It is interesting to note the diversity in their scope of exploitation. This clearly shows the need of an umbrella of solutions (social and technical) to erase the process of radicalisation and violent extremism.

Acronyms and Definitions

ACRONYM	DEFINITION
CR	Counter-radicalisation
CVEs	Counter-violent extremism
DoE	Department of Education (NYC)
GCTF	Global Counter Terrorism Forum
GRIDS	German Institute on radicalisation and de-radicalisation
LEA	Law Enforcement Agency
OSINT	Open Source Intelligence
Project SOMEONE	Project Social Media EducatiON Every day
R&D	Research and Development
R&I	Research and Innovation
SERENE-RISC	Smart Cybersecurity Network
SWOT	Strengths, Weaknesses, Opportunities and Threats
UN CTED	United Nations Counter Terrorism Executive Directorate
UNESCO	United Nations Educational, Scientific and Cultural Organisation
WP	Work Package

Annex 1 Pre structured template sent by EOS

#	NAME OF THE TECHNOLOGY	DESCRIPTION	PROVIDER	LOCATION OF PROVIDER	TECHNOLOGY FIELD	TECHNOLOGY METHODOLOGY	TECHNOLOGY PLATFORM	TECHNOLOGY LICENCE	TECHNOLOGY AVAILABILITY	URL FOR TECHNOLOGY	OPERATIONALISATION IN EU	STRENGTHS	SOURCE URL STRENGTHS	WEAKNESSES	SOURCE WEAKNESSES URL	OPPORTUNITIES	SOURCE OPPORTUNITIES URL	CHALLENGES	SOURCE CHALLENGES URL	ENTRY ADDED BY
1																				
2																				
3																				
4																				
5																				
6																				

Annex 2 Critical Technologies scheme presentation

#	Name of the Technology	Description	Provider	Location of the provider	Technology field	Technology Methodology	Technology Platform	Technology License	Technology availability	URL for technology	Operationalisation in EU	Entry added by
	European Provider											
1	**Knowledge Extraction Components**	Darkweb Crawler: The Darkweb data collection tool is a crawler and a scrapper for all websites from Clean Web and DarkWeb (Tor Darknet). It permits to realize an exact snapshot of the scraped domain with a crawling policy defined by the user. The snapshot stores all data from the website as texts or images and other multimedia entities. This tool is developed for simulating a human user to be resilient against countermeasures and realizes a graph of the domain allowing graph theory operations. Extraction Components: -Named Entity Recognition Component -Relationship Extraction Component	COPKIT project	Europe	Social Media Analysis, Big Data Analysis	Web crawling	Linux	Closed source	Not sure	https://copkit.eu/	In development	GUCI

		-Moments Recognizer Component										
2	**Components for intelligence discovery and decision support**	This tool will support the analyst's activities: knowledge discovery (pattern, anomaly detection), situation assessment (estimation and fusion) and forecasting (spatio temporal trends and prediction) at all levels from strategic to investigative.	COPKIT project	Europe	Social Media Analysis, Big Data Analysis	Decision Support	Linux	Closed source	Not sure	https://copkit.eu/	In development	GUCI
3	**MISP (the Malware Information Sharing Platform)**	The MISP threat sharing platform is a free and open source software helping information sharing of threat intelligence including cyber security indicators. A threat intelligence platform for gathering, sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information	MISP project	Europe	Threat intelligence	Shoring platform; A Web server, database and PHP support with a couple of	Windows	Open Source	Free	https://www.misp-project.org	yes, co-financed by European Union	CENTRIC

						modules.						
4	**SAIL LABS Media Mining System**	SAIL LABS Media Mining System is an integrated platform for analysts and decision makers, extracting metadata and key information from multiple sources in multiple languages in real time. The system automatically records and harvests data from multiple sources such as TV, FM Radio, YouTube, Internet (Social Media, Feeds, Websites), e-mails, and electronic documents. The raw data then runs through a series of processing steps: the speech content is transcribed, indexed and enriched with information about the content regarding language, speaker, named entities, topics, and sentiment. It is subsequently stored on a database for later search and retrieval, and can additionally be archived in the RAID Storage. Visualization and analysis of trends, relations, global hot spots, profiles, as well as ontologies and social media visualization & analytics pave the way for turning raw, unstructured data into intelligence.	SAIL LABS	Austria	Big data / OSINT analysis	OSINT data collection, structured database, processing, visualisation and decision support	Windows	Closed Source	Paid	https://www.sail-labs.com/media-mining-system/	yes	SYNYO

5	**Electronic Surveillance**	Electronic Surveillance applications are meant to provide support for investigations where the use of hidden microphones, cameras and GPS tracking devices is needed to gather information through surveillance of people and places. It includes complete HW/SW systems for audio and videomonitoring and GPS tracking. Both real time listening/viewing and offline analysis are supported. GIS tools are available to represent and analyze targets positions over maps.	IPS	Italy	Surveillance, Detection, Investigation	Audio and Video Surveillance, GPS and GIS tracking	Windows, Linux	Closed Source	Paid	https://www.ips-intelligence.com/en/electronic-surveillance/solutions/electronic-surveillance-gps-tracking-audio-video-monitoring#m22	yes	SYNYO
6	**SOCMINT**	The end-to-end Social Media and Open Source Intelligence platform monitors Social Media and Forums, analyses Deep Web and Dark Web, and transforms the data into useful information.	IPS	Italy	Surface web and dark web monitoring	Data crawling, surface web and darknet and avatar management	Windows, Linux	Closed Source	Paid	https://www.ips-intelligence.com/en/social-media-intelligence	yes	SYNYO

7	**Medusa**	MEDUSA® is an end-to-end Social Media Intelligence and OSINT product that transforms public data such as Social Media and Deep & Dark Web in valuable information. Designed to help Homeland Security departments to fight against serious crimes, MEDUSA® is a complete product that matches several industries' needs. The platform can be used to massively monitor media sources (text, pictures and videos) for preventive purposes.	Medusa	Italy	Big data / OSINT analysis Machine Learning	Surface web and darknet analysis Advanced crawling engine	Windows	Closed Source	Paid	https://www.medusa-labs.com/	Yes	CENTRIC
8	**Mantis (Model-based Analysis of Threat Intelligence Sources)**	Mantis is a platform for threat intelligence that enables the unified analysis of different standards and the correlation of threat data through a novel type-agnostic similarity algorithm based on attributed graphs. Its unified representation allows the security analyst to discover similar and related threats by linking patterns shared between seemingly unrelated attack campaigns through queries of different complexity.	Siemens	Germany	Threat Intelligence; Advanced Persistent Threat; Graph Mining; Information Retrieval	Platform	Windows	Open Source	Free	https://www.first.org/resources/papers/conference2014/first_2014_-_grobauer-_bernd_-_mantis_framework_20140606.pdf	Yes	CENTRIC

