Kacper Gradoń
University of Warsaw

COUNTERING LONE-ACTOR TERRORISM: SPECIFICATION OF REQUIREMENTS FOR POTENTIAL INTERVENTIONS

The following article[1] presents the partial 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 PRIME Report that this publication is based on, only the non-sensitive material is provided henceforth.

THE PRIME PROJECT

Preventing, Interdicting and Mitigating Extremist Events (PRIME)[2] was a collaborative research project funded under the European Union's Seventh Framework Programme (FP7). PRIME started on 1 May 2014 and is completed on the 30 April 2017. The PRIME Consortium consisted of the representatives of six Universities: University College London (UK), Kings College London (UK), University of Warsaw (Poland)[3], University of Leiden (the Netherlands), Aarhus University (Denmark) and Hebrew University of Jerusalem (Israel).

PRIME sets out to improve our understanding of lone actor terrorism and to inform about 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. In this endeavour,

[1] The statements expressed in this Paper represent only the views of the University of Warsaw PRIME team and in no way they can be interpreted as the official opinions of either the European Commission or other members of the PRIME Project Consortium.

[2] The Author would like to acknowledge the support from EC Grant Agreement n. 608354 (PRIME) FP7-SEC-2013-1. The Author would also like to acknowledge the support of the Ministry of Science and Higher Education of the Republic of Poland (Ministerstwo Nauki i Szkolnictwa Wyższego RP).

[3] University of Warsaw PRIME team consists of Dr. Kacper Gradon, Dr. Agnieszka Gutkowska and Mr. Piotr Karasek representing Faculty of Law and Administration.

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 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.

PRIME's research activities involve a range of social scientific research methodologies, for the purpose of collecting empirical data needed to produce scripts (meta-script and sub-scripts) of lone-actor extremist events (LAEE). The ultimate aim so-produced of the scripts will be to enable the identification of "pinch points", where interventions (i.e. counter-measures) can be implemented to prevent, disrupt or mitigate lone-actor terrorist activity.

PRIME seeks to go beyond the state of the art in the study of lone-actor extremism in a number of ways: first, by modelling factors, processes and indicators associated with LAEEs on several levels of analysis – individual, situational, social ecological and systemic – and, secondly, by developing for this purpose a more rigorous scripting methodology than has heretofore been used in the study of terrorism specifically, or in the field of crime analysis more generally.

PRIME COUNTER-MEASURES

The objectives of PRIME section run by University of Warsaw team (Counter-Measures Requirements) were to review and analyse existing counter-measures to lone actor extremist events, to establish a set of counter-measures requirements based on the pinch points derived from the integrated script and to produce a framework in support of decision-making, allowing stakeholders to anticipate interdependencies between counter-measures and to take into account contextual factors when selecting counter-measures.

The final stage of the PRIME activities was the preparation and presentation of the portfolio of lone actor extremism counter-measures requirements based on the findings of the review of existing counter-measures used to defend against lone actor extremist events.

The University of Warsaw team was responsible for the preparation of the White Paper providing the description of the counter-measures applicable at three stages of the lone-actor threat model: radicalization, attack preparation, and attack. For the purpose of the clarity of our 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 applica-

tion of specific methods. Our interlocutors – Subject Matter Experts from the law-enforcement community – explicitly highlighted such an observation. The White Paper concludes with a list of recommendations, which shall be considered in order to prevent, interdict and mitigate the threat of lone actor extremism and terrorism and to support public security and safety. These recommendations are based on the extensive consultations with law-enforcement and security services practitioners and Subject Matter Experts of the PRIME Project domain, representing a wide range of areas (police, intelligence, border protection, military, government, civil defence, non-governmental organizations, and the academic community) and different jurisdictions and law practices (several countries of Europe, United States, Canada, India, Japan, Georgia, Mexico, Australia and New Zealand).

METHODOLOGY

Preparation of the Counter-Measures White Paper required us to focus on the most practical aspects of countermeasures used to prevent, mitigate and interdict lone actor extremist events at three stages of the development of violent behaviour, which are: radicalization, attack preparation and the attack itself. Our objective was to present a set of recommendations aimed at the improvement of the current situation in the domain of the law-enforcement and security services, whose responsibilities include countering radicalization, violent extremism and terrorism.

As a part of the research, the team from the University of Warsaw received additional information from practitioners representing law-enforcement, intelligence and security services. Due to institutional limitations, the nature of issues being investigated, and confidentiality issues, all of the interviewed experts wished to remain anonymous. Their statements cannot be interpreted as the official views of their respective institutions, but we decided to include these observations in this report, as they present a direct commentary to the problem of countering lone actor extremism, unbiased by institutional and political interference.

The contact with practitioners was established both through direct and indirect links and interactions arising from previous collaborations unrelated to PRIME Project, as well as partnerships founded throughout the PRIME-related research. Almost all of the contacts were personal (on one-to-one basis), and out of respect for the full confidentiality conditions, the conversations were never recorded and only note taking was agreed on. Some of the discussions were limited to highly general questions (as the respondents could not refer to specifics,

due to the nature of their work) and in other cases we were allowed to get more insight, when the information presented could be provide in detail, but without jeopardizing the disclosure of the source of such data. The conditions of police work make it complicated and time-consuming to gain trust of police officers. Providing anonymity to our interlocutors on every step of obtaining and processing data was a prerequisite for such talks to happen at all. An important element of these arrangements was presenting the information in such a way that identifying a particular specialist by naming the unit in which they worked during the interview was impossible.

The law enforcement specialists represented a wide array of institutions from several countries. The persons interviewed had police, border guard, intelligence, counter-intelligence, military, government and special services background. We intended to consult practitioners representing the widest possible group of countries, in order to provide a comprehensive assessment of methods and techniques that are or may be used to counter terrorism and violent extremism. We had the unique opportunity of receiving comments from law enforcement operatives representing several regions of the world, different jurisdictions and policing practices.

In most cases we had the opportunity to receive information from single representatives of services. Sometimes we could talk to a few people representing one institution. In such cases, it is clearly stated whether an opinion comes from one person or from a group.

The interviews we held with 132 officers and took place in different countries of Europe (Poland – 12 people in total, Austria – 6 people, Germany – 6 people, Italy – 8 people, Spain – 7 people, Portugal – 4 people, Hungary – 4 people, Georgia – 6 people), North America (United States – 35 people in total, Canada – 10 people, Mexico – 4 people), as well as in India (10 people), Australia (10 people), New Zealand (6 people) and Japan (4 people). Such a choice of countries was solely based on the possibility of obtaining direct access to practitioners. Despite our efforts, we were unable to contact specialists from other countries or they were unwilling to share information. In a few cases we only received very short answers devoid of greater cognitive value. In justified situations we quote these short answers as comments to more detailed explanations.

