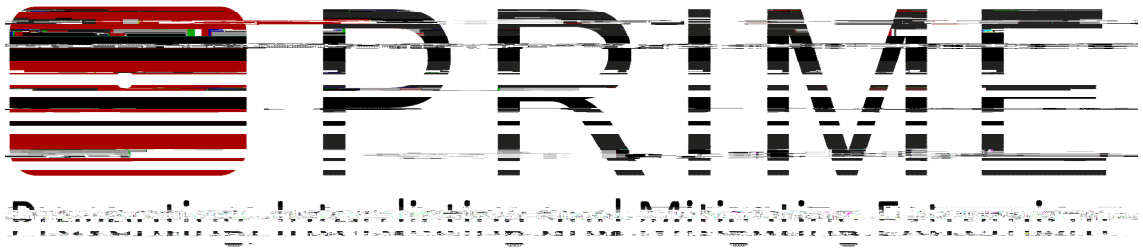

D7.1
Counter-Measures Review Report

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.

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 laattee2w1 0 0 13Ja3

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

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

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 stemmingnuonfed453.0(f)5.0(0)-2.9(5)-298.0(l)2.s0(re)-2

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".

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 ac(e)-2.3a.0(d)-4724(e)-47180(n)-4ar.0(mi)-1.9(st)5.9(2.9(f)-245.9(2.9.0

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

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

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

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]

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

users of Gmail, YouTube, Google Voice and Blogger. Subpoenas, court judgements and

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.

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).

-

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 for e nt.9(c)2.9Q7.0(f) 851-261.0(4)11.0(e)-2.0(rv)1.0(i)-1.0(c)2.9(e)-2.0(s)

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.