

*Kacper Gradoń*

## **COUNTERING LONE ACTOR TERRORISM – PRELIMINARY FINDINGS OF THE PRIME PROJECT**

### **Przeciwdziałanie terroryzmowi „samotnych wilków” – wstępne efekty projektu PRIME**

The following paper<sup>1</sup> presents the preliminary findings of the EC-funded FP7 project PRIME. Due to the sensitive nature of the problems in question and the confidential status of the Report that this publication is based on, only the non-sensitive material is provided henceforth.

PRIME – Preventing, Interdicting and Mitigating Extremist events is a collaborative research project funded under the European Commission’s Seventh Framework Programme (FP7). The research team comprises of the leading European Universities, each with a unique set of competences and expertise: University College London (Crime Science and Crime Scripting), Kings College London (radicalisation studies and risk communication), University of Warsaw (countermeasures against radicalization and terrorism), University of Leiden (counterterrorism), Aarhus University (countering radicalization) and Hebrew University of Jerusalem (lone actor attack scripting).

PRIME sets out to improve our understanding of lone actor terrorism and to inform the design of social and physical counter-measures for the prevention of lone-actor radicalisation, the disruption of lone-actor terrorist plots, and the mitigation of terrorist attacks carried out by lone extremists. Such approach is based on the behavioural matrix that we employed, known as the RAPA model and indicating the three stages of extremist behaviour (Radicalization – Attack Preparation – Attack). PRIME adopts an innovative multidisciplinary approach, which combines formal modelling techniques drawn from security engineering with relevant expertise from the ecological, social, behavioural and criminological sciences. The PRIME end product will be a decision-support tool for end-users whose remit is to deal with the lone actor terrorism threat at the local, national or international level.

The University of Warsaw team<sup>2</sup> is involved in the formulation of the so-called Counter-Measures Requirements: the strategies and techniques aimed at preventing,

---

<sup>1</sup> The Author would like to acknowledge the support from EC Grant Agreement n. 608354 (PRIME) FP7-SEC-2013-1.

<sup>2</sup> University of Warsaw PRIME team consists of Dr. Kacper Gradoń, Dr. Agnieszka Gutkowska and Mr. Piotr Karasek.

interdicting or mitigating lone actor extremist events. Our role involves a review of existing measures, which have been or can be used to prevent, interdict or mitigate lone actor extremist events, and an evaluation of their effectiveness. We also seek to identify counter-measure requirements (functions and specifications of measures which aim to disrupt the event at a particular pinch point) and integrate them, so that measures do not interfere with each other and minimize the risk of unintended consequence. Our ultimate aim is to produce a portfolio of counter-measures requirements capable of populating an intervention matrix.

The methodological approach that we employed focused on receiving reliable and practical results. Due to the fact that the topic we diagnose falls within the field of social sciences, we did our best not to make our research theoretical in nature but to reflect real situations and problems. It was our goal to reach information and opinions on the strategies, tactical methods and techniques related to the prevention and counteracting extremist and terrorist threats currently in place. Our study covered the counter-measures referring to potential and real lone actors. Several of our observations were based on a review of the available academic literature, data from open sources and legal queries. We also performed thorough consultations and interviews with practitioners – namely the personnel of the services and institutions (Police and Intelligence agencies) responsible for combating and preventing crime and terrorism (in Poland, Western Europe, North America, Israel and India). The information that we received had a two-fold benefit for our work: firstly, it allowed us to formulate a list of counter-measures used by the law-enforcement agencies and security services to combat terrorism and their thorough description; secondly, it enabled us to prepare the questionnaires concerning the practical nature of these methods and measures. The questionnaires concerned the methods used by the law-enforcement agencies and security services in preventing, detecting and combating lone-actor extremist events. Selecting a research group, we focused exclusively on practitioners (representatives of the 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 consulted Subject Matter Experts, representing the Police forces and Intelligence communities of Poland, United States, Canada, United Kingdom, Spain, Germany and India indicated that 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 the 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 the threat.