Due to the fact that most of our interlocutors did not have enough time and/or did not want to participate in anything but a direct conversation, we were not able to employ any questionnaire or survey approach. The same applies to the structured interview technique. In the overwhelming majority of the cases, we used the semi-structured interview approach. As the length, detail level and conditions of the interviews varied significantly, it was impossible to draw statistical analysis based on the outcomes of our conversations. It was however possible to find common patterns that we could then translate to a set of universal conclusions. Our scientific experience shows that qualitative approach is significantly

better in regard to such specific communities as law-enforcement and security services, as quantitative research is substantially impacted by either direct distrust or unwillingness to respond to some, most or even all questions if they are presented in a written form. Such observation was confirmed at the earlier stage of our research, where we were able to pursue the questionnaire/survey approach, but the outcomes were very limited due to the factors mentioned above. Hence, the focus on direct statements from the operational personnel, whose opinions might occasionally be considered anecdotal and/or subjective, but more often have substantial evidential value unaffected by the political interference of the official line presented by their respective institutions.

DEFINING THE TERMS

One of the first comments that occurred in the majority of interviews was confirming that there is no unanimity as to the very definition of lone actor extremism. We realized again that practitioners differ not only in terminology used, but also – depending on the issues they face in their work – they define the concept of "lone wolf terrorist" in a narrowing or (more frequently) in a broader way. They stressed that there are practically no "true lone wolves operating in the vacuum" (it was an opinion of all our interlocutors, who usually gave the isolated and highly unique example of Theodore Kaczynski (the Unabomber), with a frequent remark that even perpetrators such as Anders Behring Breivik established some kind of contacts with the "outside world"). In most cases we received answers indicating that "lone actors" are persons who (usually) act alone, but at the same time remain influenced by an outside ideology, a set of hints, recommendations given more or less directly by outside groups and organizations. A number of respondents used – consciously or unknowingly – terms similar to the one used by Brian Jenkins (RAND Corporation), who referred to "stray dogs" instead of "lone wolves", explaining that "stray dogs (…) may be found alone or in packs, estranged from but dependent on society, streetwise but lacking social skills, barking defiantly, and potentially dangerous but at the same time, suspicious, fearful, skittish. (…) They wander about in the shade of jihadist ideology, sniffing at the edges of violence before making a move"[4].

From a practical point of view, it is important to pay attention to the opinion of experts dealing with police response at the stage of the actual attack. An interesting observation was raised by the US Police hostage and crisis negotiators,

[4] B. M. Jenkins, *Stray Dogs and Virtual Armies. Radicalisation and Recruitment to Jihadist Terrorism in the United States Since 9/11*, RAND Corporation 2011, pp. 21–22.

further confirmed by their field manuals[5]. While discussing law-enforcement crisis management strategies, they specifically highlight the category of persons that they refer to as "Violent True Believers", that are put in the same operational classification as the "the lone wolves" or persons involved in the "leaderless resistance"[6]. The crisis negotiators claim that "Violent True Believers" (VTB) can be encountered across the full spectrum of law enforcement, from a patrol encounter, through a multi-jurisdictional response, to a mass casualty event. Not all VTB incidents are terror plots per se, but often unplanned violence occurs when authorities confront a volatile political extremist for any reasons. The negotiators are trained to explore common characteristics of "Violent True Believers" and act accordingly. They need to gather intelligence to identify the source of their personal grievance, but during the actual negotiations phase they must not debate the accuracy or legitimacy of these claims. VTB may claim that they are a part of a larger group of people who are abused or mistreated, so their moral outrage might cause them to become even less rational. The crisis management experts stress that the ideology held by the VTB may be obvious or nearly unrecognizable from the original ideology from which they (as the negotiators called it) "cherry picked" their beliefs. Crisis negotiators stress that, at the stage of an attack or standoff involving the "Violent True Believer", it is crucial to leverage investigative resources as soon as possible. Acting alone (VTB, lone wolf, lone actor) may mean that there is a trail of evidence, as the person involved had to make all the purchases, conduct all the reconnaissance, prepare all the equipment and conduct the operation on their own. Such intelligence can then be used directly (to enhance negotiations or to prepare a tactical approach), or indirectly – to understand and strategically analyze the modus operandi of the specific group of perpetrators in order to use it as a preventive tool to interdict future events of similar kind or the copycat attacks.

Still on the subject of terminological issues, it is worth pointing out that there is one more term popular among counterterrorism specialists, broader than the "lone wolf", and it has an additional impact on operational and investigative activities. The term was proposed by J.R. White, who writes: "(…) the term Berserker can be used to describe some individual terrorists. The term lone wolf suggests that a person suddenly pops up out of nowhere, performs a sinister act, and vanishes. (…) in reality this does not usually happen. Most lone wolves are true believers who are well-known for their associations with violent extremist circles. Some lone wolves are better viewed as true believing extremists who go off the deep end. The term glorifies their actions and should not be used. This is why I also use the term 'Berserker'. It is more than an academic term and has investigative consequences. In old Norse and British warfare, a berserker was a warrior

[5] D. L. McMahon (ed.), *Into the Chaos*, Crisis Systems Management LLC, Lebanon, MO, USA 2016.

[6] *Ibidem*, p. 245

who went crazy in the midst of battle. (…) (They) are not lone wolves. They are crazed, frightened, true believers. The concept of the berserker may capture some individual extremist violence better than the term lone wolf. This is important for investigators. Berserkers can leave a trail of clues before they 'charge a shield wall'. (…) In practice, many lone wolves do not materialize from thin air. They are berserkers who take violent, irrational actions. When extremists perpetually advocate violence and murder, they may produce a crazed individual who will go on a rampage"[7].

Regardless of our interlocutors' country of origin, there appeared references to perpetrators traditionally labelled as "mass murderers": the practitioners frequently confirmed that from the point of view of institutions responsible for counterterrorism, what really matters is not only the motivation and ideology, but primarily the modus operandi and the direct behaviour of the perpetrator at the very last stages of their action, that is the attack preparation and the attack itself. According to our sources, both categories of offenders (lone actor extremists and mass murderers) are very similar from the perspective of crime prevention and interdiction or detection. As several of the practitioners mentioned, they rarely stay completely "off the radar", but their lack of immediate connection to the established organizations (such as terrorist groups or organized crime) raises the level of difficulty of the detective and investigative operations, typically involving linkage analysis. The majority of police officers suggested what one of the New Zealand Police investigators summarized by saying "both types of actors try to stay in the shadows, but what we should count on is the human nature – they just can't control themselves forever and sooner or later they are going to brag about what they're up to. And the more they keep bragging, the better for us".

