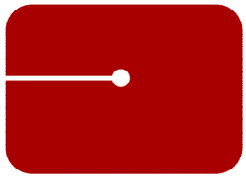

PRIME
Preventing, Interdicting and Mitigating Extremism

D7.1
Counter-Measures Review Report
Public Summary

WP7 - Counter Measures Requirements

Kacper Gradon, Agnieszka Gutkowska, Piotr Karasek
(University of Warsaw)

This research was funded by EC Grant Agreement n. 608354 (PRIME) FP7-SEC-2013-1. The information and views set out in this report are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

Table of contents

1. Introduction

Task 7.1 (Counter-Measures Review and Analysis) of Work Package WP7 (Counter-Measures Requirements) is designed to conduct a review of existing response measures intended to defend against lone actor extremist events. This has involved desktop searches and direct engagement with Subject Matter Experts and end-users with a security remit, in order to inform the identification of categories of counter-measures for which requirements must be elicited in Task 7.3 (Identification of Counter-Measures Requirements). Task 7.1 also aims to identify gaps in the defence against lone actor extremist events.

Deliverable D7.1 (Counter-Measures Review Report) presents the findings of the review of existing counter-measures used to defend against lone actor extremist events. The report identifies the existing strengths and weaknesses of these methods, and highlights areas or gaps to be addressed by further research activity.

The report focuses on the counter-measures which are presently employed at all three stages of the lone-actor threat model: radicalization, attack preparation and the attack. For the purpose of clarity within this report, we combined the measures used at the attack preparation and the attack stages. This was due to the fact that the law-enforcement agencies and security services whose responsibility it is to counter these threats use the same techniques and tactics in their work during both phases and do not distinguish them from the point of view of the application of specific methods. Our interviewees – Subject Matter Experts from the law-enforcement community – explicitly highlighted such an observation.

The deliverable includes a list of findings, summarizing the review of existing counter-measures used to defend against lone actor extremist events. The outcomes of the research are translated into a set of guidelines, taking into account the identified strengths and weaknesses of the methods assessed during the study. Due to the sensitive nature of several of the methods and techniques used by law-enforcement agencies and security services, the list of findings and guidelines cannot be considered all-inclusive, as we were not able to obtain sufficient insider information on some of these measures. However, taking into account our access to the open-source and de-classified information that we obtained, the material provided in the deliverable constitutes the current state of the art of countermeasures used to prevent and combat lone actor extremist events.

2. Methodological Approach

2.1 Overview of the research activities

The methodological approach employed to conduct the Counter-Measures Review focused on receiving reliable and practical results. Our goal was to reach information and opinions on the strategies, tactical methods and techniques related to preventing and counteracting extremist and terrorist threats currently in place. Our study covered the counter-measures referring to potential and real lone actors. The employed methodology included a review of the available academic literature, data from open sources and legal queries, as well as interviews and questionnaires with practitioners. While we hoped to get access to confidential and operational opinions and data, operational instructions on respective methods of work are available only to people with state security clearance, and publishing such operational information in a public space is illegal, so our access was limited.

2.2 Literature review

During our research we completed library queries, in order to analyse the applicable literature. We have used academic libraries located at the following Universities: the University of Warsaw (Poland), University College London (Great Britain), Universiteit van Amsterdam (the Netherlands), John Jay College of Criminal Justice (New York, the United States), University of Toronto (Canada), McGill University (Canada), as well as the central library of Harvard University (the United States). We have also made use of Police library resources and professional forensic and investigative sciences collections (National Police Academy in Szczytno, Central Police Library in Legionowo, Library of the Central Forensic Laboratory of the Police, New York Police Department Library, National Police Academy Library in Hyderabad, India). We have conducted searches of the above databases and library catalogues with a wide range of keywords related to the topic of the research performed within this work package.

It needs to be noted at this stage of our Report, that a lack of homogenous vocabulary and definitions was a big problem, as is the case with terminology referring to the notion of lone actors, and with some techniques and methods of Police work. For that reason, at the stage of library queries we noted that one of the outcomes of the PRIME project should be a development of homogenous vocabulary and a conceptual network referring to commonly applied countermeasures. Linguistic heterogeneities made our work more difficult and increased the time required to search for applicable literature for this deliverable. The materials collected as part of these library queries constituted a foundation for our work.

2.3 Legal queries

We conducted comprehensive legal queries that examined laws and judicial decisions referring to countermeasures applied to prevent and combat the activity of offenders referred to as lone actors. We investigated legal provisions on combating terrorism and the methods of work of law enforcement agencies and security services. Interestingly, the applicable legal acts available to the public show a very high level of generalisation. Specific regulations and operational instructions are highly classified and access to them is limited to a small group of people who hold the required level of security clearance. The legal analysis facilitated an effective evaluation of the usefulness of specific operational solutions to prevent and to fight terrorist threats. These legal queries allowed us to formulate a description of the counter-measures currently available to law-enforcement agencies and security services.

2.4 One-on-one consultations with practitioners

Prior to beginning work on this deliverable, we performed preliminary consultations with personnel from services and institutions responsible for combating and preventing crime and terrorism. We approached these individuals (18 in total) during conferences, working meetings, and through direct links (all of these conversations were completed between October 2014 and May 2015). The conversations were of an informal nature, and the aim of these conversations was to receive information which allowed us to adequatly focus our further enquiries, especially in reference to questions related to combating threats at the stage of Attack Preparation and Attack. The information that we received allowed us to formulate a list of counter-measures used by law-enforcement agencies and security services to combat terrorism, and provide a description of those methods which are included in this Report. It also enabled us to prepare questionnaires concerning the practical nature of these methods and measures.

We were mostly interested in responses as to whether methods of combating lone-actor terrorism differ considerably from fighting other forms of crime, such as group terrorism and "regular" criminal acts (including organized crime).It was necessary for us to determine whether methods of Police work, including operational work, differ considerably across countries representing different cultural circles and legal systems. Operational officers from a few countries we have contacted (Poland, United States, Canada, Germany and India) stated that the Police and intelligence services apply the same methods, strategies and techniques to combat lone-actor extremist events as are used to fight other forms of crime; only their adequate calibration to a specific problem is still required. Additionally, based on the consultations made, we found that the countermeasures operating in the arsenal of the law-enforcement agencies and the security services do not differ considerably across countries. They are governed by similar legal regulations and Police and other services have similar measures and

methods at their disposal. The provisions providing the grounds for applying respective solutions can differ to some extent across different EU countries, however, their practical side is, in fact, identical.

In each consultation we held, the officers we contacted maintained total anonymity. During such conversations they did not reveal any confidential details of their work. They were able to present their opinions on technical or tactical problems which affect their work, and which are not found, for political reasons, in official declarations of their institutions.