As one of our interlocutors noted, “The same operational methods are used against the whole spectrum of criminals, without prior differentiation if they are the terrorists, drug dealers or burglars. (...) Methods used by the Police and security services are very similar, they are just modified depending on the specific case. We can use them against both the ‘common’ criminals and against lone wolf terrorists.” The other officer noted: “There are no general differences between the types of methods and the

ways we use them. Each case that we investigate is unique and we never use a countermeasure in exactly the same way. The methods might differ depending on the specific context of the case, but our skills and tools remain the same”. The practitioners that we interviewed shared a very similar approach, regardless of the country and the type of service (Police, Intelligence) that they work for. They also stressed that their respective agencies employ the full spectrum of countermeasures both at the stage of the attack preparation and when they investigate the imminent or potential attack.

In our research, apart from the methods and approaches used to prevent and combat radicalization, we focused preliminarily on the countermeasures used at the Attack Preparation and the Attack Phases of the lone-actor terrorism scenario. The measures that we considered in our analysis included the Denial of Means strategies (restricting access to physical tools and agents to be used to perform an attack; restricting access to knowledge, skills and information; physical protection of potential attack targets), Pretextual (Pre-emptive) prosecution; Operational reconnaissance; Controlled delivery; Operational surveillance; Infiltration; Provocation; Criminal analysis; Internet monitoring; Open Source Intelligence. We thoroughly describe these methods, taking into account the practical implications of their use, the legal grounds governing their application, and both the limitations and benefits of each of the measures. Such analysis allowed us to formulate the questionnaire that we then used to assess the ranking of the countermeasures in terms of their application to the problem of extremism and lone-actor terrorism. We decided to focus on the practitioners representing the Police forces, as well as Intelligence and security services, aiming at the insider perspective of the officers whose duties involve the management of investigations and countering terrorist threats.

Our preliminary inquiry concerning the possible differences between the methods used for countering lone-actor extremist events in comparison with the 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 interlocutors confirmed that basically the very same methods are used to countering lone actor extremist events as to combating 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.

The questionnaire concerned thirteen different countermeasures that are used by the 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 the very specific terms while asking the questions, but use the semi-descriptive approach to the methods. It was suggested to us by several Subject Matter Experts that we consulted prior to the preparation of the final version of the survey. For example, when asking about the official involvement of the Police force in the direct co-operation with the segments of the society from which the potential or actual lone actors might arise from, we used the descriptive statement: “Is 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?”. We constructed all of the questions in a following manner, in order to avoid misunderstanding or misinterpretation of our queries.

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 the law enforcement or security agency. 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 threat. The options that the participants could choose from were: Effective and Ineffective.
- c) Assessment of the cost of use of a specific countermeasure. The options that the participants could choose from were: Expensive and Inexpensive.

The first study (completed between July and October 2015) consisted of fifty participants – the practitioners representing the law-enforcement agencies, intelligence and security services. These were the high-ranking officers with at least 15 years of professional experience, whose job (either exclusively or partially) involves countering terrorism and violent crime. The participants came from the variety of European

and North American countries: Poland, Germany, France, United Kingdom, Spain, United States and Canada. They questionnaires were handed over to them personally (on the occasions such as working meetings, consultations, or during the conferences held in The Hague, Forth Worth (Texas), Warsaw, New York, Boston, Montreal, Toronto and Prague). Due to the specific nature of the audience that we approached, it was not possible to prepare neither the quantitative nor qualitative study (in accordance with the rules governing the sociological research) – we were not able to draw the representative sample, because it was not possible to enforce the completion of the questionnaire by the drawn respondents. Similarly, the participants did not allow us to perform the personal interviews and only agreed to take part in the general survey study – hence the lack of the proper qualitative approach. Our preliminary pilot study allowed us to estimate that (taking into account the specific audience), we were only able to choose between the estimated study (that is: the general questionnaire) and terminating the empirical part of our research. Only the persons who agreed to participate were given the questionnaires.

All of the participants were first presented with the overview of the PRIME Project and with the explanation of the objective of PRIME in regards to the prevention, interdiction and mitigation of the lone actor extremist events. It was also explained to them that the questionnaire concerns the difficulty level, effectiveness and cost assessment of several countermeasures used against such threats. The participants were assured that the questionnaires are fully anonymous. No personal information enabling their identification was elicited from the studied population. The first page of the questionnaire gave further explanation of the PRIME Project as well as the re-assurance of the survey’s anonymity.