9	**MBIS SUITE**	In order to meet the demand for real-time identification of suspects and criminals, MBIS offers a range of products centered on an innovative Automated Biometric Identification System. MBIS provides investigators with a biometric search engine and is backed by a range of tools for editing, selection and image enhancement. Front-end workstations manage fingerprint, palm and facial images, and display verification and comparison tools, while backend platforms provide processing and archive storage.	IDEMIA	France	Individual identifcation	Automated Biometric Identification	Windows, Linux	Closed Source	Paid	https://www.idemia.com/mbis	Yes	SYNYO
10	**Cosain**	COSAIN is a secure cloud based (Software as a Service) open source and data listening platform. - Designed for law enforcement to reduce threat, risk and harm, - Supports situational awareness, collaborative working and decision making, - A tool for both specialist and passive users - Learn, collaborate and share best practice within the COSAIN community - Strategic roadmap with continual innovative software development designed with users - Ongoing support by dedicated account manager - ITIL Service Management - Two-factor authentication - Dashboarding capability to review results as analytics - On-site and computer-based training designed by experienced professionals	Barrchd (CAPITA)	UK	Data visualisation and processing	Process information into actionable intelligence	Web App (All browsers supported, Windows	Closed Source	Paid	https://www.digitalmarketplace.service.gov.uk/g-cloud/services/236186891130458	Yes	CENTRIC

11	**Repknight / Skurio**	The main aim of Skurio is to help security and IT security professionals to see things clearly across the full spectrum of risk. The company looks at digital risk from the 'outside in' and illuminates parts of the web that can't be seen across the surface, social, deep and Dark Web. Repknight is a cost-effective, intuitive and powerful Cloud based solutions to identify threats, detect data breaches outside the network and automate the response; allowing companies to mitigate any risk and minimise financial loss.	Skurio	UK	Data visualisation and processing	Process information into actionable intelligence	Web Browser (Safari, IE, Firefox and Chrome), Windows Aplication	Closed Source	Paid	https://repknight.com	Yes	CENTRIC
12	**X1 Discovery**	X1 Social Discovery is a industry-leading solution for anyone who needs to collect and search data from social networks and the internet. X1 Social Discovery aggregates comprehensive social media content and web-based data into a single user interface, collects vital metadata in a legally defensible manner and preserves the chain of custody. X1 Social Discovery saves customers vast amounts of time and money through the automated and simultaneous collection of data from multiple social media accounts.	QBS Software	UK	Data visualisation and processing	Process information into actionable intelligence	Web Browser (Safari, IE, Firefox and Chrome), Windows Aplication	Closed Source	Paid	http://www.qbssoftware.com/products/X1_Social_Discovery/overview/_prodx1socdisc	Yes	CENTRIC
13	**THREAT-ARREST**	THREAT-ARREST aims to develop an advanced training platform incorporating emulation, simulation, serious gaming and visualization capabilities to adequately prepare stakeholders	Hellas (FORTH) and others	Greece	counter advanced, known	emulation, simulation,	Windows	Closed Source	Paid	https://www.threat-	yes	CENTRIC

		with different types of responsibility and levels of expertise in defending high-risk cyber systems and organizations to counter advanced, known and new cyber-attacks. The THREAT-ARREST platform will deliver security training, based on a model driven approach where cyber threat and training preparation (CTTP) models, specifying the potential attacks, the security controls of cyber systems against them, and the tools that may be used to assess the effectiveness of these controls, will drive the training process, and align it (where possible) with operational cyber system security assurance mechanisms to ensure the relevance of training. The platform will also support trainee performance evaluation and training programme evaluation and adapt training programmes based on them.	in the consortium (Atos, IBM, etc.)		and new cyber-attacks	serious gaming and visualization capabilities; CTTP model				arrest.eu/		
14	**Sophos' Intercept X tool**	Not indicated	Not indicated	UK	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated
15	**Darktrace Antigena**	Not indicated	Not indicated	UK	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated
16	**Sophos' Intercept X tool**	Not indicated	Not indicated	UK	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated
	Non-European provider											
17	**I2**	IBM i2 Intelligence Analysis Platform provides an extensible, service-oriented environment designed to integrate into your existing enterprise	IBM	USA	Data visualisation	Process informa	Windows,	Closed Source	Paid	https://www.ibm.com/s	Yes	CENTRIC

		infrastructure. The platform helps facilitate and support operational analysis, improving situational awareness, and providing faster, more informed decision making across and inside organizations. I2 is used by law enforcement for a variety of outcomes including; visualising complex information for analysis, visualising evidence for trial processes, mapping out criminal and CT organisational heirarchies, cross matching comionalities in datasets, etc.			and processing	tion into actionable intelligence	Mac, Lunux			upport/knowledgecenter/en/SSBK6W_5.2.0/com.ibm.icmideployment.doc/t_ibm_i2_intelligence_analysis_p.htm		
18	**Virtual humint**	Avatars (virtual agents) are created, managed and operated by intelligence analysts with the prime objective to gather data from various open and human sources on the web. Lynx assists analysts in the creation, management, and maintenance of these avatars' information over time. The system provides analysts with relevant and critical data in real time.	Cobwebs Technologies	USA	Human intelligence operations	Surface web and darknet analysis through avatars	Windows	Closed Source	Paid	https://www.cobwebs.com/virtual-humint/	unknown	SYNYO
19	**goTravel**	goTravel is a United Nations-owned software solution derived from the Travel Information Portal (TRIP), developed by The Netherlands. goTravel supports the end-to-end process for law enforcement to obtain passenger data from (airline) carriers and conduct targeted analysis as well as share the findings of their data assessment. Member States adopt the UN-owned and operated goTravel solution to enable the	OICT	USA	Data matching	Receive and analyze passenger data	Windows	Closed Source	Free	https://www.un.org/cttravel/goTravel	yes	CENTRIC