2.5 Questionnaires

As part of our work, we prepared questionnaires on the methods used by law-enforcement agencies and security services in preventing, detecting and combating lone-actor extremist events. When deciding upon a research group on which to focus, we chose to select practitioners who were representatives of law-enforcement agencies. The first survey covered a group of fifty law enforcement practitioners from Poland, Western Europe, the United States and Canada. Survey questionnaires were handed over personally or by e-mail to officers from law-enforcement agencies who were asked to provide an answer on the effectiveness, user-friendliness and costs related to the use of selected methods of Police work. The second survey, aiming at a comparison of opinions on the same issues, was conducted in September 2015 in India during a training symposium of the Indian Police held in the National Police Academy in Hyderabad, India. The survey questionnaires were given to fifty high ranking officers representing all 29 states of India.

3. Summary of activities and research findings

3.1 Introduction

The following part of the Report presents the findings of the review of existing counter-measures used to defend against lone actor extremist events. It is focused on counter-measures which are presently employed at the three stages of the lone-actor threat model: radicalization, attack preparation and the attack. As explained above in the presentation of the general objectives of this Report, for the purpose of clarity we combined measures used at the attack preparation and the attack stages. This was due to the fact that law-enforcement agencies and security services whose responsibility it is to counter these threats use the same techniques and tactics in their work during both phases and do not distinguish them from the point of view of the application of specific methods. Our interviewees – Subject Matter Experts from the law-enforcement community – explicitly highlighted this observation.

All of the consulted Subject Matter Experts, representing Police forces and Intelligence communities in Poland, the United States, Canada, the United Kingdom, Spain, Germany and India, indicated that the methods, techniques and tactical approaches used in combating the terrorist threat (including lone actor extremism) do not differ from the measures used against criminal offenders (including organised crime groups). What is different is the scale and context in which the specific method may be used as well as the calibration of such methods to the specific type of threat.

Due to the fact that the PRIME Project investigates the problem of lone-actor extremism and terrorism from a multi-level perspective, this Report does not only concentrate on the countermeasures employed at the attack preparation and the attack phases. Also, the Report does not focus only on law-enforcement perspectives. For this reason, we devoted an important part of our activities to the countermeasures that are used to prevent and mitigate radicalization. As counter-radicalization strategies play an extremely important role in responding to extremist and terrorist threats, this Report shall begin with a presentation of the policies and approaches designed to prevent radicalization.

3.2 Counter-radicalization Measures

3.2.1 Legal and institutional actions to prevent and counteract radicalisation

In October 2001, a working group tasked with developing a policy against terrorism was established within the United Nations[1]. Its aim has been to determine the directions of actions in terms of counteracting terrorism and the effect of its work were recommendations, divided into three categories, presented in September 2002 to the Secretary General. The first included 12 guidelines in terms of 'discouraging groups from taking up terrorist activity'[2]. Item 8 states that the UN Department of Public Information should develop a strategy to reach local communities susceptible to any potential agitation by terrorist organisations'[3]. In his speech of 10 March 2005 Secretary-General Kofi Annan paid attention to the need to take up such actions to 'dissuade' dissatisfied social groups from choosing terrorism as a tactic of operations. ‘The opponents reach for terrorist measures since they believe that they are effective and that they will ensure their wide social support. Such is the 'root cause' of terrorism. Our job is to prove to those groups that they are wrong.'[4]

[1] Detailed description of the documents passed and radicalisation prevention activity, see e.g. E. Bakker (2015), *EU Counter-radicalization Policies: A Comprehensive and Consistent Approach?* Intelligence and National Security, 30:2-3, 281-305
[2] http://www.unic.un.org.pl/terroryzm/polityka.php access 12.10..2015
[3] *ibidem*
[4] http://www.unic.un.org.pl/terroryzm/madryt.php

Similarly among the actions taken by the Council of Europe, support for the implementation of the UN Global Strategy to Combat Terrorism is significant, including supporting actions to prevent the radicalisation of attitudes, which could lead to terrorism. Such actions are reflected in institutions including the Committee of Experts on Terrorism (CODEXTER)[5], who are an international team established in 2003 to coordinate the actions of the Council of Europe against terrorism. Interestingly, among the most urgent tasks determined by CODEXTER itself is the analysis of the latest trends in global terrorism, including self-radicalisation, the role of the Internet in radicalisation, and the phenomenon of lone actors[6].

The European Union has also determined its own policy of combating terrorism. In 2005 the European Counter-Terrorism Strategy[7] was adopted. It divides actions taken by the EU in terms of fighting terrorism into four groups: prevention, protection, prosecution and response. 'Prevent' stands for stemming the radicalisation process by tackling its root causes and terrorist recruitment. But it is in this part of the strategy that progress has been most laggardly. Drawing on their own experiences of (largely but not solely domestic) terrorism, the EU and its member states have been acutely aware, from a very early stage in the current campaign against terrorism, that victory will not be achieved as long as the circumstances by which individuals turn into terrorists are not addressed[8]. From the perspective of actions against the causes of terrorism, the most essential in the policy of the European Union is the European Union Strategy for Combating Radicalisation and Recruitment to Terrorism, adopted in 2005[9]. The document was modified in 2008, while norms and measures to prevent radicalisation of attitudes and recruiting terrorists were divided into three major categories: disturbing the activity of persons and the network recruiting new members to become terrorists; a reassurance for moderate views to prevail over the voice of extremists; and an increase focus upon propagating security, justice, democracy and opportunities for everyone[10]. Since 2013 discussions have been held in relation to the evolution of the specific nature of terrorism in Europe and globally. Finally, in 2014 the Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism was

[5] See Comittee of Experts on Terrorism (CODEXTER), http://www.coe.int/t/dlapil/codexter/about_en.asp, accessed 29 May 2015
[6] CODEXTER, *Expected Results*, program of the leading committee 1 Jan. 2014 to 31 Dec. 2015, http://www.coe.int/t/dlapil/codexter/3_CODEXTER/TOR%202014-2015_EN.pdf accessed 30 May 2015.
[7] Council of the European Union, 30 Nov. 2005: The European Union Counter-Terrorism Strategy, see http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33275_en.htm
[8] R. Coolsaet *EU counterterrorism strategy: value added or chimera?* International Affairs, 86/4/June 2010
[9] Council of the European Union, 24 Nov. 2005: European Union Strategy for Combating Radicalisation and Recruitment to Terrorism, see: http://www.msz.gov.pl/resource/466d2bf9-c927-402d-9310-f0a25eb21d61
[10] http://www.europe-direct.poznan.pl/aktualnosci/2486/wzmocnienie-reakcji-ue-na-radykalizacje.html

adopted[11]. One of the new threats pointed out was indeed the activity of lone actor extremists as well as the problem of homegrown terrorism. The execution of the recommendations resulting from the strategy is vested mostly in the member countries[12], whereas the EU institutions must support and potentially coordinate the joint actions taken by member countries[13].