The statistical results (percentages of responses) of the questionnaires completed by the participants representing the European and North American agencies (N = 50) are as follows:

	Easy	Moder.	Diffic.	Expens.	Inexpens.	Effect.	Ineffect.
General Reconnaissance	0%	32%	68%	84%	16%	64%	36%
Cooperation w. Communities	4%	56%	40%	40%	60%	68%	32%
Undercover Operations	0%	40%	60%	96%	4%	84%	16%
Use of Informants	4%	72%	24%	60%	40%	84%	16%
Use of Paid Agents	4%	56%	40%	96%	4%	60%	40%
Sting Operations	0%	20%	80%	96%	4%	60%	40%

Electronic Surveillance	20%	40%	40%	84%	16%	96%	4%
Delivery Monitoring	8%	24%	68%	92%	8%	84%	16%
Purchase Monitoring	4%	32%	64%	100%	0%	68%	32%
Internet Monitoring	24%	48%	28%	40%	60%	96%	4%
Criminal Analysis	4%	64%	32%	80%	20%	84%	16%
Supply Control	4%	32%	64%	100%	0%	64%	36%
Criminalization (Law changes)	20%	32%	48%	76%	24%	28%	72%

The statistical results (number of responses) of the questionnaires completed by the participants representing the European and North American agencies (N = 50) are as follows:

	Easy	Moderate	Difficult	Expensive	Inexpens.	Effective	Ineffective
Reconnaissance	0	16	34	42	8	32	18
Co-op w/co	2	28	20	20	30	34	16
Undercover	0	20	30	48	2	42	8
Informants	2	36	12	30	20	42	8
Paid Agents	2	28	20	48	2	30	20
Sting Oper.	0	10	40	48	2	30	20
Elect. Surv.	10	20	20	42	8	48	2
Deliv. Mon.	4	12	34	46	4	42	8
Purch. Mon	2	16	32	50	0	34	16
Internet	12	24	14	20	30	48	2

CrimAnalys	2	32	16	40	10	42	8
SupplyCtrl	2	16	32	50	0	32	18
Crimin. Law	10	16	24	38	12	14	36

Whereby:

- “Reconnaiss” is: General reconnaissance of the communities/environments in which Lone Actors might arise or in which they operate.
- “Co-op w/co” is: 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.
- “Undercover” is: Undercover operations within communities/environments in which Lone Actors might arise or in which they operate.
- “Informants” is: Use of informants from the communities/environments in which Lone Actors might arise or in which they operate.
- “Paid Agents” is: Use of paid agents in the communities/environments in which Lone Actors might arise or in which they operate.
- “Sting Oper.” is: Direct sting operations / provocations against radicalized individuals and potential perpetrators.
- “Elect. Surv.” is: Electronic (remote) surveillance of communications.
- “Deliv. Mon.” is: Undercover operations to monitor delivery of (terrorist related) goods, equipment and service (so-called controlled delivery).
- “Purch. Mon.” is: Undercover operations to monitor purchase of (terrorist related) goods, equipment and services (so-called controlled purchase).
- “Internet” is: Internet monitoring (monitoring of websites, discussion boards, web forums, social networks analysis).
- “CrimAnalys” is: Operational/intelligence analysis.
- “SupplyCtrl” is: Controlling the supply of certain (terrorist related) goods/services.
- “CriminLaw” is: Criminalization of trade in certain goods/services (changes in legislation).

The top six methods (out of thirteen) methods that were assessed as the most effective by the majority of the participants representing the European and North American agencies were (in order from the highest to the lowest rate of approval): Internet Monitoring, Electronic Surveillance, Criminal Analysis, Use of Informants, Undercover Operations and the Controlled Delivery.

The second study (completed in October 2015) was designed for comparative purposes and consisted of fifty participants – the practitioners representing the Police forces of all 29 States of India. The occasion for such a study was my participation in the Government of India Phase IV Masterclass Training Programme (MCTP) for India Police held at the National Police Academy in Hyderabad. The participants were the top-ranking officers with at least 20 years of professional experience, whose job



(either exclusively or partially) involves countering terrorism and violent crime. They questionnaires were handed over to them personally and only persons who agreed to participate were given the survey documents. As explained above (section describing the European and American questionnaires), we could only perform the estimated study, so they can not be considered representative (we had no authority to enforce the completion of the survey; similarly, our respondents allowed us only to use the brief and general questionnaire).

As in the case of the European and American questionnaires, all of the participants were first presented with the overview of the PRIME Project and with the explanation of the objective of PRIME in regards to the prevention, interdiction and mitigation of the lone actor extremist events. It was also explained to them that the questionnaire concerns the difficulty level, effectiveness and cost assessment of several countermeasures used against such threats. The participants were assured that the questionnaires are fully anonymous. No personal information enabling their identification was elicited from the studied population. The first page of the questionnaire gave further explanation of the PRIME Project as well as the re-assurance of the survey's anonymity.