		automated analysis of large data volumes on passengers on all inbound and outbound traffic. The goTravel software solution is provided to Member States free of charge.										
20	**Palantir Gotham**	Palantir Gotham integrates and transforms data, regardless of type or volume, into a single, coherent data asset. As data flows into the platform, it is enriched and mapped into meaningfully defined objects — people, places, things, and events — and the relationships that connect them. Palantir Gotham brings intelligence, people, and data together to empower one another. As users collaborate and build off one another's work, they create and grow a body of shared intelligence for their organization.	Palantir	USA	Data visualisation and processing	Process information into actionable intelligence	WebApp (Windows, Mac, Linux), IOS and Android mobile platforms	Closed Source	Paid	https://www.palantir.com/palantir-gotham/	Yes	CENTRIC
21	**Vehere (e.g.Custom Network Situational Awareness tool called PacketWorker or CommuSAS)**	Vehere is trusted by Government & Organisations to secure their Cyber Defences and provide proactive Communications Intelligence. Vehere's Convergent Multiservice Interception System CommuSAS, acquires multiple data formats and protocols covering the widest gambit of sensor platforms for both structured and unstructured data and provides a unified view. Powerful and robust Big Data storage platform incorporates scalability and high availability without compromising on performance.	Vehere	USA	Cyber Intelligence, cyber security - satellite monitoring, GSM and Wi-Fi monitor	network traffic analysis, network forensics, analytical engine powered by Machin	Not indicated	Closed Source	Paid	https://vehere.com/	Yes	CENTRIC

					ing, lawful interception	e Learning algorithms; Big Data storage platform						
22	**IBM QRadar Advisor**	Not indicated	Not indicated	USA	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated
23	**HART**	OBIM (Office of Biometric Identity Management) operates and maintains the Automated Biometric Identification System (IDENT), the largest automated biometric identification system in the U.S. government. With the advent of advanced technology and the expansion of biometric services, DHS (Department for Homeland Security) OBIM is replacing IDENT with a new biometric system known as Homeland Advanced Recognition Technology (HART).	Department of Homeland Security, USA	USA	Individual identifcation	Automated Biometric Identification Database	Windows	Closed Source	Paid	http://www.planetbiometrics.com/article-details/i/5614/desc/dhs-reveals-details-of-rfp-for-hart	unknown	CENTRIC
24	**SecurityTrails**	SecurityTrails currently offers three different products that can help you enrich your data, search for information, and find relevant security information for organizations in no time: SecurityTrails API Data enrichment for applications that consume IP,	Algoro, LLC	USA	Cyber Threat Intelligence	APIs	Windows	Closed Source	Paid	https://securitytrails.com/	Not indicated	CENTRIC

		DNS, WHOIS and company data, such as SIEM systems and security automation products. Accessing the SecurityTrails REST API For any data input outside of headers, path or query the JSON format is used. POST request bodies should supply JSON data. Any responses will be in JSON.									
25	**Symantec's Targeted attack analytics (TAA) tool**	Not indicated	Not indicated	USA	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated
26	**Vectra's Cognito**	Not indicated	Not indicated	USA	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated	Not indicated
27	**Maltego CE**	Maltego is an open source intelligence analysis tool also used for digital forensics. Maltego is an interactive data mining tool that renders directed graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the Internet.	Paterva	South Africa	Data visualisation and processing	Process information into actionable intelligence	Web App (All browsers supported), WIndows, Linux	Open Source	Free	https://www.paterva.com/buy/maltego-clients/maltego-ce.php	Yes	CENTRIC
28	**GISs > not a tool per se, rather technologies/systems**	GIS provides the technology that enables geographical data collection from LIDAR, aerial photography and satellite imagery, data that is captured, stored, analysed and displayed in maps. The maps can reflect hot-spot gas field and oil field where terrorist activities are carried out. This	N/A	Saudi Arabia	Geographic Information System , GIS,	Not indicated	Windows	Closed Source	Paid	http://www.worldinwar.eu/fighting-terrorism	Not indicated	CENTRIC

		also makes geography a key subject in understanding such activities. Apart from terrorism, the public health sector also has a huge application for GIS. Such technological method requires effective mapping and when combined with geospatial technologies, terrorism can be countered with appropriate action. The age of big data, digital mapping and other remote sensing technologies are discussed in the paper.			Counter terrorism, Geographical data collection, KSA, Egypt, Lidar					-more-effectively-with-the-aid-of-gis-kingdom-of-saudi-arabia-case-study/		
29	**MASAR**	MASAR, which means "path" or "trajectory" in Arabic, helps steer designers of preventing and countering violent extremism (P/CVE) projects on the right "path" to achieving measurable outcomes and projecting the impact in terms of reducing radicalisation and recruitment to violent extremism. MASAR assists practitioners and policymakers in creating a plan for monitoring, measurement, and evaluation (MM&E) of P/CVE programs and projects. MASAR walks a user through a comprehensive process for helping design P/CVE programs, collecting information about the user's activities and recommending resources to support the development of goals and objectives, indicators, data collection methods and evaluation.	Hedayah and (RUSI).	Abu Dhabi, United Arab Emirates	Evaluating the Effectiveness of CVE Programs	Decision Support	IOS, Android, Windows	Closed Source	Free	http://www.hedayahcenter.org/what-we-do/91/departments/98/research-and-analysis/914/masar	Not indicated	GUCI
	Critical technologies with a global scope											

30	**NICE Situator (PSIM solution) > for building security**	NICE Situator is an advanced physical security information management (PSIM) solution that enables situation planning, response and analysis for the security, safety and emergency markets where the risk of human error can lead to financial loss, injury and damage to public image. By integrating and correlating information from multiple and diverse systems across the organization and coordinating response actions, NICE Situator ensures that everyone in the operational chain knows what is happening and what to do.	Software House	Global	Not indicated	Software platform	Windows	Closed Source	Paid	https://www.swhouse.com/products/nice-situator.aspx	Not indicated	CENTRIC
31	**Hash Sharing Consortium**	In December 2016, the founding member companies of the GIFCT (Facebook, Microsoft, Twitter, and YouTube), committed to creating a shared industry database of "hashes" — unique digital "fingerprints" — for violent terrorist imagery or terrorist recruitment videos that they have removed from their services. By sharing these hashes with one another, they can identify potential terrorist images and videos on our respective hosted consumer platforms.	GIFCT	Global	Social Media Analysis, Big Data Analysis	Shared hash database	Not indicated	Not indicated	Free	https://gifct.org/joint-tech-innovation/	Yes	GUCI
	Terrorgence (only the company, not a tool)	Founded in 2004, Terrorgence is a global pioneer and leader in the field of Web Intelligence (WEBINT). The principal assets over the years have been the highly-experienced in-house analysts, presently counting 40+ experts in different fields such as, Terror Funding and Recruiting, Criminal Activities, Cyber Threat Intelligence, Strategic Research, Improvised	Terrorgence					Not indicated	Not indicated			None listed

		Explosive Devices (IED) and Homemade Explosives (HME) and more. Terrogence delivers intelligence solutions to customers around the world, including government organizations, law enforcement agencies, business enterprises with international operations, and more.										