LEAKAGE BEHAVIOUR

Such observation fits very well into the "leakage" behaviour pattern described in the PRIME Attack Preparation Subscript[8]. Behaviour of that kind is well aligned with the observations regarding the "telegraphing" conduct of mass murderers, including school shooters, who tend to "broadcast" their hatred and homicidal manifestos ahead of the actual attack[9]. Such behaviour is sometimes a chance for someone from the perpetrator's surroundings to notice it and inform the police. Unfortunately, as was stressed by a Toronto Police investigator: "most people

[7] J. R. White, *Terrorism and Homeland Security*, Thomson-Wadsworth, Belmont, CA 2006, pp. 44–45.

[8] University of Leiden PRIME Deliverable; confidential report.

[9] K. Gradoń, *Zabójstwo wielokrotne. Profilowanie kryminalne*, Warszawa 2010.

just don't care, and what we call 'leakage' and what we would take seriously, they call 'letting steam off' – they think that the verbal aggression might release tension and that nothing serious would happen". The law enforcement professionals frequently comment on such leakage behaviour and it seems to be a widely accepted indicator of the attack preparation. According to the official data of the Police Executive Research Forum, "more than 50 percent of these attackers (active shooters) had broadcasted their intent. Some of them made remarks in person, and others posted statements online"[10]. Several of our interlocutors from the United States, Canada and Australia said during the interviews that the antecedent behaviour of lone actor extremists at the stage of attack preparation involves leakage and other forms of signalling of the attack; they compared it regularly to the conduct of school shooters, who – from the perspective of law enforcement operatives that we interviewed – exhibit very similar behavioural traits. Such observations are officially confirmed by the US governmental reports, which say that "prior to most incidents, other people knew about the attacker's idea and/or plan to attack. (…) In over three-quarters of the incidents, at least one person had information that the attacker was thinking about or planning the school attack. (…) In nearly two-thirds of the incidents, more than one person had information about the attack before it occurred. (…) In nearly all of these cases, the person who knew was a peer: a friend, schoolmate or sibling. (…) Some peers knew exactly what the attacker planned to do; others knew something 'big' or 'bad' was going to happen, and in several cases knew the time and date it was to occur"[11]. The professionals operating in the counterterrorism domain claimed that leakage, telegraphing or broadcasting behaviour should be considered to be one of the major leverages for the law-enforcement if such information is (as a US. Federal agent told us) "reported or intercepted and then acknowledged, recognized as serious and then dealt with accordingly".

Based on the extensive discussions with law-enforcement specialists, we can draw a conclusion that there are multiple indicators of crossing the line between radicalization and attack preparation in lone actor extremist events that are strikingly similar to the well-established theories concerning active shootings (and especially school shootings). Such observations were regularly raised by the Western European (German, Austrian) and North American (US, Canadian) officers, as well as their Australian counterparts. It is then worth listing what are the warning indicators as listed by the US Secret Service in relation to school attacks, which can be translated to lone wolf terrorism scenarios almost in their entirety. Examination of the thinking and behaviours of school shooters suggest

[10] J. Nicoletti, *Preventing the next active shooter incident* in The Police Response to Active Shooter Incidents. PERF, Washington, D.C. 2014.

[11] United States Secret Service & United States Department of Education: "The final report and findings of the Safe School Initiative: implications for the prevention of school attacks in the United States", Washington, D.C. 2004.

that most attacks are preceded by discernible behaviours, as the (perpetrator) plans or prepares for the attack. These behaviours are referred to as "attack-related behaviours" and the list of ones that should raise concern about potential violence includes[12]:

1) ideas or plans about injuring him/herself or attacking a school or persons at school;

2) communications or writings that suggest that the student has an unusual or worrisome interest in school attacks;

3) comments that express or imply the student is considering mounting an attack at school;

4) recent weapon-seeking behaviour, especially if weapon-seeking is linked to ideas about attack or expressions about interest in attack;

5) communications or writings suggesting the student condones or is considering violence to redress a grievance or solve a problem;

6) rehearsals of attacks or ambushes.

In the opinion of our interviewees, similar warning indicators can be attributed to the lone-actor extremists, and (using the above list compiled by the US Secret Service) we can substitute "student" for "lone-wolf" and "school" for "target" (of any kind, depending on the specific objectives and grievances of the particular extremist). The key to success is, as the Spanish intelligence officer said is to "focus on the regular police work, consider every signal from the local community to be serious (and never ignore it) and to focus on the minute details that show that a person's behaviour deviates from the norm or is subject to rapid changes – be it change of daily routine, change in friends and associates group, religious conversion, vocabulary used, etc. It doesn't have to reach the stage of verbal abuse or radical and extremist views explicitly worded out – sometimes it is enough for the persons close to the soon-to-be extremist, especially to the immediate family or next door neighbours to see the slight but consistent changes in the daily routine to send the warning signal. Our usual biggest failure is when somebody tries to reach out and let us know and we ignore it, using excuses in order to avoid extra workload. But we need to remember that if we ignore it and something bad happens, we will be the ones to blame".

While drawing the parallels between lone wolf terrorists and mass murderers, our respondents often stressed the role of "leakage behaviour" as an element with possible fundamental role in preventing and interdicting violent extremism. At the same time, it was emphasized that (as one the employees of a US federal agency put it) just the labelling "is important mostly from the administrative point of view. We need to understand who these perpetrators are, but not for the sake of definitions, but rather to adjust our methods to specific types of threats that

[12] United States Secret Service & United States Department of Education: "Threat assessment in schools: a guide to managing threatening situations and to creating safe school climates", Washington, D.C. 2004.

we are dealing with". Representatives of eighteen police forces from the United States (on federal, state and local levels), who took part in training and dissemination activities hosted by the Portland Police in February 2017, where PRIME outcomes were extensively covered and presented to over two hundred participants, agreed during in-depth discussions, that very often labelling is a purely political issue that may change depending on the particular geo-political situation, while for the law-enforcement it is much more important to focus on tackling the problem regardless of the terminology being used. The need to understand the differences between various types of extremists appears in the words of most of our interlocutors, who also stress that it has to serve very practical purposes, the most important of which being calibrating the particular methods of intelligence, operational and investigative work.