The statistical results (percentages of responses) of the questionnaires completed by the participants representing the Indian Police (N = 50) are as follows:

	Easy	Moder.	Diffic.	Expens.	Inexpens.	Effect.	Ineffect.
General Reconnaissance	4%	16%	80%	76%	24%	72%	28%
Cooperation w. Communities	12%	20%	68%	56%	44%	68%	32%
Undercover Operations	0%	24%	76%	96%	4%	92%	8%
Use of Informants	12%	48%	40%	84%	16%	84%	16%
Use of Paid Agents	4%	36%	60%	88%	12%	60%	40%
Sting Operations	0%	16%	84%	92%	8%	56%	44%
Electronic Surveillance	20%	20%	60%	96%	4%	88%	12%
Delivery Monitoring	4%	20%	76%	96%	4%	76%	24%
Purchase Monitoring	4%	24%	72%	92%	8%	80%	20%
Internet Monitoring	8%	44%	48%	72%	28%	92%	8%



Criminal Analysis	12%	24%	64%	68%	32%	96%	4%
Supply Control	12%	16%	72%	80%	20%	84%	16%
Criminalization (Law changes)	20%	40%	40%	52%	48%	76%	24%

The statistical results (number of responses) of the questionnaires completed by the participants representing the Indian Police (N = 50) are as follows:

	Easy	Moderate	Difficult	Expensive	Inexpens.	Effective	Ineffective
Reconnaiss.	2	8	40	38	12	36	14
Co-op w/co	6	10	34	28	22	34	16
Undercover	0	12	38	48	2	46	4
Informants	6	24	20	42	8	42	8
Paid Agents	2	18	30	44	6	30	20
Sting Oper.	0	8	42	46	4	28	22
Elect. Surv.	10	10	30	48	2	44	6
Deliv. Mon.	2	10	38	48	2	38	12
Purch. Mon	2	12	36	46	4	40	10
Internet	4	22	24	36	14	46	4
CrimAnalys	6	12	32	34	16	48	2
SupplyCtrl	6	8	36	40	10	42	8
Crimin. Law	10	20	20	26	24	38	12

Whereby:

- “Reconnaiss” is: General reconnaissance of the communities/environments in which Lone Actors might arise or in which they operate.
- “Co-op w/co” is: 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.

- “Undercover” is: Undercover operations within communities/environments in which Lone Actors might arise or in which they operate.
- “Informants” is: Use of informants from the communities/environments in which Lone Actors might arise or in which they operate.
- “Paid Agents” is: Use of paid agents in the communities/environments in which Lone Actors might arise or in which they operate.
- “Sting Oper.” is: Direct sting operations / provocations against radicalized individuals and potential perpetrators.
- “Elect. Surv.” is: Electronic (remote) surveillance of communications.
- “Deliv. Mon.” is: Undercover operations to monitor delivery of (terrorist related) goods, equipment and service (so-called controlled delivery).
- “Purch. Mon.” is: Undercover operations to monitor purchase of (terrorist related) goods, equipment and services (so-called controlled purchase).
- “Internet” is: Internet monitoring (monitoring of websites, discussion boards, web forums, social networks analysis).
- “CrimAnalys” is: Operational/intelligence analysis.
- “SupplyCtrl” is: Controlling the supply of certain (terrorist related) goods/services.
- “CriminLaw” is: Criminalization of trade in certain goods/services (changes in legislation).

The top six methods (out of thirteen) methods that were assessed as the most effective by the majority of the participants representing the Indian Police forces were (in order from the highest to the lowest rate of approval): Criminal analysis, Internet Monitoring, Undercover Operations, Electronic Surveillance, Supply Control and the Use of Informants.

It is worth noting that regardless of the differences in operational practices as well as the threat types and levels, there are not too many differences between the answers given by the European/American participants and their Indian counterparts. Both groups selected highly similar categories of the countermeasures that they consider the most effective for the purpose of combating the terrorist threat.