It is stressed that, despite the necessity of close cooperation between Member States, it is not possible to make the strategy and specific radicalisation prevention and combating actions homogeneous and adjust them to the specific nature (legal, cultural, technical) of all European Union Member States. This has led to a high diversity of EU projects connected with the prevention and combatting of radicalisation, which will be discussed below. However, in appreciation of the differences in experience of respective countries, the Counter-Terrorism Coordinator contacted those countries with the most experience in the field or who showed initiative in the area of counter-radicalisation operations in March 2008, with the hope that they could become a model for other countries. As a result, some specialisation has developed; e.g. Great Britain became a leader in terms of communication and the media to counter extremist narratives; Sweden (and since 2009, Belgium) in terms of community policing, especially the role of the police in perceiving the threat of radicalisation and counteracting it; Spain specialised in preparing imams; Holland in the role of local communities; and Denmark in the problem of the radicalisation of young people[14].

3.2.2 Strategic operations of European states and organizations

Not all EU member states have existing strategies to prevent radicalisation of their citizens at home and abroad. The existing ones are based on horizontal and vertical cooperation between interested parties from the local to the international level. It is recommended that domestic strategies be developed, to be related to the updated EU strategy in that field and to consider cooperation between member states and other competent entities to create innovative methods of preventing and counteracting radicalisation and violent extremism. An essential role, as part of the domestic strategies, will be played by not only the security services but also non-governmental organizations, experts and employees of various institutions in the front line of contact with people susceptible to radicalisation or who are already radicalised.

[11] http://data.consilium.europa.eu/doc/document/ST-9956-2014-INIT/en/pdf
[12] Jihadi Terrorism and the radicalisation challenge in Europe R. Coolsaet (eds.)p.149
[13] A detailed review of the chronology of legal acts on counteracting radicalisation, see E.Bakker 2015
[14] R. Coolset *EU counterterrorism strategy: value added or chimera?* In: International Affairs 86:4,2000 p. 870

It is very important for the effectiveness of counter-radicalisation activities to develop research into factors and causal mechanisms of radicalisation. Further high-quality studies which investigate the role played in the radicalisation process by violent ideology, Internet techniques of recruitment and role-models, are also necessary. Cooperation between decision-makers at the national level with scientists and academics is crucially important from a practical point of view.

Of importance is the adequate preparation of specialists that have direct contact with individuals who are at risk of radicalisation. It is necessary to make the training of specialists across Europe homogeneous, since different countries have followed different practices; some have developed training programs for different sectors, while others limit their training programs to more traditional target groups (e.g. the personnel of law-enforcement services and prison services). While facing the challenges of radicalisation, it is necessary to provide specialized training to other professional groups; e.g. social workers, teachers, child protection workers, health care services and probation officers. They are the specialists who, due to the specific nature of their contacts, have a possibility of recognising the first symptoms of vulnerability to radicalisation, far before the intervention of law-enforcement agencies is necessary. However, since their earlier professional preparation does not generally include knowledge on how the radicalisation process may appear and how best to react, it is necessary to supplement their professional competencies in a way that they could recognise and interpret the signs of radicalisation and evaluate whether an intervention is required and if so, of what type.

Bearing in mind that the process of radicalisation may take place, to differing extents, outside the European Union, e.g. in terrorist training camps or in areas of conflict, attention should be paid to the necessity of undertaking not only internal actions in the EU member states but also in partner countries; hence the European Commission stressing its the intention to continue cooperation with third countries to counteract radicalisation by the use of EU financing for training or support of the media and other bottom-up prevention initiatives.

3.2.3 Strategies against radicalisation

There are a number of support programs to counteract radicalisation and the involvement of individuals within extremist groups, which aim at either demobilisation or disengagement (abandoning violence or violent groups without abandoning the underlying ideology) or de-radicalisation (abandoning both violence and the ideology). These strategies differ in terms of the scope of their objectives, ranging from dissuading extremists from violence to the reintegration of ex-radicals into society, but they are based mostly on an individual mentor's care covering psychological support and counselling, supplemented with social and economic assistance to help

reintegration. A multi-agency approach is usually needed in order for individuals to receive the support they need.

The EU FP7 SAFIRE project conducted a search for programmes which intervened in the radicalisation process, including deradicalisation and disengagement programmes[15]. They found 87 different interventions which were referenced in the literature, and grouped them into preventative, restorative and suppressive programmes. Preventative programmes target those who are vulnerable to radicalisation, whereas suppressive programmes are at the other end of the spectrum, dealing with those who have been radicalised and may not be amenable to deradicalisation and continue to pose a threat. The vast majority of programmes are preventative or restorative (focussing on reintegration of those who may have been radicalised), attempt to both disengage and deradicalise individuals, and focus on Islamist or right-wing extremism. SAFIRE concludes that the content of programmes must be tailored to the ideology in question as well as to the individuals involved.

It is stressed that for such programs to be effective, the cooperation of both institutional support and of social support networks such as the family and friends of the radicalised individual is necessary; hence a serious emphasis on supporting a greater involvement of families, helping them recognise the radicalisation of their relatives and mitigating, or if possible preventing, such attitudes altogether. It is assumed that it is the family and those nearest who are often best predisposed to help in the de-radicalisation process, by paying attention to disturbing changes in the behaviour of their loved ones, starting discussions on difficult topics as well as searching for the effective support of a wider community (including the specialists help). Programmes for prisoners are becoming more common, but one particular focus for the future is the need to design effective counter-narratives which can be promoted and spread on the Internet – the site of so much radicalising content and activity.

3.2.4 Community Engagement and Community Policing

Several publications on the prevention of radicalisation stress the importance of community engagement and community policing. Essential elements of building such public partnership systems are information and social campaigns, with the aim of building a proper image of policing in society and developing their knowledge about potential security and crime threats. The aim of such actions is to achieve a relationship between the authorities and society in which individuals will have the

[15] 'Synthesis report on the results from work package 2: inventory of the factors of radicalization and counterterrorism interventions', p13-21 available at http://www.safire-project-results.eu/deliverables.html

desire and confidence to report 'suspicious' behaviours regarding potential radicalisation and extremism which can be verified by the competent services. It is especially important in communities which are vulnerable to radicalisation. In general, it is indicated that building confidence in the authorities within societies and developing pro-active attitudes enhances the effectiveness of law-enforcement services in terms of crime fighting[16]. Similarly, the practitioners that we interviewed said that the communities could play an essential role in preventing radicalisation and providing support to affected community members. Our interviewees stressed that 'information from informants – the community members – have a paramount practical value as the person psychologically pays attention to the aspects of behaviours which cannot be grasped from raw data analysed 'on the computer'. The data collected in a standard way are needed, important and useful but the informal information from the communities of the people close to our persons of interest (colleagues, neighbours, co-workers, social workers, doctors, teachers) can give us many more details'.

With regards to the terrorist threat, the value of implementing *community policing* is in terms of the fight both with the processes of radicalisation of lone actors (and self-radicalisation) and with the terrorist acts themselves (both of groups and 'lone actors'). Terrorists require an arena in which to act; in places where social ties are limited and where there is no mutual trust between the authorities and local residents, it is easier for potential terrorists to acquire recruits and help when executing their intentions[17]. It is also noted that the basic units of social structure (the family, local community or local public or non-public institutions), when adequately informed of the threats and not afraid of contacts with Police services, are the best line of defence against terrorist threats emenating from individuals coming from those communities[18].