A NEED FOR THE DATABASE

Another practical element that our interlocutors claimed should be addressed by the countermeasures strategies on both national and international levels is the creation of uniform databases enabling law enforcement and security services to share data and information in a flawless and direct manner. The problem does not only concern the exchange of information between countries as remote as India and Australia or Japan and Canada, but also within the EU, where – as practitioners noticed – the flow of data is limited, incomplete and ineffective. This is due to reasons as simple as incompatible software and inadequate quality or level of security in transmission networks, but what is much more serious is the lack of trust between some departments or the unwillingness to share information considered „sensitive". Such situations were cited by persons from Polish and German, Italian, Hungarian, Spanish and Portuguese intelligence services. What was regularly mentioned was that the problem is not only the "third party rule" that functions in special services' circles (which means that if one (foreign) intelligence service passes information to a different country's intelligence agency, it often restricts that information from being passed on to other national services justifying such an approach by the possible risk of „data leakage"; it obviously hinders an effective solution to the problem in situations where the cooperation of other institutions is required).

It was also said that the flow of information is often complicated between services within one country (e.g. between border services and the police), and between similar institutions in two friendly countries (e.g. between two police agencies). A Canadian provincial police officer cited an example of exchanging information with the police forces of other Provinces of Canada, where the lack of mutual trust (or treating partners from another part of the country as competitors)

caused limiting the transmitted data to the most essential elements. Furthermore, the information was being transferred by the federal police (in this case the Royal Canadian Mounted Police), although there was no legal obligation to do so, and such action greatly lengthened the procedure. If such problems occur within a single country, cross-border cooperation is even more complex. Add to that the problems with the lack of uniform police terminology, differences in cultural contexts, working styles, methods of action, and things as mundane as transmission errors resulting from linguistic differences.

Consolidating databases and developing consistent naming was one of the most common demands made by practitioners with whom we conducted our consultations. One example of this may be the advanced attempt to unify the working methods and systems used (as well as the terminological issues) in crime analysis circles. Our interlocutors from many countries, often as different as India, Spain and Canada mentioned the example of IALEIA – International Association of Law Enforcement Intelligence Analysts – whose mission is to advance high standards of professionalism in law enforcement intelligence analysis at the local, state/provincial, national, and international levels. IALEIA's aim is to enhance understanding of the role of intelligence analysis, encourage the recognition of intelligence analysis as a professional endeavour, develop international qualification and competency standards, reinforce professional concepts, devise training standards and curricula, furnish advisory and related services on intelligence analysis matters, conduct analytic-related research studies, and provide the ability to disseminate information regarding analytical techniques and methods[13]. Police officers from Australia and New Zealand mentioned the example of good practices of a similar organization from their area of the World: the Australian Institute of Professional Intelligence Officers (AIPIO). The opinions collected during this stage of PRIME research show that organizations like IALEIA or AIPIO should become a model for intelligence and police agencies dealing with the issue of radicalisation, extremism and terrorism, both on the organized, group-based level and the disorganized, lone actor level. It applies to the broadest spectrum of services involved, including – but not limited to – police forces, border protection units, and financial control institutions.

FOLLOW THE MONEY

Financial analysis is another topic, originally raised during our preliminary discussions held at EUROPOL, when we established the contextual framework of the problems associated with the effective counteraction of violent extrem-

[13] IALEIA Mission Statement. See: http://www.ialeia.org.

ist events. As mentioned by the EUROPOL analyst, the officers should seek to establish a relationship of the extremists with a broader structure, and they might also need to „follow the money", i.e. they should examine the financial flows and connections which could lead them to get to know the ordering parties, sponsors, other members of the group, to recognize the group network and structure or to associate a specific person with other people (including those acting alone). The same problem was acknowledged by our interlocutors at the most recent stages of our research. According to our sources in the United States, Europe and Japan, the principle of "following the money" is significantly underestimated in regards to the perpetrators acting alone. Even if the perpetrators indeed act alone, it is likely that at some stage they might receive financial assistance from the outside world – either terrorist organizations, individual "sponsors" who support the political agenda of the extremist group, or by unrelated network of sympathizers who might provide financial assistance to radicalized individuals.

Obviously the above observations relate most frequently to group-based form of terrorism, but – as stated by some of our interviewees – the possibility of such an aid directed to lone actors cannot be excluded, especially if they tend to seek data, know-how and support on-line, when outsiders – unbeknownst to them on a personal level – might not only encourage them to radical behaviour, but also sponsor them, sending money through wire transfers, or – more likely with the development of technology – by using payment methods that are more difficult to trace, such as on-line transfers, especially involving crypto-currency. Our interlocutors representing German and Spanish Police, as well as the Australian investigators used Bitcoin example specifically, indicating that such transfer are most difficult to trace, especially when involved parties have some counter-surveillance knowledge or experience. The general theme of financing of terrorism was prevalent in our conversations, especially with more senior-level officers. They would usually focus on the group-based terrorism, and the role of organized crime and "drug money" in terrorism sponsorship (as well as "state-sponsored" terrorism), but they also confirmed that lone actors could benefit from such funding to some extent. Senior officer from one of the Japanese services mentioned the areas previously unexplored in the lone-actor terrorism research, indicating the maritime piracy in Southeast Asia as an example of organized criminal enterprise, whose objectives include raising money for group-based terrorism and indirect funding of what he called "extremism nurseries" in Asia (he referred to Indonesia, Malaysia, Cambodia and the Philippines)[14]. The same problem was raised by the American and Italian experts in border protection (military and police institutions), who suggested that maritime piracy at the Horn of Africa might be linked to terrorism sponsorship in Africa, Europe and beyond. Our interviewees

[14] Confirmed officially by e.g. A. Ibrahim Almuttaqi, Head of ASEAN Studies Program, The Habibie Center: "The 'Islamic State' and the rise of violent extremism in Southeast Asia", https://thcasean.org.

stressed that the financial analysis techniques shall be used to retroactively study the cash flow and money transfers in the cases of known lone-actor extremists, in order to search for patterns that could be later applied to investigate radicalized individuals.

COMMUNITY POLICING

Another set of problems that were addressed by our interlocutors were the extreme difficulties in infiltrating, or even in establishing links and co-operation with the communities that lone-actor arise from. Interviews held for the present report show that in the case of countries with complex national and ethnic structure, this may be one of the most serious obstacles for preventing and fighting radicalization, extremism and "lone wolf" terrorism. One of the more important sources of information were interviews held in Spain, Portugal and the United States with criminal intelligence operatives whose duties include official and/or unofficial work with the ethnic minorities, and also with persons who, due to their professional duties, function in those environments (journalists, NGO workers). Police officers that we talked to emphasized that the use of paid agents, secret informers, and other "unofficial" associates is a solution that their services regularly use, but they are usually not the most effective methods. Furthermore, they are costly, dangerous and do not always result in obtaining valuable information. The best results may be obtained by cooperating directly and (usually) overtly with given communities, usually while performing the tasks included in community policing. The biggest problem is to breach the distrust of those communities, and the internal fear of persons who could become valuable sources of information that they could be considered traitors or police "snitches".