Annex 3 Social Innovation scheme presentation

#	Name of the social Innovation	Description	Provider	Location of Provider	Social Innovation Field	Social Innovation target Audience	URL for social Innovation	Operationalisation in EU	Entry added By
	Provider in the EU								
1	**The Prevent Duty**	The 'Prevent Duty' placed on schools to safeguard pupils from radicalisation and being drawn into terrorism. It includes government definitions on terrorism, radicalisation and extremism and explains the obligations of schools to assess risk, train staff, educate pupils and refer to the 'Channel' programme when there is a need for intervention.	DOE- Schools	UK	Guideline/ Statutory responsibility	Educationists, practitioners	https://childlawadvice.org.uk/information-pages/radicalisation-in-schools-and-the-prevent-duty/	yes	CENTRIC

2	**Handbook for Structural Quality Standards in Deradicalisation Work**	The handbook provides a guide for structural integrity and quality standards in CVE and deradicalisation work. It teaches practitioners, policy makers and academics how effective deradicalisation programs need to be built and how their structural quality can be assessed.	GRIDS	Germany	Guidelines	practitioners, policy makers and academics	http://girds.org/file_download/23/final-handbook-quality-standards.pdf	yes	SYNYO
3	**MotherSchools**	MotherSchools create a transformational experience for mothers by providing a save space where self-awareness, self-expression and self-empowerment are appreciated and encouraged. Through trusted community leaders and NGOs, mothers who are concerned about violent extremism are approached about safety of their children and their community. In a playful and highly interactive way, mothers learn about parenting, adolescent development and early warning signals of radicalisation.	Women Without Borders	Austria	Community building, prevention	Local communities	http://www.women-without-borders.org/	yes	SYNYO
4	**Counter Narratives for Countering Violent Extremism**	Extremists and violent extremists have always sought to use compelling messages and narratives as a means of attracting followers to their cause. In the modern age it follows that the internet and social media represent a significant	The Commonwealth	UK	Countering Violent Extremism Toolkits	Local communities, First-Line-Practitioenrs	http://thecommonwealth.org/countering-violent-	yes	SYNYO

		and easy to use medium to inspire, radicalise and recruit young people. It is apparent that if Countering Violent Extremism (CVE) is to be effective, there must be greater focus and resources made available to the development of effective counter narratives, both online and offline. It must be noted that Counter Narrative Programmes are time and resource intensive and require committed action.					extremism-toolkits		
5	**Lifecycle Initiative Toolkit**	The “Lifecycle Initiative” aims to equip policy-makers and practitioners with conceptual tools they can apply at various points of the life cycle of radicalisation to violence: from prevention, to intervention, to rehabilitation and reintegration. In order to make the tools accessible and useful to stakeholders, the Lifecycle Initiative Toolkit was developed in 2016, intending to give policy-makers and practitioners access to consolidated information on the GCTF and related Good Practices documents, program models, research, and other counterterrorism and countering violent extremism resources.	GCTF - Global Counterterrorism Forum	The Netherlands	Prevention and intervention toolkit	First-Line-Practitioenrs, local communities	https://toolkit.thegctf.org/en/	yes	SYNYO

6	**The UNESCO Guide to Stopping Violence in Schools**	Examines various forms of violence that take place in schools, and offers practical suggestions as to what teachers can do to prevent them. Ten action areas are proposed, each with specific examples that teachers can adapt to address and prevent violence. Except from relevant international normative instruments as well as a list of links to online resources for stopping violence in schools are annexed at the end of the book.	Schools	EU	Guideline	Teachers & Policy makers	https://www.unesco-vlaanderen.be/media/72169/stopping%20violence%20in%20schools.pdf	yes	CENTRIC
7	**Asia-Europe Counter Terrorism Dialogue**	The Konrad Adenauer Stiftung's Regional Programme Political Dialogue Asia and the Pacific aims to provide platforms and fora which shall enable the key stakeholders to foster their exchange and develop tools as well as joint initiatives, ultimately resulting in a stronger cooperation between Asia and Europe to counter this global threat.	Stakeholders	Europe, Asia	Guideline (publication)	Schools, Teachers, Academics, Practitioners, Policy-makers	https://www.kas.de/laenderberichte/detail/-/content/countering-daesh-extremism-european-and-asian-responses1	yes	CENTRIC
8	**Extreme Dialogue**	Extreme Dialogue is a cutting-edge project designed to provide young people with the tools they need to challenge extremism in all its forms. Through a series of compelling films telling the true stories of those affected by extremism, with supporting educational resources, it	Institute for Strategic Dialogue	London, England	Education	Young people	https://extremedialogue.org/	Yes	GUCI

		provides a range of perspectives on how violence, exclusion and hate change lives. Designed to be delivered by teachers, other education or youth practitioners, external facilitators or young people themselves, the free Extreme Dialogue films and educational resources can be supported by training workshops.							
9	**Police-type education as antiradical prophylaxis.**	Influence of police oriented highschool education has a significant influence on youth and that this kind of influence manifests itself in its preventive character with respect to the radicalisation issues, and as such can be considered as an element of antiradical prophylaxis.	Regional Police HQ in Poznań and high schools in Wielkopolska.	Wielkopolska (Poland)	Education	Students of uniformed classess in high schools.		Yes	POZNAN
	Provider outside of the EU								
10	**A Teacher's guide on the prevention of violent extremism**	The UNESCO guide provides countries with a set of resources that can help build and reinforce national capacities to address the drivers of violent extremism through holistic and pragmatic education sector-wide responses.	UNESCO	USA	Guidelines	Teachers	https://unesdoc.unesco.org/ark:/48223/pf0000244676	yes	SYNYO
11	**ReDirect**	ReDirect is a programme that works to prevent Calgary youth and young adults	The City of Calgary	Canada	Guidelines	Educationists, LEAs,	https://www.calgary.ca/cps/	no	CENTRIC

		from being radicalized to violence through education, awareness, prevention and intervention.	Community & Neighbourhood Services			council partners, practitioners	Pages/Youth-programs-and-resources/Youth-intervention/ReDirect.aspx		
12	**Tech Against Terrorism**	Tech Against Terrorism is an initiative launched and supported by the United Nations Counter Terrorism Executive Directorate (UN CTED) working with the global tech industry to tackle terrorist use of the internet whilst respecting human rights.	United Nations Counter Terrorism Executive Directorate (UN CTED)	New York, United States	Education	Tech (particularly SMEs and start-Ups) & Government Sectors	https://www.techagainstterrorism.org/	Not indicated	Not indicated
13	**Countering Violent Extremism Curriculum**	This Curriculum is an attempt at overcoming the challenges encountered by the societies when it comes to CVE. It is designed to provide training for government and civil society workers on the field of countering violent extremism, whether or not they have prior experience with it. It is structured into ten learning modules and is accompanied by training materials, including a facilitator's guide, slide presentations, handouts, and pre-recorded webinars to allow for multi-day trainings. The materials include a series of activities for each module and links to	Schools, Teachers, Academics, Practitioners, Policy-makers	Abu Dhabi	Curriculum	Schools, Teachers, Academics, Practitioners, Policy-makers	http://www.hedayahcenter.org/what-we-do/509/strive-global-program/948/countering-violent-extremism-curriculum/952/the-mena-edition	no	CENTRIC