Adequately selected preventive/information campaigns play a very important role in developing appropriate attitudes among citizens and employees as well as officers of law enforcement agencies in terms of terrorist threats and the best ways in which to react to them. The role of these campaigns is to 'imprint' in their audience the adequate mechanisms of acting when exposed to the threat. Those include certain mechanisms of social self-defence[19]. Such actions are also very important for attack prevention. Social campaigns must aim to convince people that normal people are the first and the last line of defence before the attacks. They try to encourage members of

[16] Zob. T.R. Tyler, J. Fagan, *Legitimacy and cooperation: why do people help the Police fight crime in their communities?,* Ohio State Journal of Criminology and Law, nr. 6/2008, s. 231-233.
[17] OSCE, *Preventing terrorism and countering violent extremism and radicalization that lead to terrorism: a community-policing approach,* online: http://www.coppra.eu/dl%5COSCE%20guidebook.pdf, accessed 19 Oct. 2015, p. 67-69.
[18] The White House, *Empowering local partners to present violent extremism in the United States,* August 2011, p. 5.
[19] Zob.: K. Liedel, P. Piasecka, *op.cit.*

a given community to notify the police of any suspicious behaviour. The police or security services must also react appropriately upon receiving this kind of information, otherwise no effective prevention can take place. A general lack of trust towards law enforcement agencies and security services, especially among people representing minorities, is often declared to be a serious problem, and one which must be tackled if communities and law enforcement agencies are to work together to combat the threat of radicalisation.

3.2.5 Recent developments in counter-radicalization

The European Commission released a document on 15 January 2014 entitled "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Preventing Radicalisation to Terrorism and Violent Extremism: Strengthening the EU's Response".[20] This communication focuses on the necessity of conducting specific actions which will facilitate the process of individuals exiting radicalised communities or facilitating deradicalisation. Its additional element, designed to protect youths from radicalisation, encourages them to look critically at extremist narratives through an adequate education. They pointed to intercultural dialogue and personal contacts between young people as key methods of developing resilience to extremist propaganda. Civic involvement and participating in social life as well as educating and school exchanges are key areas which may assist young people in being able to critically analyse the views and discourses of extremists and to reveal the defects of such propaganda, thus enhancing the promotion of positive models of behaviour and attitudes and weakening the effects of radical propaganda.

One other way of enhancing the skills of independent critical thinking is to confront potential and current extremists with former radical extremists (as those who can describe the reality of war and terrorist training camps) and with the victims of their violence. A safe and controlled method of doing so is to use narratives told by the representatives of both of those groups. The narratives told by victims of extremism and terrorism (their personal and direct experience) make potential extremists confront individual, explicit and non-anonymous effects of their actions. Such confrontation can have a greater effect on preventing radicalisation or terrorism than the work of a public organization. Demonstrating real consequences of terrorism can

[20] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and ahe Committee of the Regions: Preventing Radicalisation to Terrorism and Violent Extremism: Strengthening the EU's Response , 15.01.2014 COM(2013) 941 final, available online: http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/crisis-and-terrorism/radicalisation/docs/communication_on_preventing_radicalisation_and_violence_promoting_extremism_201301_en.pdf

be an effective counterbalance for the unilateral propaganda of extremists. Within this framework, there are projects increasing the rights of victims, both in the EU and outside the EU. Such projects make it possible for victims to tell the story of their experiences, including elements of their return to normal life and as part of the efforts aimed at the creation of new and alternative methods of communication and counter-narratives.

3.3 Countermeasures used at the Attack Preparation and the Attack Phases

Due to the specific nature of the actions of lone actors, their attacks constitute a major challenge for law-enforcement agencies. As indicated earlier, with the investigation and operational methods available, in practice no special early lone actor extremist attack detection methods have been developed. The methods applied, in fact, do overlap with those used in detecting and fighting 'traditional' crimes and differ only in their application context. Most aim at early detection and, as a result, neutralising the threat of the attack. The effectiveness of such methods varies, but we definitely cannot consider them sufficient in counteracting terrorist incidents. The scale of the threat calls for a comprehensive strategic approach to the development of methods of counteracting terrorism. These methods are summarised below.

3.3.1 Denial of Means

This approach involves depriving potential terrorists of the measures necessary to perform an attack. This includes laws restricting the availability and purchase of the physical tools and agents to be used to carry out an attack, including firearms, ammunition, explosives and other hazardous materials which can be used for that purpose. It also includes preventing terrorists from acquiring the knowledge, skills and information needed to perform a successful attack, including the construction and use of weapons, explosives and other hazardous materials as well as information on their acquisition methods and potential attack targets. This again can include laws preventing access to such information, including on the Internet, though in practical terms it is difficult to totally prevent access via this medium.

In theory, the total restriction of access to the means of both categories above would effectively counteract the occurrence of terrorist attacks. For many reasons, however, it is not possible in practice. With that in mind, the next step is the physical protection of places and people which are potential attack targets. Physical protection aims to counteract, disturb or at least minimise the damage caused by a terrorist attack[21]. This

[21] Centre for the Protection of National Infrastructure, *Protecting against terrorism,* online: http://www.cpni.gov.uk/documents/publications/2010/2010002-protecting_against_terrorism_3rd_edition.pdf?epslanguage=en-gb, accessed 10 Sept. 2015, p. 15.

can include the use of security guards and checks at buildings and infrastructure of importance, such as airports, transport terminals and government buildings.

Interestingly, all the three categories of actions are passive in nature; their application is not to identify and neutralize a threat but to prevent its occurrence or minimise the effects of the attack. No category of actions is absolutely effective; the methods are not a barrier which would be impossible to overcome. Implementing restrictions in terms of access to weapons or explosives, making access to specialist knowledge difficult or, finally, the physical protection of potential targets of terrorist attacks, facilitates introducing obstacles to planning, preparation and execution of the attacks. It is essential especially for attacks planned by individuals not acting as part of organized structures and, as such, it is a major part of anti-terrorist strategies.

3.3.2 Information Policy

This includes controlling the information available to the public after an attack in order to mitigate its effects upon the levels of fear felt by the wider population. This naturally involves close cooperation with the media, or potentially legislation to ensure their compliance with the release of information during and after an attack. While this is a potentially fruitful approach, it is incredibly difficult to enact, as the nature of the constant availability of information through the Internet in today's society encourages the media to report the latest news in a way in which to gain the most readers. There are laws in many countries requiring a level of responsibility in media reporting, but equally the freedom which the press enjoys in most democracies allows little regulation of their actions.

3.3.3 Pretextual Prosecution

Pretextual prosecution occurs in a situation where the prosecution makes charges based on suspicion of one crime but prosecutes for committing another. Thus, for example, a person suspected of murder (primary element) can in fact be prosecuted and convicted for tax fraud (secondary element). The motivation for choosing this tactic is in order to stop any future criminal activity of the suspect. This gives the prosecutor a real tool to allow the effective initiation of proceedings and prosecution. Pretextual prosecution might be used in a number of contexts, e.g. in the case of suspicion of conducting terrorist activity but where direct evidence of this activity is lacking; or in a case where proving terrorist activity would require disclosure of classified information. A circle of crimes can be pointed out, which potentially pose the *modus operandi* and are often committed by persons involved in terrorist activity. Prosecutors often file a few charges used as an excuse for conviction. Then the chances of a conviction can be increased; there is more certainty that if the court was

unfavourable to one charge, a conviction can be made on the grounds of one of the other charges[22].