Criminal intelligence officer representing one of the major Police forces in the large US city told us during the interview that the key to success is a patient, often long-term cooperation with communities, frequently consisting of, e.g. providing them safety from organized crime or gangs. Another method of gaining trust is holding regular meetings, lectures, and workshops on crime prevention, implementation of good security practices, and others (examples of neighbourhood watch, coping with teen bullying, avoiding bullying, showing the opportunities for channelling emotions and aggression in sports competitions, etc.). According to our interlocutor, such "soft methods", whose beneficiaries are the whole communities, but whose active participants are mostly women and the elderly, are a successful platform for building an understanding. Their effectiveness lies in the fact that they are successful in providing these communities with valuable and positive patterns that translate into a general increase in the level and quality of life, but at the same time they allow them to gain confidence.

This aligns very well with our previous observations, when we indicated an observation of an American Police officer operating in the Somali community who was able to receive the most precious information as a result of informal relations that this person established with that community. As our interlocutor explained: "the most effective method of work and acquiring information is to enter the community while helping that community (social work, assistance actions, e.g. in the case of domestic violence; trust is built and information is acquired in exchange for help, often even from very homogeneous and hermetic ethnic groups). And such information is often most essential".

Trust is the foundation for relationships where people in a given community are not afraid to talk to their friendly police officer and tell them about distressing or otherwise "sensitive" observations that can have tremendous operational, preventive, and detection value for an experienced investigative officer. In the opinion of our interlocutor, building such relationships sometimes lasts for many years, so it cannot be treated as a short-term way to achieve one's goals quickly. The same speaker noted that, unfortunately, most police institutions do not have particular patience and expect fast and „usable" effects as quickly as possible. Long-term commitment is absolutely crucial to establish quality links and any shortcuts my render an intelligence strategy useless. As the operational analyst told us, the intelligence officers should be tasked with his or her duties in a specific environment for years and should remain in that position for as long as possible, gradually introducing colleagues to the community in question. The Spanish intelligence officer we interviewed compared that approach to the work of the handler who works with secret informants, saying that "quite frequently, the handlers cannot be replaced, as any change of the contact personnel might scare off the informant who (working under extreme stress and huge danger of exposure) might suspect that he or she is being framed. Any inevitable changes of handlers must be gradual and the new officer needs to meet the same criteria for co-operation as his predecessor". Community policing is of course different to the management of the secret informants, but the general rules still apply if such work has side effects such as access to information and intelligence that would be very difficult to obtain otherwise.

The American officer said that in their jurisdiction they deal with communities that are particularly difficult to infiltrate using the "traditional" covert methods – persons from Chechnya and Afghanistan. Getting through to them is very complicated and sometimes the strategies used involve establishing the first contact with them as soon as possible after their arrival to the United States, by offering them information on the American judicial system, presenting crime prevention tips, informing on methods of seeking help and advice. Such first contacts serve as foundation for future co-operation and if the officer in charge is consistent in their approach, they might gather high quality and reliable intelligence, which can then be used either for further strategies (such as de-radicalization, attack interdiction) or as a data set for strategic analysis.

SAFE2TELL PROGRAM[15]

One of the interesting preventive programs that we assessed and that fits in the general scope of community policing is the Colorado Safe2Tell program. It deals mostly with school violence, but it can be replicated and re-adjusted to cover the problems of lone actor extremism. The Safe2Tell Initiative was created as a direct outcome of the Columbine Commission's Report[16] to implement a critical recommendation: "to provide an anonymous venue for parents, students, teachers, school administrators, and law enforcement to share information".

Safe2Tell was founded on the idea that prevention and early intervention is the key to preventing violence and saving lives. The guiding principles of this safety and prevention initiative model include educating young people and school staff on critical issues, encouraging them to play a role in prevention, equipping them with a tangible direct way to report anonymously, while empowering them to make a difference.

Bringing a proactive plan of reporting to focus, the Safe2Tell Colorado model allows for early interventions to take place in regards to behaviours identified as precipitators to violence and for those behaviours that endanger the health and well-being of youth. The strategy framework established by the model provides a sophisticated and efficient method for sharing information to local responders and schools.

Research shows that in 81% of violent incidents in U.S. schools, someone other than the attacker knew it was going to happen but failed to report it[17]. Typically, the information goes unreported because of fear of being a "snitch" or that the attacker will then target the informant, thereby creating a "code of silence".

To penetrate this code of silence, Safe2Tell Colorado initially was founded as a non-profit organization, incorporated to develop a state-wide anonymous reporting tool available 24-hours a day to accept reports whenever a Colorado youth or concerned adult perceived a threat to their safety or the safety of others.

Anonymity is the key to the success of the Safe2Tell Colorado model. Both state law and the procedures established by Safe2Tell Colorado guarantees the anonymity of every reporter. Calls were answered at a Colorado State Patrol communication centre; later web and mobile app reports were added. When action is needed, information immediately is forwarded to local school officials and law enforcement agencies, as appropriate. Safe2Tell Colorado developed a component

[15] Based on materials of the University of Colorado Boulder – Center for the Study and Prevention of Violence, Colorado Office of the Attorney General, The Colorado Trust and Safe2Tell Program on-line.

[16] https://www.safe2tell.org/sites/default/files/u18/Columbine_20Report_WEB.pdf

[17] US Secret Service and US Department of Education, The Final Report and Findings of the Safe School Initiative and Implications of School Attacks in the United States. May 2002, p. 34.

of accountability ensuring that each report was investigated by school and law enforcement agencies, that action was taken, and that the outcome was tracked. The assurance that calls were not traced and that appropriate action was taken established the trust needed to persuade young people to move away from a code of silence and to take a stand. Safe2Tell Colorado has worked to create positive peer pressure and empower young people to keep their community safe.

The key components of the Safe2Tell Program are as follows:

1) Colorado State law guarantees the anonymity of every caller;

2) Anonymity is guaranteed by law; there is no caller id and callers' names are not asked;

3) Safe2Tell Colorado is available to all Colorado schools, students, teachers, and parents;

4) Reports can be made to Safe2Tell Colorado by calling a designated toll-free hotline;

5) Reports can be submitted through the Safe2Tell Colorado's website by clicking "submit a tip" button;

6) Tips may be submitted using a smartphone through the Safe2Tell Colorado mobile app;

7) Calls to Safe2Tell Colorado are answered 24 hours a day, seven days a week by trained Colorado State Patrol Dispatchers;

8) A trained communications officer collects information for the report and assigns a tip number to the reporting party;

9) Every tip submitted to Safe2Tell Colorado is thoroughly investigated once given to the appropriate school and/or law enforcement agency;

10) Safe2Tell Colorado serves as a conduit for the information received, sending it directly to the school and/or law enforcement for local investigation and/or intervention;

11) Safe2Tell Colorado uses a unique and highly sophisticated database program that allows for two-way dialogue between the reporting party and the answering point;

12) All information is encrypted, allowing for complete anonymity;

13) Web reporting and mobile app options allow reporting parties to upload photos and social media posts, which aid law enforcement in conducting thorough investigations;

14) The sophistication of the Safe2Tell Colorado database system is ever-evolving and helps identify trends of violence in schools and communities.