		illustrative videos that provide primers for discussion and reflection.							
14	**Asia-Europe Counter Terrorism Dialogue**	The Konrad Adenauer Stiftung's Regional Programme Political Dialogue Asia and the Pacific aims to provide platforms and fora which shall enable the key stakeholders to foster their exchange and develop tools as well as joint initiatives, ultimately resulting in a stronger cooperation between Asia and Europe to counter this global threat.	Stakeholders	Europe, Asia	Guideline (publication)	Schools, Teachers, Academics, Practitioners, Policy-makers	https://www.kas.de/laenderberichte/detail/-/content/countering-daesh-extremism-european-and-asian-responses1	yes	CENTRIC
15	**Antiterrorism programme assistance (ATA)**	Since its creation in 1983, the Antiterrorism Assistance (ATA) programme has served as the primary provider of U.S. government antiterrorism training and equipment to law-enforcement agencies of partner nations throughout the world, and has delivered counterterrorism training to more than 90,000 law enforcement personnel from 154 countries.	Policy-makers, practitioners, LEAs	USA	Training Programmes	Policy-makers, practitioners, LEAs	https://www.state.gov/anti-terrorism-assistance-ata-program-summary/	yes	CENTRIC
16	**Canadian Practitioners Network for Prevention of Radicalisation**	CPN-PREV (Canadian Practitioners Network for Prevention of Radicalisation and Extremist Violence) is an evidence-based and practitioners-centered network established to bring forward	Canada Centre	Montreal Canada	Education	Researchers, practitioners, policymakers, and various	https://cpnprev.ca/	No	GUCI

	and Extremist Violence	Canadian leadership and develop excellence in countering violent radicalisation. CPN-PREV supports best practices and collaborations among intervention teams, through sustained knowledge mobilization between researchers, practitioners, policymakers, and various community sectors.				community sectors.			
17	**Addressing Online Hate**	The "Addressing Online Hate " module developed by Project Someone and partner SERENE-RISC was launched on January 30th. This module was developed to enable libraries and community organizations to offer educational sessions and raise awareness about online hate.	SERENE-RISC & Project Someone	Montréal , Québec, Canada	Education	Social media users	https://www.cybersec101.ca/themes/addressing-online-hate/	Not indicated	Not inidicated
18	**Project Someone**	The SOMEONE (SOcial Media EducatiON Every day) initiative was launched in April 2016. It has been funded under Public Safety Canada's Kanishka (2014-2016) and Community Resilience Fund (2017-2019) programs as well as Global Affairs Canada's Counter-Terrorism Capacity Building Program (2018-2019). It consists of a web-based portal of multimedia materials aimed at preventing hate speech and building resilience towards radicalisation that	Project Someone	Montréal , Québec, Canada	Education	Social media users	https://projectsomeone.ca/	Yes	GUCI

		leads to violent extremism. The materials target youth, school and community members, public policy officials, as well as the broader public by focusing on the development of critical thinking and information literacy skills, and encouraging democratic dialogues in online and offline spaces. The initiative has seen the rigorous development and evaluation of curricular activities for elementary, secondary and post-secondary institutions. Such activities include: first-person narrative documentaries, textual and multimedia social media feeds, visual art-based public pedagogical materials, graphic novels, public panel discussions, lectures and workshops, academic articles and conference papers, and descriptions and workshops on novel research methodologies. Our work is framed in principles of social pedagogy which encourages the inclusive adoption of mobile and digital media by members of the public to create alternative narratives to divisive and violent messages propagated by hate groups.							

Annex 4 Critical Technologies SWOT analysis

#	Name of the technology	Strengths	Weaknesses	Opportunities	Challenges	Entry added by
	European Provider					
1	**Knowledge Extraction Components**	Because is under development, there is a posibility to adapt the technology with the MINDb4ACT requirements.	It is not on the market yet	None listed	None listed	GUCI
2	**Components for intelligence discovery and decision support**	Because is under development, there is a posibility to adapt the technology with the MINDb4ACT requirements.	It is not on the market yet	None listed	None listed	GUCI
3	**MISP (The Malware Information Sharing Platform)**	The Malware Information Sharing Platform, needs to be installed on a server in your infrastructure. You need a Web server, database and PHP support with a couple of modules. All of the data is stored on your premises and is under your control. The hardening of the server, securing the access and communication and foreseeing backups and redundancy are your	None listed	A single instance of MISP will start with an empty database. Different MISP instances can be connected to each other. This allows you to get threat	None listed	CENTRIC

		responsibility. Obviously, you fully control what happens with the data.		information from other instances and then store that data locally, which ensures that the queries for information remain confidential and limited to your server. MISP foresees four community sharing models: Share with your organization only; Share with this community only; Share with connected communities; and Share with all communities.		
4	**SAIL LABS Media Mining System**	Real-time information analysis from various media sources (OSINT); works with multiple languages; structures the data and provides visualisations and decision support information	Relies strongly on OSINT data, which might be incorrect or fake; focusses on the surface web, but not encrypted services or dark web	Collects OSINT data from various (open) sources and can provide a more holistic picture of threats, which then need to be investigated in-depth	Due to the GDPR regulations, it needs to be assessed, which personal information is included in the output; however, if it is only aggregated information, it will not provide a	SYNYO

					targeted threat analysis	
5	**Electronic Surveillance**	The data, which are collected through tracking, watching and listening, can be accessed through a central command and control center. A case management application allows to correlate and sync+M3:M23hronize data from heterogeneous sources. It also allows real time alerts when a specific event happens.	It is conceptualized as a closed and customizable surveillance system, which doesn't include further open or big data. Hence, important sources or activities of a suspect might be overlooked.	If combined with social media and open source intelligence - such as the SOCMINT solution by the same company - it provides a holistic for monitoring and surveillance of offenders.	The data are very sensitive and contain private information. Hence, data protection is crucial in this context to avoid any misuse.	SYNYO
6	**SOCMINT**	Harvests and crawls information from the surface web (social media and forums) as well as from the dark web	None listed	Allows to trace violent extremists and terrorist from the social media and the surface web to the dark web through deep web analysis	The surface and dark web analysis has strong security and privacy implications - especially when it comes to profiling, which the technology actually allows.	SYNYO
7	**Medusa**	Dealing with large amount of data disseminated in heterogeneous sources will no longer be an issue. MEDUSA® dramatically reduce the time needed to understand what is happening thanks to its sophisticated Artificial Intelligence algorithms.	None listed	Real Time Trend Analysis, Multisource, Public Sentiment and Opinion Awareness, Media Mining, Target Profiling Social Engagement	Integration and compatibility	CENTRIC