3.3.4 Operational Reconnaissance

Operational reconnaissance involves performing non-classified and classified operations aiming at the acquisition of information applicable for the actions of police or intelligence services. As part of operational reconnaissance the services focus their actions on a specific committed or planned crime. The aim of the reconnaissance is to prevent a crime, and in the case where it has already been committed, to disclose its circumstances, offenders and to collect and to secure information essential for prosecution[23]. The essence of operational reconnaissance is the acquisition of some new and useful information by the services performing such reconnaissance. With that in mind, methods which are especially useful here include observation, cooperation with informants and Police intelligence.

The application of operational reconnaissance towards lone actors is, to some extent, more difficult than operational reconnaissance towards criminal and terrorist groups. When the entire planning and organization of a potential attack is made by one person only, receiving any information on their future moves may be impossible. In such a case it is necessary to focus the reconnaissance on a specific person, although, in practice it is difficult to identify the persons posing a real terrorist threat effectively, even when such individuals clearly preach radical views. It should also be remembered that the information acquired as part of operational work cannot be directly considered evidence and it requires transformation into evidence provided for in state regulations. Bearing in mind that the essence of operational work involves the acquisition of information, also in a classified way, it is absolutely essential for the services carrying out operational reconnaissance to operate based on and compliant with the law. The reconnaissance operations can naturally limit the rights and freedoms of individuals, e.g. their right to privacy, and so it is important for the services using such operations to have a clear statutory right to apply them.

3.3.5 Controlled Delivery

Controlled delivery is a method of operational work which aims to document crimes, determine the identity of the persons participating in those crimes or seize the objects used to commit a crime or derived from them. An advantage of this type of reconnaissance operations is the fact that it can be applied to prevent, accumulate

[22] B. D. Barnes, *Confronting the one-man wolf pack: adapting law enforcement and prosecution responses to the threat of lone wolf terrorism*, 2012 r., str. 1646- 1655 http://www.bu.edu/law/central/jd/organizations/journals/bulr/volume92n4/documents/BARNES.pdf
[23] Ibidem, p.64

evidence, facilitate the detection of 'dangerous' individuals and carry out reconnaissance of the structure of organised criminal networks. This may involve tracking a delivery of goods suspected to be involved in crime, or replacing those goods with other (legal or non-harmful) goods.

Controlled delivery has many advantages. It is an uncomplicated and multi-functional tool as well as being relatively simple to keep secret from the persons being infiltrated. With this method one can identify the recipient and the sender, their addresses, place of residence or place of activity. Also the recipients can be arrested *in flagranti* or its receipt can be secretely supervised in order to arrest at a time suitable for further evidence proceedings. It is a very simple, relatively cheap and important tool to ensure security, especially by paying attention to 'critical' senders or recipients of interest to the security services. Scanning the contents of international deliveries is also an important source of information to begin operational surveillance.

3.3.6 Controlled Purchase

Controlled purchase involves conducting a secret purchase, disposal or takeover of objects which are connected with a crime, are subjected to confiscation or whose production, possession, transport or retail are prohibited.[24] Controlled purchase is used in cases of those types of crimes where the possession or the intent to possess particular goods might indicate a possibility of committing that crime. The specifics of controlled purchase – primarily the necessity of a prior infiltration or at least collection of reliable intelligence – allow further investigation of the person to whom it is applied. In that case 'tracking the goods' – a product for sale or purchase – equals tracking the owner, thereby meaning a possibility of monitoring an eventual attempted crime.

It is important to note that making a sale does not usually constitute the final stage leading directly to arrest. It is a way of having control over the possession or distribution of given goods, which in later stages of the operation allows for a much wider range of accusations. Any goods, which can later be used for committing a crime, can be the subject of controlled purchase. Such flexibility of this operation offers a wide range of applications in terms of the PRIME project, for there happen to be cases of the sale or purchase of explosives or their ingredients, illegal documents (mainly passports issued by the countries of the Schengen Area) and pornographic materials.

In spite of the downsides connected with the costly observation and long-term preparation required, controlled purchase is certainly a useful method in the prosecution of potential lone actors. Each of the preparation stages brings further

[24] Art. 19 a Clause 1 of Police Act of 6 April 1990, Journal of Laws 1990 No. 30 item 179

information, the collecting and processing of which is key to the proper identification of a terrorist suspect. The obvious cost relating to the conduct of the whole operation and the significant input of forces and commitment seems to be worthwhile in terms of the possible outcomes. A confirmation of intentions to commit a crime at controlled purchase is a signal allowing the early detection of an eventual offender. Thus, controlled purchase is one of the best and most effective methods used in the case of lone actor terrorists.

3.3.7 Operational Surveillance

Operational surveillance consists of classified surveillance of correspondence and mail and the use of technical means allowing classified surveillance and recording of information and evidence, particularly the content of calls and other information shared by means of transmission networks[25]. Currently, correspondence is not just the exchange of letters, but also phone calls, exchange of text or multimedia messages. Thus, surveillance of correspondence content allows access to the content of different forms of transmission between sender and the recipient in strictly determined situations. This includes large parcels often sent across borders. Technical means include listening and registering devices, recording phone calls and any other form of distance transmission, as well as the sound and image in rooms. Operational surveillance is considered to be one of the most effective methods of acquiring information on misdeeds, offenders and evidence for their guilt. There are an extensive number of technical means of eavesdropping, starting from regular mobile phones and landlines to microtransmitters, sound amplifiers or laser devices.

3.3.8 Infiltration

Infiltration involves introducing a person to a given organization or community; the person is to acquire essential information on the actions of the group being infiltrated and to report to their principals. For obvious reasons it is a highly confidential operation and so all the documents and regulations of its application by the Police and intelligence services are covered by a confidentiality clause and not available to the public.

The role of the agent is usually assumed by Police officers or officers of other services with a special predisposition to perform such a task. One should bear in mind that the infiltration of a given community can be a time-consuming process as it is necessary for the agent to achieve the right position in the organization to facilitate access to important information. For the success of a specific operation, it is essential to keep the infiltration and the identity of the officer a secret from other group members. Any

[25] Internal Security Agency and Intelligence Agency Act of 24 May 2002 (Journal of Laws of 2002 No. 74, item 676 with further amendments) Art. 27 clause 6

disclosure of such information poses a threat to the life and health of the agent, especially in the case of the infiltration of especially dangerous groups and communities.