According to our conversations with U.S. Police officers familiar with the Safe2Tell Program – both from Colorado and from other jurisdictions of the United States, the program that originated in the general system of Blueprints for Violence Prevention projects (led by the Center for the Study and Prevention of Violence based at the University of Colorado at Boulder) is not only successful and useful in school-focused crime prevention, but can also be used as a set of

best practices calibrated to counter other types of threats, such as the lone wolf terrorism. Similar strategies can be applied in order to create a secure and anonymous communication platform, which members of the communities that are considered to be the "nurseries" for lone-actor extremists could use to report dangerous behaviour and to provide tips on radicalization and attack preparation. We consulted such opportunities not only with the American Police officers, but also with their European counterparts and although the program was not known in Europe, Polish, Italian, German and Spanish Police officers to whom we presented the Safe2Tell idea considered it to be a very promising crime prevention tool.

OPEN SOURCE INTELLIGENCE

Another confirmation of our earlier findings that needs to be seriously taken into account and should be employed as one of the major elements of the countermeasures framework is the fact that the Open Source Intelligence (OSINT) approach is getting priority as a tool in disposal of the law-enforcement and security services.

During the interviews and consultations that we performed, we received feedback from the practitioners who employ these techniques in their work in the domain of counterterrorism and risk assessment. According to officers representing three different Polish institutions of the central level (police and two special services agencies), the use of information from open sources begins to play an ever-greater role in the analysis of trends in crime and analysis of threats, including terrorism. According to our interlocutors representing the police services of all the countries in which we conducted the study, the vast majority of the information used by intelligence agencies comes from the open network, and in particular from discussion forums and social media. Most of the searches used for threat profiling are based on keyword combinations, contact analysis, or operationally and implicitly obtained registries of queries and visits to websites identified as sources of radicalisation, know-how resources, and instructions for preparing an attack.

A linguistic analysis of speech that can be considered as verbalizing intent of an attack is also used – the latter element is not automated or computer-assisted, although there are advanced technological solutions available in the market (tools for semantic natural language analysis). Not all countries possess the right technological possibilities to conduct such actions in an integrated and holistic manner. Often their activity is profiled to particular discussion forums and groups in popular social media. One of our interlocutors, an officer from Southern Europe, stated directly that his institution did not have the ability to use Big Data categories, so his subordinates must, based on specific guidelines, search the previously

selected discussion forums for content that could direct further operational activities. Some countries have the financial and organizational possibilities to employ specialist data mining software, but at present it is not yet a common practice. As our interlocutors stated, at this stage it is difficult to talk about a comprehensive search of the Internet for the purpose of identifying and locating threats from the lone actor extremism category, but everyone considered this approach to be an absolute necessity, realizing that, together with generational changes, interpersonal interactions move from the real world to the virtual realm.

CONCLUSIONS, RECOMMENDATIONS AND FUTURE STEPS[18]

Based on the extensive consultations with law-enforcement and security services practitioners and Subject Matter Experts of the PRIME Project domain, representing a wide range of areas (police, intelligence, border protection, military, government, civil defence, non-governmental organizations, and the academic community) and different jurisdictions and law practices (several countries of Europe, United States, Canada, India, Japan, Georgia, Mexico, Australia and New Zealand), we designed a portfolio of Recommendations that – in our (University of Warsaw PRIME team) opinion – shall be considered in order to prevent, interdict and mitigate the threat of lone actor extremism and terrorism and to support public security and safety.

The Recommendations are not all-inclusive and their implementation would be a long-term process, requiring the international collaboration of the widest possible range of institutions on national and international level. We present them for consideration of all interested parties, assuming that the introduction of at least a selection of the proposed measures would significantly improve the system of countermeasures that are available today.

We found it necessary to establish an international working group of practitioners and experts in counterterrorism, representing the widest possible range of disciplines (preventive, operational, intelligence, tactical) and countries. We are aware of the fact that such networks exist, but according to the specialists we thoroughly consulted, most of these entities are purely bureaucratic and limited to administrative duties. The practical aspects of cooperation are impacted by either the direct distrust or confidentiality clauses forbidding the participants of such networks from sharing information with their peers from other countries, or even

[18] The Recommendations provided in this Paper represent only the views of the University of Warsaw PRIME team and in no way they can be interpreted as the official recommendations or statements of either the European Commission or other members of the PRIME Project Consortium.

with their colleagues representing different institutions from their own country. It was explicitly confirmed by the practitioners that we interviewed, who, on several occasions, mentioned that they are required to keep the operational know--how secret, even though they are certain that such knowledge – if widely used – would prove practical and effective; they are however bound by their institutional policies and cannot share the best practices with other agencies.

The bureaucratic nature of existing international structures could be replaced or at least supplemented by the designated forum of experts with necessary security clearance, who would be allowed to share and discuss the operational know-how with their peers representing international law-enforcement community. It is crucial not to limit such forum to one region (e.g. European Union or North America), but to include the representatives of the broadest spectrum of institutions from around the world. It is necessitated by the vast differences between problems with which particular countries deal and which might not yet be experienced in other parts of the world. As our interviewees regularly stressed, the phenomena associated with globalization are not only positive, so we can expect that the terrorist strategies practised in a completely different region might become quickly adapted by the violent extremists elsewhere. It is necessary to set up such a platform that would take into account the specifics of various problems and experiences – including all input from the wide range of cultures, customs, traditions and regions.

The practically oriented, international working group on counter-terrorism and counter-extremism should be designed in such way, that the participants would have a carte blanche to share information and influence the restructuration of security practices. One of the steps we propose is to make sure that such forum consists only of experts with practical and operational merit in countering terrorism and extremism. One of the significant failures of the contemporary platforms of that kind is the over-representation of the most senior delegates who have held the managerial and administrative positions for a long time and have no immediate and most recent experience with counter-terrorism practice; their sheer presence "paralyses" (in the opinion of substantial proportion of our interlocutors) the work of all such groups as they are usually detached from the operational dimension of law-enforcement work.