The combined statistical 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	Inexpens.	Effective	Ineffective
Reconnaiss.	2%	24%	74%	80%	20%	68%	32%
Co-op w/co	8%	38%	54%	48%	52%	68%	32%
Undercover	0%	32%	68%	96%	4%	88%	12%
Informants	8%	60%	32%	72%	28%	84%	16%
Paid Agents	4%	46%	50%	92%	8%	60%	40%
Sting Oper.	0%	18%	82%	88%	12%	76%	24%

Elect. Surv.	20%	30%	50%	90%	10%	92%	8%
Deliv. Mon.	6%	22%	72%	94%	6%	80%	20%
Purch. Mon	4%	28%	68%	96%	4%	74%	26%
Internet	16%	46%	38%	56%	44%	94%	6%
CrimAnalys	8%	44%	48%	74%	26%	90%	10%
SupplyCtrl	8%	24%	68%	90%	10%	74%	26%
Crimin. Law	20%	36%	44%	64%	36%	52%	48%

Whereby:

- “Reconnaiss” is: General reconnaissance of the communities/environments in which Lone Actors might arise or in which they operate.
- “Co-op w/co” is: 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.
- “Undercover” is: Undercover operations within communities/environments in which Lone Actors might arise or in which they operate.
- “Informants” is: Use of informants from the communities/environments in which Lone Actors might arise or in which they operate.
- “Paid Agents” is: Use of paid agents in the communities/environments in which Lone Actors might arise or in which they operate.
- “Sting Oper.” is: Direct sting operations / provocations against radicalized individuals and potential perpetrators.
- “Elect. Surv.” is: Electronic (remote) surveillance of communications.
- “Deliv. Mon.” is: Undercover operations to monitor delivery of (terrorist related) goods, equipment and service (so-called controlled delivery).
- “Purch. Mon.” is: Undercover operations to monitor purchase of (terrorist related) goods, equipment and services (so-called controlled purchase).
- “Internet” is: Internet monitoring (monitoring of websites, discussion boards, web forums, social networks analysis).
- “CrimAnalys” is: Operational/intelligence analysis.
- “SupplyCtrl” is: Controlling the supply of certain (terrorist related) goods/ services.
- “CriminLaw” is: Criminalization of trade in certain goods/services (changes in legislation).

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 the operational countermeasures that are beyond the traditional notion of a 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 coalesced 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 the law enforcement or security agencies. The options that the participants could choose from were: Easy, Moderate and Difficult. Only three countermeasures received the “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”: the Internet monitoring and the electronic surveillance. Additionally, the Internet monitoring is also considered the inexpensive method of the law enforcement. The method that ranked high both in terms of “easiness” and “inexpensiveness” is the

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.

In summary, the 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, where the majority of the contributors (when asked which methods they consider most effective and relevant) select the operational countermeasures that are beyond the traditional notion of a 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.

### **Streszczenie**

Artykuł przedstawia deklasyfikowane wstępne wyniki finansowanego przez Komisję Europejską projektu badawczego FP7 PRIME, poświęconego ekstremizmowi, radykalizacji i terroryzmowi sprawców określanym mianem tzw. samotnych wilków. Przedstawiono wyniki badań odnoszących się do metod zwalczania tego rodzaju zagrożeń na etapach przygotowania i dokonania ataku. Analizie poddano trzynaście metod pracy policyjnej i wywiadowczej, ocenianych z punktu widzenia ich efektywności, łatwości wykorzystania i kosztów związanych z ich użyciem przez organa ścigania i instytucje odpowiedzialne za bezpieczeństwo i porządek publiczny.

**Słowa kluczowe:** ekstremizm; radykalizacja; terroryzm; samotni sprawcy; terroryzm samotnych wilków; PRIME; zwalczanie terroryzmu; policja; wywiad; służby specjalne; monitoring Internetu; biały wywiad; OSInt

### **Summary**

The paper presents the de-classified preliminary findings of the European Commission funded FP7 research project PRIME, dealing with the extremism, radicalization and lone-actor terrorism (also known as “lone wolf terrorism”). The Article provides the results of the research devoted to the existing counter-measures used against such threats during the stages of Attack Preparation and Attack Execution. Thirteen such Police and Intelligence methods were analysed from the point of view of their effectiveness, ease of use and costs associated with them, from the point of view of the law-enforcement agencies and security services.

**Keywords:** extremism; radicalization; terrorism; lone actors; lone wolf terrorism; PRIME; counter-terrorism; Police; Intelligence; special services; Internet monitoring; Open Source Intelligence; OSInt