8	**Mantis (Model-based Analysis of Threat Intelligence Sources)**	An analysis platform that enables the aggregation and correlation of threat data into a unified representation based on attributed graphs. In particular, the platform is able to merge information from different exchange formats, solving the problem of analysing data contained in heterogeneous or overlapping standards. Furthermore, different threat objects that are typically analysed independently are correlated through a datatype-agnostic representation. Such an approach allows unveiling high-level relations not visible within individual threat reports and linking unconventional patterns shared between seemingly unrelated attack campaigns.	None listed	MANTIS is the first open-source platform to provide a unified representation of threat data constructs from different standards that allows for assessing the similarity between heterogeneous reports at different levels of granularity regardless of their content, size or structure. The security analyst can initiate a search for similar constructs to a related incident with a query that goes from a simple string to a full report describing a multi-faceted attack.	None listed	CENTRIC
9	**MBSIS Suite**	It combines a set of technologies for biometric investigations along face, iris, palm, finger and tattoo parameters	None listed	It is a modular and scaleable system that can be integrated into existing security IT infrastructures.	The major challenge is the integration into existing systems due to compatibility and database connections.	SYNNYO

10	**Cosain**	Features Near real time access to multiple internet data streams Securely hosted, developed and supported in the UK Automated alerting Integrates with multiple third-party tools De-duplication of volume data Intelligent location filtering Evolving machine learning capability Library of ready to use search parameters Data mining to identify key search terms GDPR / ISO27001 compliant	COSAIN's strengths lie in it's ability to be run on public sentiment analysis events as well as on evaluating threats from community disorder	Able to monitor police reputations, community tensions, and potential public disorder events.	Better for proactive analysis than investigation individuals.	CENTRIC
11	**Repknight / Skurio**	Ability to crawl and monitor dark web content, as well as detect and notify users of data breaches and user custom search monitoring of dark web sources.	The main focus of the product is on the Dark Web analytical front, meaning that there is a limitation on looking at other forms of deep web - particularly enclosed social media pages.	Able to put your data and custom databases/ taxonomies into the system, this allows them to crawl for key words matching these repositories online, and will notify you in real time if they have been discovered. This is useful for discovering insider threats, data breaches and hacking attempts on personal and private data.	Main focus on Dark Web crawling.	CENTRIC
12	**X1 Discovery**	Key Features: Collections: Data is collected and indexed from social media streams, linked content and websites through APIs, webmail connectors and direct web navigation. X1 Social Discovery aggregates data from these	Heavy reliance on APIs, some social media providers (e.g; Facebook) are increasingly moving	Allows for data to be collected form multiple social media feeds as well as documenting and hashing it as the	Reliance on APIs which in the future may become more expensive/ more	CENTRIC

		multiple sources in real time, in a highly scalable and case-centric manner. Search: Perform broad, unified searches across multiple accounts, social media streams and websites from a single interface. Linked content is automatically indexed and searched through the patented X1 fast-as-you-type search from one user interface. Results are aggregated for sorting, tagging and export consistent with standard eDiscovery or investigative, workflow. Authentication: MD5 hash values of individual items are calculated upon capture and maintained through export. Automated logging and reports are generated. Key metadata unique to social media & web streams are captured through deep integration with APIs provided by the publishers. This metadata is important to establishing chain of custody and also provides key evidence relevant to the substantive case as well as authentication. Production: Maintain data in a searchable native format from collection through production, uniquely providing a complete platform to address social media in the same manner as devices, e-mail and e-documents. Deliver collected email in PST format while maintaining hierarchical structure.	away from having these open to private/ law enforcement organisations.	crawling proceeds. This helps with the chain of evidence when reportting evidence in court.	difficult to acquire.	
13	**Threat-Arrest**	None listed	None listed	The effectiveness of the framework will be validated using a prototype implementation interconnected with real cyber systems	None listed	CENTRIC

				pilots in the areas of smart energy, healthcare and shipping, and from technical, legal and business perspectives.		
	Non European provider					
14	**I2**	Flexible analytical toolkit with modular add ins available for a variety of analyst needs. Able to produce simplified flow charts and heirarchies for presentations and court proceedings.	Expensive, some complaints that it lacks more modern features of competitor products and that it takes IBM a great deal of time/ or money to add things like new icons	Modular aspect allows for continual upgrades and new capabilities	Requires training to use, arguably some poeple contest it is slow/ out of date, runs poorly with big data sets.	CENTRIC
15	**Virtual humint**	Allows the management of multiple avatars; can be integrated in existing intelligence systems	Might not correspond with EU regulations for information security and police investigations	Supports the investigation of radicalisation and terrorist attacks planning through the infiltration of closed forums with the avatar	Especially for the EU, questions of GDPR as well as ethics and privacy compliance need to be adressed. Such information is not available online.	SYNYO
16	**GoTravel**	The monitoring system is operated on a national level and connects databases of passenger information. It allows tracing individuals as well as creating watch lists and alerts for preventing terrorist attacks. The UN, through UNOCT and OICT fully supports the	It currently only limited to air travel (flights). It does not include maritime, international	In the future, enhancements of the platform including extending the use of Artificial Intelligence	Possible expansion of scope to maritime, international	CENTRIC

		technology implementation for goTravel in relevant requesting country.	high-speed rail and coach information.	algorithms are foreseen as well as a mobile applications.	high-speed rail and coach information is under consideration.	
17	**Palantir Gothaml**	Advanced platform for data analytics, big data processing, live monitoring, taxonomy building, and intelligence documenting.	Very expensive, extensive training required to master	One of the most powerful platforms to date, ability to integrate live situational awareness data into historic and 'bottom up' datasets.	Training and cost requirement	CENTRIC
18	**Vehere**	Provides services such as speech recognition, natural language processing and behavioural analytics. Innovation and research driven.	None listed	Harnesses data from multi-sensors viz. satellite, submarine cable, web		CENTRIC
19	**HART**	HART will support at least seven types of biometric identifiers, including face and voice data, DNA, scars and tattoos, and a blanket category for “other modalities.” It will also include biographic information, like name, date of birth, physical descriptors, country of origin, and government ID numbers. And it will include highly subjective data, including information collected from officer “encounters” with the public and information about people's “relationship patterns.”	Can include highly inaccurate data. FBI and MIT research has shown that current face recognition systems misidentify people of color and women at higher rates than whites and men, and the number of mistaken IDs increases for people with darker skin tones. False positives represent real people who may erroneously	None listed	It will be shared with federal agencies outside of DHS as well as state and local law enforcement and foreign governments (might oppose First Amendment protected rights)	CENTRIC