The first step that should be taken in order to create such a working group would be to organize an international conference that would focus on the problems identified by us (namely: obstacles and barriers to the pursuit and effective implementation of strategies, methods and practices utilized in countering violent extremism). We propose that such conference is organized with a specific theme and objective – that is not only to present the problems, but mainly to put forth the proposition of creating the practical working group and to receive the conclusive decisions enabling the creation of such structure. The conference shall gather the representatives of international law-enforcement and security community, both

on the administrative and operational level, but the explicit and perspicuous goal should be to form a platform that would consist only of practitioners with immediate, direct and personal experience in counter-terrorism and counter-extremism. The participants of the conference should include representatives of law-enforcement administration and management, as well as governmental, non-governmental and academic experts, but their role should be limited to discussion on the framework of the entity described above, and – possibly – to formation of an advisory board that would provide the practitioners with all the necessary assistance needed.

We consulted the above scenario with security experts from numerous countries and disciplines of law enforcement. They believe that even though it might sound as a "wishful thinking", considering the inertia of the bureaucratic structures that they are managed by, it is still the only plausible option. If such structure is not created, then we are losing the reasonable opportunity to create a practical and (potentially) highly effective measure that could possibly have direct impact on general security and safety. Our respondents frequently remarked on the indolence and apathy of existing structures and they blamed the incompetent administrative circles and political environment for rendering their work useless. We believe that the strategy described earlier is possible to achieve, as we learned from the experience of services who were responsible for safeguarding two events considered to be the most difficult, most demanding and having the highest risk level ever experienced by the law enforcement, civil defence and intelligence services in Poland – that is the NATO Summit and the World Youth Days – both organized in Poland in 2016. Securing these two events was the most significant security operation in the country and its success is undoubtedly due to the fact that practitioners and experts representing the widest range of disciplines were allowed to cover the strategic and operational dimension of the task in a fashion similar to the one described above. Of course, it was an operation limited to one country, and our recommendation is to employ the similar approach on an international level, but – as our respondents remarked – such "best practices" prove that the effectiveness of countering terrorism and violent extremism is reliant on the introduction of the practitioners-only forum operating on the widest possible international scale.

Another recommendation closely linked to the ones above is to prepare a unified system of terminology related to prevention, interdiction and mitigation of violent extremism and terrorism. As it was described earlier, the law-enforcement community considers the practices of IALEIA – International Association of Law Enforcement Intelligence Analysts – whose mission is to advance high standards of professionalism in law enforcement intelligence analysis at the local, state/provincial, national, and international levels. IALEIA's aim is to enhance the understanding of the role of intelligence analysis, encourage the recognition of intelligence analysis as a professional endeavour, develop interna-

tional qualification and competency standards, reinforce professional concepts, devise training standards and curricula, furnish advisory and related services on intelligence analysis matters, conduct analytic-related research studies, and provide the possibility to disseminate information regarding analytical techniques and methods.

According to the law-enforcement and counter-terrorism experts that we interviewed, IALEIA systems should become a blueprint for other domains of law enforcement, because the existing incompatibilities of terminology and operational practices seriously affect the exchange of information and limit the potential of joint operations. Crime analysts "speak the same language", as the systems designed as tools for analytical purposes (operational, strategic, financial) operate in the same way, using the same set of commands, identical icons, etc., so even if the services exchanging information use different languages and come from different cultures, the analytical flow is not affected by what might be otherwise "lost in translation". The same applies to the proposition of establishing the joint counter-extremism and counter-terrorism databases.

From the purely technical point of view, it is one of the easiest tasks that could be accomplished fairly quickly. The problem that should be addressed is the incompatibility of laws governing present-day (incompatible) databases and data protection – it would require bi-lateral legal agreements, but the only method to achieve such an objective is to do so on the widest international scale possible. We investigated several software platforms enabling the technical solution of the problem (some of them are very advanced and tested to meet the requirements of law-enforcement and intelligence services, beyond proof of concept – allowing their utilization both as an analytical tool with highly sophisticated data mining capabilities that include the semantic analysis of numerous natural languages, as well as the secure database), but the legal side of the enterprise needs to be met before such solutions are implemented and used. It will definitely be the most time-consuming task, so it must be safeguarded as soon as it is possible, in order to give the law-enforcement services the opportunity to use tools that are already available, on the scale exceeding local (national) level.

An important additional element of such information exchange is the exchange of financial information, considered by the majority of the consulted experts to be the crucial part of the counter-terrorism toolbox. According to our sources in the United States, Europe and Japan, the principle of "following the money" is significantly underestimated in regards to the perpetrators acting alone. Even if the perpetrators indeed act alone, it is likely that at some stage they might receive financial assistance from the outside world – either terrorist organizations, individual "sponsors" who support the political agenda of the extremist group, or by unrelated network of sympathisers who might provide financial assistance to radicalized individuals. Our interviewees stressed that the financial analysis techniques should be used to retroactively study the cash flow and money trans-

fers (including crypto-currency such as Bitcoin) in the cases of known lone-actor extremists, in order to search for patterns that could be later applied to investigate radicalized individuals.

Another element closely linked to the above recommendations is the potential of the utilization of Open Source Intelligence (including Social Media Intelligence) tools to study leakage behaviour of real and potential extremists. Such approach may indeed suffer from "Big Data problem" (resulting in a substantial proportion of false-positive observations), but it can be addressed with an aid of the aforementioned intelligence-assisting data mining tools, which are already on the market and can be calibrated to the specific needs of particular law-enforcement agencies and intelligence services.

As it was described earlier, another important issue that should be taken very seriously if the results of PRIME Projects were to be implemented is the role of community engagement. The vast majority of field officers that we interviewed claimed that the information from communities have the highest intelligence value. Obtaining such information is a difficult process, as building trust and establishing contacts with communities that are considered to be "nurseries" for extremists is highly problematic and challenging. According to our sources, long-term commitment is absolutely crucial to establish quality links and any shortcuts may render an intelligence strategy useless. The operational intelligence officers (police professionals) should be tasked with their duties in a specific environment for years and should remain in that position for as long as possible, gradually introducing colleagues to the community in question. Such approach was compared to the work of the handler who works with secret informants. Quite frequently, the handlers cannot be replaced, as any change of the contact personnel might scare off the informant who (working under extreme stress and huge danger of exposure) might suspect that he or she is being framed. Any inevitable changes of handlers must be gradual and the new officer needs to meet the same criteria for co-operation as their predecessor. Community policing is of course different to the management of secret informants, but the general rules still apply if such work has side effects such as access to information and intelligence that would be very difficult to obtain otherwise.