While the application of infiltration and its usefulness do not seem to leave any doubts, its use to counteract terrorism conducted by so-called lone actors is more questionable. First of all, one should note that the object of the infiltration is always groups, communities or organizations, and so entities with at least a few members. The essence of the operation of lone actors is their 'loneness' and so performing attacks in, at least, formal separation from specific groups or communities. The use of infiltration against such offenders seems thus inapplicable since there are no groups against which infiltration could be carried out. One should bear in mind, however, that, in practice, lone actors very rarely operate totally separately from groups and radical and/or terrorist communities, which has been stressed in the report definitions section. For that reason, infiltration of the said communities can aim to identify potential terrorists and apply other methods of operational work, e.g. observations. It is also important to note that even lone attackers sometimes have no choice but to establish contacts with crime groups, trading in firearms or explosives. The infiltration of such groups thus facilitates the acquisition of information on the individuals in possession of means or striving to gain such means to perform a potential attack. Unfortunately, due to the classified nature of those operations, there is no official data on the effectiveness of such infiltration.

3.3.9 Provocation

Provocation is built upon the participation of a so-called *agent provocateur*, who is usually an officer or staff member of the police services concealing his ties to law enforcement agencies. Civilians working as secret agents may also be among the surveillers, i.e. individuals not connected to law enforcement services. However, according to the majority of opinions these activities can only be conducted by persons authorized to do so based on legislative provision. A secret agent establishes a relationship with a criminal community in order to acquire evidence of a crime being committed. This method has been criticised when, in some cases, it has been used to entrap individuals who had not necessarily decided to embark upon terrorist activity, and in these cases such ‘sting operations’ have been unethical at best, and illegal at worst. Provocation is an extremely effective operational-reconnaissance activity if conducted by properly qualified officers. Legislature should regulate the basis for using provocation in an unambiguous manner so that it does not turn into malpractice and cross the limits to which the method described might undoubtedly lead. The effectiveness of this method has repeatedly prevented terrorist and other crimes.

3.3.10 Criminal Analysis

Criminal analysis is defined as a 'determination and presumption of relations between the data describing criminal activity and other potentially related data with the aim of the practical use of that data by the law-enforcement agencies and the courts of law'.[26] Thus, the role of criminal analysis is to support the law-enforcement agencies through the analysis of the data collected for a particular case and to plan further actions based on the analysis results acquired. Two fundamental types of criminal analysis may be distinguished: operational criminal analysis and strategic criminal analysis. The first applies to reaching a set goal in a short period of time by detecting the crime and capturing the offender. The second deals with analysing and drawing long-term conclusions and mostly concerns the study of range, directions and crime development as well as developing long-term strategies of fighting against it[27]. While conducting criminal analyses, the following analytical techniques are used: maps, statistics, Police essays or reports. The most important tool in an analyst's work, however, is the existence of adequate computer programs enabling the facilitation of comparisons of all the data collected. The information used mostly in compiling criminal analysis includes phone calls, border crossing information, funds flows, and comparison between the current case and different pending or closed cases showing similar characteristics.

Criminal analysis is a very complex method which can be divided into several types described here; some may be considered more and some less useful when combating terrorists operating without organized structures. Above all it should be noted that strategic analysis, used for developing long-term methods and concepts of fighting particular types of crime, has proven particularly significant. Its application facilitates for example identifying places or circumstances especially exposed to terrorist attacks and their proper protection. A flaw of criminal analysis in fighting lone actors is the fact that the precision of its results depends directly on the amount of information collected in a given case. Unfortunately, this type of terrorist activity, in many cases, delivers little adequate data. For this reason it is important to create databases as large as possible to facilitate the performance of more and more accurate criminal analyses. Actions focused on managing international databases and information on criminal activity, with particular regard to terrorist activity, will undoubtedly enhance the effectiveness of criminal analysis, both strategic and operational.

[26] J. Konieczny, M. Wierzbicki, *Wersje śledcze i analiza kryminalna* (in:) J. Widacki (eds.), *Kryminalistyka*, Warszawa 2002, p. 83
[27] *Ibidem,* p.84

3.3.11 Internet Monitoring and Open Source Intelligence

Open source intelligence can come from a number of locations, including the media (newspapers, periodicals, radio broadcasts, television programmes, electronic media); public data (government reports, official data (budgets, demographics), official appearances, legislature debates, press conferences, speeches); and professional and academic sources (conferences, symposia, professional corporate information, scientific articles, experts' statements).[28]

Currently, as a result of the predominant role of electronic media and modern IT technologies connected or using Internet tools, directly or indirectly, the element of Internet-based source information in the form of open-source intelligence is gaining in importance. It was already mentioned over a decade ago that open Internet-based sources are a rapidly growing area of interest for intelligence institutions, [29] and since then this tendency has clearly intensified.

With today's information society and mass communication where information is an elementary part of life, it is also a key tool of terrorist actions. Terrorists have their own TV and radio stations, channels and websites to propagate their ideas, recruit young fighters and determine the enemies they fight. They apply open-source intelligence as a channel through which they glorify and demonstrate their strength but also become an object of interest of special services which, applying open source intelligence, monitor their activity. Today terrorists use the Internet and Internet-related state-of-the-art technologies mostly to: propagate their ideologies, spread violence, and preach extremist rhetoric; encourage self-radicalisation and individual acts of terrorism; recruit and radicalise younger and younger fighters, depending on the age, via multimedia games, Internet forums, social networking services, animations, comics, films, articles, etc.; plan and coordinate terrorist actions with Internet communication tools; and provide online training, including instructional films on video hosting portals, social networking services and in digital versions of magazines created by terrorist groups.

As for counter-terrorism, each of the special services has an analytical and informative unit at their disposal, with specialists in counteracting and fighting terrorist threats, which ensures an international flow of information between various services. The services responsible for state security, responding to the actions of terrorists, under the present law can request information from private institutions. The demands for disclosing the information described by US government bodies concern mostly the

[28] M.M. Lowenthal, Intelligence. From Secrets to Policy. Fourth Edition. CQ Press, Washington D.C., 2009, p. 103.
[29] H. Fergusson, Spy: a Handbook. Bloomsbury Publishing, London, 2004, p. 81.

users of Gmail, YouTube, Google Voice and Blogger. Subpoenas, court judgements and search warrants are issued in order to gain access to required information.

The attempts of special services to fight terrorism, to a large extent, have moved to the virtual zone where a greater and greater amount of activity is demonstrated by potential attackers. Such actions involve monitoring of the media, social networking services or Internet forums. Obviously, due to the number of potential platforms of communication and the number of users, it is a task which is very complex in terms of logistics; however, according to our interviewees representing Police agencies and special services, monitoring the Internet is beginning to be the key element of the operation of special services responsible for general security and fighting crime.

3.4 Questionnaires

3.4.1. Introduction

We prepared a questionnaire concerning the methods used by law enforcement agencies and security services to prevent, detect and combat lone-actor extremist events. We decided to focus on practitioners representing the Police forces, as well as Intelligence and security services, aiming to utilise the insider perspective of the officers whose duties involve the management of investigations and countering terrorist threats.

Our preliminary inquiry concerning possible differences between the methods used for countering lone-actor extremist events compared to those used to combat group-based terrorism and other forms of crime (including organized crime and "regular" criminal activities) showed that – in the opinion of the practitioners that we consulted – there are no substantial (if any) disparities between the methods being used. Our interviewees confirmed that basically the same methods are used to counter lone actor extremist events as to combat other forms of crimes. They are, of course, specifically tailored or calibrated to the individual types of threats, but in their core they remain the same.