			become suspects in a law enforcement or immigration investigation.			
20	**SecurityTrail**	The SecurityTrails API allows you to programmatically access all IP, DNS, WHOIS, and company related information that is available in the SecurityTrails Web Platform and beyond. It is based on REST principles and allows you to fetch data mainly using HTTP GET and POST methods. To be noted that API is read-only and there is no way of saving information.	None listed	APIs for Security Companies, Researchers and Teams	None listed	CENTRIC
21	**Maltego CE**	Maltego CE includes most of the same functionality as the commercial version however it has some limitations.	The main limitation with the community version is that the application cannot be used for commercial purposes and there is also a limitation on the maximum number of entities that can be returned from a single transform. In the community version of Maltego there is no graph export functionality that is available in the commercial versions.	Free and convenient abitlity to analyse soc mint data	Limited capacities	CENTRIC
22	**MASAR**	MASAR, addresses the challenges of monitoring, measuring and evaluating P/CVE programs. It helps steer designers of P/CVE programs such as yourself	Supported by the Public Safety Canada's Community Resilience	MASAR assists practitioners and policymakers in	None listed	CENTRIC

		on the right "path" to achieving measurable outcomes and projecting the impact in terms of reducing radicalisation and recruitment to violent extremism.	Fund (CRF), so is not under European Laws.	crafting a plan for MM&E of P/CVE programs and projects. It walks the policymakers through a comprehensive process for helping design better P/CVE programs, collecting information about their activities while recommending resources to support the development of goals and objectives, indicators, data collection methods and evaluation.		
	Critical technologies with a global scope					
23	**NICE Situator (PSIM solution) for building security**	Cross-channel and multi-sensor analytic	None listed	None listed	None listed	CENTRIC
24	**Hash Sharing Cosnortium**	The database now contains more than 200,000 hashes. It allows member companies to use those hashes to identify and remove matching content – videos and images – that violate our respective	Increasingly, terrorist content is shared on one platform, linking to content hosted on	It could be the seed to eradicate terrorism and extremism files from internet.	Add more companies, goverments and LEAs.	GUCI

		policies or, in some cases, block terrorist content before it is even posted. The Hash Sharing Consortium includes Ask.fm, Cloudinary, Facebook, Google, Instagram, Justpaste.it, LinkedIn, Microsoft, Verizon Media, Reddit, Snap, Twitter and Yellow.	another platform. Companies only have jurisdiction to remove the primary source content from what is hosted on their services, meaning they can remove a post, but the source link and hosted content remains intact on the 3rd party platform. There have been no formal requests from Law Enforcement or Governments to gain access to the hash sharing consortium database.			

Annex 5 Social Innovations SWOT analysis

#	Name of Social Innovation Initiative	Strengths	Weaknesses	Opportunities	Challenges	Entry added by
	Provider in the EU					
1	**The Prevent Duty**	The Prevent operates in 3 key stages of Channel and are: 1. to identify individuals at risk of being drawn into terrorism; 2. to assess the nature and extent of that risk; and 3. to develop the most appropriate support plan for the individuals concerned.	Does not provide adequate training to the teachers nor gives them the power to decide according to thier understanding of the contexts and individuals in question.	The programme relates to the general contexts of the EU countries and addresses the challenges that are most often common to these countries. So, it provides a common understanding and mechanism to operationalise similar activities.	The programme was developed in the aftermath of a wave of terrorist attacks across the country and in a sense it was rushed to supplement the existing counter-radicalisation measures. As such, it appears to not heed sufficiently the general factors e.g. social, economic, religious, and political factors that drive	CENTRIC

					individuals to extremism.	
2	**Handbook for structural Quality Standards in Deradicalisation Work**	The handbook provides the first-ever guide for implementing and monitoring quality standards in deradicalisation work.	It is written from a German perspective and against the background of the challenges of radicalisation and deradicalisation in Germany.	The handbook could be used as a framework for developing tailored criteria for other national or regional) contexts.	A lack of funding might block attempts of the adaption of the standards to other national and regional contexts.	SYNYO
3	**MotherScholls**	The work forms the missing link between women at the community level where radicalism is propagated and decision-making levels where counter violent extremism strategies are shaped.	Needs a strong engagement of the local level and the communities; it takes time and ressources for the implementation through the train the teachers approach	The program has been rolled out in several countries and is continuosly growing.	According to the organisation, it is very difficult to reach mothers (and parents in general) of right-wing extremists.	SYNYO
4	**Counter Narratives for Cuntering Violent Extremism**	The presentation/pdf offers a comprehensive overview of the concept and the implementation of counter narratives in the CVE practice	The toolkit only consists of a presentation that presents the framework related to counter narratives, but it actually neither provides actual narratives nor material for those working in the field.	The provided outline of the framework could be extended with practical information as well as with material for the practitioners. Furthermore, a good practices collection as well as links to existing resources (such as the	At the moment, the page seems to be a static repository, where no updates or follow-ups with practical resources are planned.	SYNYO

				RAN) would be beneficial.		
5	**Lifecycle Initiative Toolkit**	The toolkit provides a knowledge hub for practitioners from different field, who are looking for basic knowledge and more in-depth ressources (links) on prevention, detection/intervention and rehabilitation/reintegration.	In addition to the very basic concepts on the three main domains, the toolkit mainy provides links to documents and external resources. However, only few of the resources are actually practical guidelines.	The toolkit is well-structured and especially the initial pages provides consumable information. A major opportunity would be to provide more practical tools.	Due to the context dependency, toolkits need to rather tailored to a specific environment. Therefore, the "global" approach can only remain on the surface and refer to other sources.	SYNYO
6	**The UNESCO Guide to Stopping Violence in Schools**	The guideline covers a wide range of issues that ultimately lead to violence including radicalisation. A particular feature of this guideline lies in its strength to inform, prepare, encourage and help its subjects to make appropriate approach to stand up to problems that they feel drive them or impact them when it comes down to violence.	It is relatively outdated and needs updating. Moreover, the guideline does not particularly focus on radicalisation leading to acts of terrorism. It would have been more effective, had it been informed by contextually-specific drivers of radicalisation.	The guideline covers the basic factors of radicalisation which could be utilised as building blocks for furture similar activities.		CENTRIC
7	**Asia-Europe Counter Terroris**	This special issue of our Panorama analyses recent developments concerning Daesh extremism and their implications on societies in Asia and Europe. The papers share and discuss current and possible future	None listed	None listed	None listed	CENTRIC

	m Dialogue	threats, identify the target groups vulnerable to extreme militant ideology and examine the various recruitment channels. The counter-measures and de-radicalisation and rehabilitation efforts adopted by various governments have also been highlighted. Special attention was given to Daesh-linked activities in the respective countries, reactions by the local Muslim communities, and possible future developments as well as responses.				
8	**Extreme Dialogue**	Extreme Dialogue aims to build long-term, sustainable relationships with schools to ensure the highest levels of impact for both students and teachers.	None listed	Extreme Dialogue is open to run an Extreme Dialogue session in schools or communities.	None listed	GUCI
9	**Police-Type education as antiradical prophylaxis**	Knowledge-sharing: - best practice (policy, guidelines, learning materials, practical workshops, and tools) within the high school education area and across the private, public, and civil society sectors.	Not EU-specific (particularly from regulatory perspective)	Introduction of police type uniformed high school classess in educational systems of other EU countries.	EU Member State regulatory measures that could limit the possibilities of introduction of the initiative. E.g. restrictions in the educational area.	POZNAN
	Providers outside of the EU					
10	**A teacher's guide on the prevention of**	The guide combines global knowledge and practices from the field of radicalisation prevention in schools, and it puts them in a global guidebook.	Due to the scope of the topic and the global approach, the guide is to some extend generic.	The guide could be taken up by the EU or nation states and adapted to their particular challenges.	Although attempts such as the guide from the UNESCO exist, many organisations on	SYNYO

	violent extremism				a national or European level develop their own guidebook instead of adapting existing ones such as this one.	
11	**ReDirect**	The programme has a variety of strategies that can be applied to help young people vulnerable to being radicalised. These strategies range from simply educating individuals on the dangers of radicalisation all the way up to helping people exit radical groups. The goal of all these strategies is to keep individuals out of the formal justice system by treating the underlying causes of their turn to criminal behaviour. Moreover, the programme seeks to focus on the root causes of radicalisation which adds significance.	The programme is designed from Canada's security priority perspectives and as such, it remains limited in its scope of covering and extending to a wider geographical context such as the EU.	The guideline could be duplicated in the EU, especially the educational face of this programme offers a potential.	There is no specific reference made as to whether and how the programme could be sustained in the future or could be extended to other areas in Canada.	CENTRIC
12	**Tech Against Terrorism**	Knowledge-sharing: - best practice (policy, guidelines, learning materials, practical workshops, and tools) within the tech industry and across the private, public, and civil society sectors, including the Global Internet Forum to Counter Terrorism. - 2017 launch of Knowledge Sharing Platform, a collection of tools that startups and small tech companies can use to better protect themselves from the terrorist exploitation of their services. - Offering tech companies practical and operational support to help implement effective mechanisms to	Not EU-specific (particularly from regulatory perspective)	Cooperation with EU Internet Forum	EU Member State regulatory measures that could limit the objectives of the initiative. E.g. restrictions,orders compelling companies to provide access to user data and steps to increase	

		respond to terrorist use of the internet. - 2018 launch of Data Science Network, the world's first network of experts working on developing and deploying automated solutions to counter terrorist use of smaller tech platforms whilst respecting human rights.			greater State involvement in internet governance.	
13	**Countering Violent Extremism Curriculum**	This Curriculum delivers a contextually literate training program on countering violent extremism and awareness-raising that is relevant and accessible across regional contexts. It highlights the benefits of collaborative approaches that go beyond military or securitized responses to violent extremism and offers tools and guidance for easy adaptation to local contexts and cultures. Finally, it encourages the early identification and mitigation of risks with programming, as well as ensuring a Do No Harm approach.	Since the curriculum was developed in a relatively politicised region of the globe, it is feared that it might have compromised some features of educational activities in favour of political understanding of and approaches to counter-radicalisation.	It appears a promoting resource and is particularly significant as it has been adapted for Central Asia and MENA, the regions that have been the core of radicalisation for both EU and non-EU radical groups and individuals. So, it might be duplicated to be deployed in other similar contexts.	In terms of its applicability to the EU contexts, the resource lacks the necessary socio-economic and cultural underpinnings that are dominant in radicalisation and de-radicalisation narratives and processes.	CENTRIC
14	**Antiterrorism Assistance Programme**	ATA Program serves as a primary provider of U.S. government antiterrorism training and equipment to 53 active partner nations, building capacity to investigate, detect, deter, and disrupt terrorist activities while bolstering foreign civilian law enforcement counterterrorism skills. Through a blend of training, equipping, mentoring, advising, and consulting partner nations, ATA has successfully delivered services to 100,000+ law enforcement personnel from 154	Relatively US driven to reflect USA's security priorities in particular.	None listed	None listed	CENTRIC

		countries and has offers antiterrorism course divided into 11 main disciplines, including: Police Operations and Law Enforcement Management; Maritime & Police Training; Protection of National Leaders; Police Tactical training and Infrastructure Security; Chemical, Biological, Radiological, and Nuclear (CBRN) & Mass Casualty training; Senior Investigative & Crisis Management; Human Rights, Trends, and Cyber; Explosives; and Homeland Security.				
15	**Canadian Practitioners Network for Prevention of Radicalisation and Extremist Violence**	- Generate evidence-based best practice guidelines related to assessment, prevention, and intervention; - Identify existing assets and examine the level of collaboration through a Canada wide mapping of existing initiatives; - Strengthen collaborative resource development by and for practitioners across multiple sectors and disciplines, through capacity building in areas of high need; - Expand and improve access to the collection of evidence-based resources tailored to Canadian practitioners.	Not EU-specific (particularly from regulatory perspective)	Cooperation with EU Internet Forum	To share their experience with the EU members.	GUCI
16	**Project Someone**	The objectives of SOMEONE project are to build capacity for knowledge mobilization and transfer of the existing SOMEONE materials on a national and international scale via the following four mechanisms: - To co-develop, implement and evaluate multimedia materials and workshops to foster resilience against the ill effects of hate speech and radicalisation that leads to violent extremism with social and community	Supported by the Public Safety Canada's Community Resilience Fund (CRF) and Global Affairs Canada, so is not under European Laws.	None listed	None listed	GUCI

		organizations that work with disadvantaged communities, at-risk youth, minority communities, and aging populations, both within Canada and abroad. - To implement curricular strategies developed for the SOMEONE initiative within specific elementary, secondary, and post-secondary scholastic systems in Canada, and to begin exploring options of working with international educational counterparts in Europe and the Middle East to benefit from knowledge exchange opportunities. - To work with national and international partners in arts, culture and media – including radio, television, newspapers and web-based services – to create public engagement exercises to enable the broader public to contribute to creating alternative narratives to messages of hate and radicalisation. - To engage with expert partners in software development with the objective of creating a framework for an online database which provides rigorous, evidence-based linguistic analysis of the patterns of hate speech which are proliferated across the open online internet.				

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 740543