3.4.2 Questionnaire layout

The questionnaire concerned thirteen different countermeasures that are used by law enforcement agencies. We selected specific methods, based on the preliminary literature review and consultations with practitioners. Due to the fact that there is no uniform and universally accepted terminology concerning these measures, we decided not to use very specific terms while asking the questions, but use a semi-descriptive approach to the methods. This was suggested to us by several Subject Matter Experts that we consulted prior to the preparation of the final version of the survey.

The countermeasures that were selected for the questionnaire were as follows:

a. General reconnaissance of the communities/environments in which Lone Actors might arise or in which they operate.
b. Direct and official co-operation (through community work, meetings, cultural and social involvement), with communities/environments in which Lone Actors might arise or in which they operate.
c. Undercover operations within communities/environments in which Lone Actors might arise or in which they operate.
d. Use of informants from the communities/environments in which Lone Actors might arise or in which they operate.
e. Use of paid agents in the communities/environments in which Lone Actors might arise or in which they operate.
f. Direct sting operations/provocations against radicalized individuals and potential perpetrators.
g. Electronic (remote) surveillance of communications.
h. Undercover operations to monitor delivery of (terrorist related) goods, equipment and service (so-called controlled delivery).
i. Undercover operations to monitor purchase of (terrorist related) goods, equipment and services (so-called controlled purchase).
j. Internet monitoring (monitoring of websites, discussion boards, web forums, social networks analysis).
k. Operational/intelligence analysis.
l. Controlling the supply of certain (terrorist related) goods/services.
m. Criminalization of trade in certain goods/services (changes in legislation).

While presenting the participants with a list of thirteen countermeasures, we asked them to give their opinion on three groups of issues:

a. Difficulty level of the use of a specific method for law enforcement or security agencies. The options that the participants could choose from were: Easy, Moderate and Difficult.
b. Effectiveness of the application of a specific method for the purpose of combating lone-actor terrorist threats. The options that the participants could choose from were: Effective and Ineffective.
c. Assessment of the cost of the use of a specific countermeasure. The options that the participants could choose from were: Expensive and Inexpensive.

3.4.3 Combined Summary of Questionnaires

It is worth noting that regardless of the differences in operational practices as well as the threat types and levels, there are few differences between the answers given by

the European/American participants and their Indian counterparts. Both groups selected similar categories of countermeasures that they consider the most effective for the purpose of combating the terrorist threat.

The combined results (percentages of responses) of both questionnaires completed by the European, North American and Indian practitioners (N=100) are as follows:

	Easy	Moderate	Difficult	Expensive	Inexpensive	Effective	Ineffective
General Reconnaissance	2%	24%	74%	80%	20%	68%	32%
Cooperation with Communities	8%	38%	54%	48%	52%	68%	32%
Undercover Operations	0%	32%	68%	96%	4%	88%	12%
Use of Informants	8%	60%	32%	72%	28%	84%	16%
Use of Paid Agents	4%	46%	50%	92%	8%	60%	40%
Sting Operations	0%	18%	82%	88%	12%	76%	24%
Electronic Surveillance	20%	30%	50%	90%	10%	92%	8%
Delivery Monitoring	6%	22%	72%	94%	6%	80%	20%
Purchase Monitoring	4%	28%	68%	96%	4%	74%	26%
Internet Monitoring	16%	46%	38%	56%	44%	94%	6%
Criminal Analysis	8%	44%	48%	74%	26%	90%	10%
Supply Control	8%	24%	68%	90%	10%	74%	26%
Criminalization	20%	36%	44%	64%	36%	52%	48%

Combined data from both questionnaires completed by 100 participants show an interesting trend, where the majority of the contributors (when asked which methods they consider most effective and relevant) select operational countermeasures that are beyond the traditional notion of Police work. Three of the methods with the highest rank of effectiveness (over 90% responses) are the ones that are the most technologically advanced: Internet monitoring, electronic surveillance and criminal analysis.

The combined effectiveness hierarchy chart of the countermeasures is as follows (ranked from the most to the least effective):

1. Internet Monitoring (94% of responses).
2. Electronic Surveillance (92% of responses).
3. Criminal Analysis (90% of responses).
4. Undercover operations (88% of responses).
5. Use of Informants (84% of responses).
6. Controlled Delivery / Delivery Monitoring (80% of responses).
7. Sting Operations (76% of responses).

8a. Controlled Purchase /Purchase Monitoring (74% of responses).
8b. Supply Control (74% of responses).
9a. Reconnaissance (68% of responses).
9b. Cooperation with communities (68% of responses).

10. Paid Agents (60% of responses).
11. Criminalization / Criminal Law changes (52% of responses).

The combined hierarchy chart showing the estimated cost of use of countermeasures as assessed by the participants is as follows (ranked from the methods considered to be more expensive to the ones perceived as less expensive):

1a. Undercover operations (96% of responses).
1b. Controlled Purchase/Purchase Monitoring (96% of responses).
2. Controlled Delivery/Delivery Monitoring (94% of responses).
3. Paid Agents (92% of responses).
4a. Electronic Surveillance (90% of responses).
4b. Supply Control (90% of responses).
5. Sting Operations (88% of responses).
6. Reconnaissance (80% of responses).
7. Criminal Analysis (74% of responses).
8. Use of Informants (72% of responses).
9. Criminalization / Criminal Law changes (64% of responses).
10. Internet Monitoring (56% of responses).
11. Cooperation with communities (48% of responses).

The participants were also asked to assess the countermeasures in terms of the difficulty level of use of a specific method for law enforcement or security agencies. The options that the participants could choose from were: Easy, Moderate and Difficult. Only three countermeasures received a "double digit" score (over 10% of responses) if ranked as "Easy" by the participants. These were:

1a. Electronic surveillance (20% of responses).
1b. Criminalization/Criminal Law changes (20% of responses).
2. Internet monitoring (16% of responses).

It is worth noting that only two methods are considered both "Easy" and "Effective": Internet monitoring and electronic surveillance. Additionally, Internet monitoring is also considered an inexpensive method of law enforcement. The method that ranked high both in terms of "easiness" and "inexpensiveness" is criminalization (criminal law changes) aimed at the illegalization of trade in certain goods and services – it needs to be stressed however, that the same method is also considered the least effective.

4. Conclusions

This Report summarises a set of existing countermeasures to defend against lone actor extremist events, and acknowledged the areas to be addressed by further research activity. The most important conclusions based on the activities and findings of the Report are summarised here.

With regards to countering radicalization, community engagement and community policing, the key conclusions and problems are:

Building trust between police services and society, creating socially desirable attitudes and counteracting radicalisation provide a potentially very effective method of combating lone actor terrorism. However, at the same time, those are difficult tasks to perform which require the application of adequate techniques and strategies of operation, supported by evidence from studies carried out and earlier experience. To meet that objective, one points especially to:

- The need to create national strategies to prevent radicalisation, based on the horizontal and vertical cooperation between parties at both the local and national level. In combating radicalisation, one should apply a multi-agency approach, involving the cross-sectional cooperation of various institutions;

- The need to perform in-depth studies of radicalisation, helping to determine factors or circumstances favourable to radical attitudes, the role which ideology plays in the process of radicalisation, Internet recruitment techniques and the models to follow. Essential in this context is also the development of an adequate model of cooperation between scientists and the representatives of state authorities, in their broad sense;

- The need for adequate preparation of specialists who may have direct contact with individuals who are vulnerable to radicalisation, or who have already been radicalised. Professional training should cover not only the personnel of law-enforcement agencies but also social workers, teachers and healthcare personnel. Specially oriented training should include schoolteachers to equip them with the tools to build a cohesive and inclusive school community;

- The need to take up actions not only inside the European Union but also in partner countries. The process of radicalisation may take place outside the EU and so it can be especially important to cooperate with third countries to counteract radicalisation in areas of conflicts;

- The need to create an 'exit strategy' to enable the disengagement or even deradicalisation of individuals who have been radicalised. These support programmes should be based on an individual mentor's care combined with cooperation with the friends and family of the radicalised individual to aim to achieve their reintegration. Programmes should cover individuals who have radicalised or are vulnerable to radicalisation both for preventive purposes and after committing a crime (in prisons or when probation measures are in place). They should also involve persons returning to the European Union as foreign fighters. One should bear in mind, however, that the effective implementation of an exit strategy is not possible in every case;

- The importance of supporting families threatened with extremism. The family and friends of vulnerable individuals are crucial for preventing radicalisation. Supporting them is possible thanks to workshop programmes, development of contact points and advisers. However, one should bear in mind that the source of radicalisation can be found in the family itself;

- The need to carry out deradicalisation actions on the Internet, this being one of the primary means of transferring radical ideologies and attitudes. Such actions should include, on the one hand, combating the presence of illegal content on the Internet and, on the other hand, posting communications propagating attitudes different from extremist ones (counter-narratives). Due to the impossibility of completely clearing the Internet of illegal contents, one should focus especially on offering an easily available alternative to terrorist propaganda;

- The need to build positive relations between law-enforcement agencies and society in a way that the trust between them would allow for uninhibited communication about potential problems. Law-enforcement agencies cannot act effectively without help from civilians and to receive such assistance, trust and an adequate image of the services in a given community is required;

- The need for law-enforcement agencies to build appropriate relations with the communities threatened with radicalisation, e.g. by finding 'allies' among their members who will counteract the emergence of radical attitudes inside the community. Such people can include the clergy or other people in authority. In that context it can be valuable to take actions aiming at the Europeanisation of the ideology which radical attitudes come from (e.g. by a ban on financing foreign religious associations or creating 'local' schools for imams in Europe);

- The need to promote cross-cultural dialogue and personal contacts among young people. This is demonstrated to be a key and extremely effective

method of creating resilience to extremist propaganda. The civil involvement and participation in social life, education and exchange of young people are major areas supporting them in a critical analysis of extremist views and discourses; they allow themselves to disclose the defects of such propaganda.

With regards to the operational practices of law enforcement agencies and security services and the countermeasures employed in order to prevent and combat lone actor extremist events (including terrorist attacks) during the attack preparation and attack stages:

There is a need to create a uniform and internationally acknowledged terminology referring to the countermeasures defined as technical, tactical and operational methods of counteracting terrorist threats. Such a need was not only perceived during the preparation of this Report, where the lack of unified terminology made literature and open source reviews difficult, but it was also stressed by practitioners and Subject Matter Experts who experience difficulties in data sharing and information exchange due to the incompatibilities in the vocabulary used by different law enforcement services (even if they operate in the same linguistic environment: i.e. differences in terminology used by British, Canadian and US agencies).

The law-enforcement agencies and security services whose responsibility it is to counter lone actor extremist and terrorist threats use the same techniques and tactics (countermeasures) against and during the phases of the attack preparation and the attack itself, and they do not distinguish them from the point of view of the application of specific methods. The agencies employ the full spectrum of countermeasures both at the stage of the attack preparation and when they investigate an imminent or potential attack.

Most of the legal regulations governing operational methods and techniques are very general and do not disclose practical issues related to the actual work of the Police forces and Intelligence agencies. Such issues are usually classified and their access is limited to the very narrow audience of practitioners holding the proper security clearance. Hence, it is very difficult to access the actual "operational instructions" that govern the practicalities of investigative work.

The methods, techniques and tactical approaches used in combating the terrorist threat (including the lone actor extremism) do not differ from the measures used against criminal offenders (including organised crime groups). What is different is the scale and context in which the specific method may be used as well as the calibration of such a method to the specific type of threat.

There is a clear need for the development of cross-national databases containing information on criminal and terrorist activity that would allow the increase of the efficiency and effectiveness of data sharing and exchange. It would also enhance the effectiveness of criminal analysis, both at the strategic and operational levels.

The criminal analysis related to the problem of lone actor extremist and terrorist events suffers from the fact that the precision and accuracy of the results of such analyses is directly linked to the amount of data collected for and about the particular cases, objects, persons and events. The nature of lone actor terrorism makes this difficult to achieve, mostly because lone actor offenders leave much less information of evidential value prior to the attack preparation phase, compared to other groups or types of offenders (including group-based terrorists).

According to the literature reviews conducted for this report, consultations with Subject Matter Experts and the results of the questionnaires developed for the purpose of this Report, Internet monitoring now plays a crucial role in the work of law enforcement agencies and security services in regards to countering violent extremism and terrorism (including lone actor terrorism).

Internet monitoring as part of the operational activities of law enforcement agencies currently requires a substantial investment in technology allowing the effective surveillance of on-line communications (sometimes difficult due to the use of encryption and anonymity tools such as TOR by offenders).

The so-called operational control (including the remote surveillance and control of communications) plays an important role in countering terrorist threats, but access to counter-surveillance technologies and know-how allows offenders to disrupt the investigative strategies of law enforcement agencies.

Some of the "classic" Police and Intelligence techniques such as infiltration or undercover work may be considered ineffective and time consuming when used against lone actors, whose environment is usually difficult to penetrate by outsiders.

One of the countermeasures that is used against potential terrorists and radicalized individuals is provocation (so-called "sting operations"). It is necessary to note however, that such techniques are frequently considered to be unethical and balancing on the edge of legality; it is also stressed that such a method may lead to instances of serious breaches of law and abuse of investigative powers.

Combined data from the questionnaires completed by 100 participants (from Europe, North America and India), dealing with the effectiveness, efficiency and economy of several countermeasures that are currently available to the law-enforcement agencies and security services show an interesting trend.The majority of the contributors (when asked which methods they consider most effective and relevant) selected operational countermeasures that are beyond the traditional notion of Police work. Three of the methods with the highest rank of effectiveness (over 90% responses) are the ones that are the most technologically advanced: Internet monitoring, electronic surveillance and criminal analysis.