Our recommendation in this domain is to provide front line police officers with substantial amount of education and training related to the work and co-operation with affected communities in cases when community engagement is a mutually beneficial strategy. It needs to be a part of the basic police training, as – according to our interviewees – community work of the police officers is linked to acquiring information by entering the community while helping that community (social work, assistance actions, e.g. in the case of domestic violence; trust is built and information is acquired in exchange for help, often even from very homogeneous and hermetic ethnic groups), and such information is often most essential.

We described in detail a programme that could also be used as a blueprint for community engagement on a different level. Such strategy was presented using the example of the Safe2Tell Programme, founded in the State of Colorado on the idea that prevention and early intervention is the key to preventing violence and saving lives. The guiding principles of this safety and prevention initiative model include educating young people and school staff on critical issues, encouraging them to play a role in prevention, equipping them with a tangible, direct way to report anonymously, while empowering them to make a difference. Bringing a proactive plan of reporting to focus, the Safe2Tell Colorado model allows for early interventions to take place in regards to behaviours identified as precipitators to violence and for those behaviours that endanger the health and well-being of the youth. The strategy framework established by the model provides a sophisticated and efficient method for sharing information with local responders and schools. Safe2Tell Programme ideas, although originally designed to tackle school violence, can also be used as a set of best practices calibrated to counter other types of threats, such as lone wolf terrorism. Similar strategies can be applied in order to create a secure and anonymous communication platform, which members of the communities that are considered to be the "nurseries" for lone-actor extremists could use to report dangerous behaviour and to provide tips on radicalization and attack preparation.

It is critically important to raise awareness and educate law-enforcement and (especially) general public on the slightest warning signals that may indicate radicalization. Under no circumstance shall they be ignored, but they should rather be immediately and thoroughly verified. The persons who have regular contact with society, due to the nature of their work, such as teachers, medical professionals, social workers or even postal workers (mail delivery personnel was specifically indicated by our American respondents) should be trained and educated in regards to the identification and reporting of such warning signals. Our recommendation is to prepare an information campaign directed to the society in general and to the specific professional groups in particular, communicating the methods of understanding, identifying and "flagging" of the pre-selected warning signals, calibrated to particular local situation, including the socio-economic and cultural makeup of a specific area or community.

Calibration of counter-measures to the specific threats that may be relevant to a particular community is absolutely crucial in order to properly allocate law-enforcement resources. It might seem obvious that different methods and techniques should be used in regards to different types of extremism, but according to the results of our interviews, in several jurisdictions it is far from the truth. Instead of focusing on the particular threat (such as Jihadi terrorism, extreme right-wing terrorism or left-wing extremism), some agencies try to employ "general" approaches, furthering the problem by what they understand as "holistic" approach (that is: without taking into account the local context). In our opinion,

based on the outcomes of our studies in the law-enforcement community, there is a widespread opinion of front-line professionals that the strategy should definitely be context-specific and locally-oriented. Counter-terrorism and counter-extremism must be general at the level of national or international guidelines and recommendations, but at the operational level it should not differ from the approach employed for combating violent gangs, drug trafficking and other forms of serious crime. The problem with countering terrorism is that it became a political issue and the global strategies suffer from being "over-politicized" and being used as leverage in political power plays. In the opinion of law-enforcement operatives, one of the recommendations that shall be publicized in effect of PRIME Project is enabling the police and intelligence officers to approach incidents of violent extremism in a similar fashion that they would apply to crime (including its most extreme forms, such as multiple homicide, active shooters and school shootings), without the burden of political interference and unnecessary media hype, which more often than not increases the pressure and leads to further escalation of violence.

As several of our interlocutors noted, we need to be aware of the new and emerging threats that were not considered to be very significant in the Western world until recently. These threats include specifically the application of the unique modus operandi that was frequently used by the terrorists in the Middle East (especially in Israel); that is the so-called run-over attacks. As the recent tragedies in Niece, Berlin and London indicate, tactics as easy as the theft of a motor vehicle and turning it into a weapon must become a priority for practitioners designing the counter-measures and helping to prevent, interdict and mitigate terrorist events. Obviously, it is not possible to limit access to vehicles, so the only plausible solution is to design measures that would either displace the attacks or limit their potential consequences. One of the approaches is the strategy used in Israel, where the permanent heavy-duty barriers protect bus stops and street corners (the usual target of run over attacks) – as described in the PRIME Lone-Actor attack sub-script. The other method advocated by the Indian law-enforcement are mobile steel and concrete barriers, which are strategically located in the cities and can be easily moved around and positioned in case of emergency. We saw the use of such structures in Hyderabad (India) and their simplicity and ease of use (together with their stopping-power) would make them very useful for the prevention of run-over attacks. According to our interlocutors, such structures should be strategically located in the cities, so that they could be quickly deployed, especially around high profile targets (as in the case of the July 14th 2016 Nice attack at the Promenade des Anglais).

Another emerging threat that needs to be taken into account, as noted by the practitioners that we interviewed and consulted, is the use of arson as weapon. Some of the experts explicitly refer to this trend as "pyro-terrorism". The 2016 wildfires in the United States, Australia, Europe (especially in Spain and Portu-

gal) and Israel are considered by our interlocutors to be deliberate actions of the terrorist organizations and radicalized individuals. As the cost of preparation of such an attack is very low and the area to be controlled for the purpose of prevention is extremely large, it is likely that such strategy might be employed on a larger scale in the near future, especially as it is openly advocated by terrorist organizations (e.g. Al-Qaida in the Arabian Peninsula "Inspire" Magazine No. 9 (2012), encouraging the use of wildfires as a form of Jihad). These are just the examples of the potential threats that need to be taken into account by the law-enforcement and security services.

We suggest that counter-extremism and counter-terrorism experts focus on the predictive and forecasting analysis of the potential changes of the terrorist modus operandi, as the cost-effectiveness of the newly-applied methods makes them especially appealing to the radicalized individuals who lack the financial and logistic support of larger, organized structures. The know-how sharing potential of the Internet and the social media means that it is very likely for the new methods of attacks to be quickly adapted by the potential followers and perpetrators of copycat attacks worldwide.

Finally, our recommendation is to note that the key to success in countering terrorism and violent extremism is, most often, regular police work. We realize that it might come as a basic and obvious observation, but our study shows that this is a significantly overlooked and underestimated part of the "general" counter-terrorism strategy. Obviously, the criminal analysis and intelligence are both needed to understand and assess the threat, but in the end it is a job of "regular" patrol officers to notice behaviours and actions that are out of ordinary. It is their duty to notice the unusual, and proceed accordingly. The biggest problem is when the police officers are desensitized by their routine and indifferent to the problems experienced in the local community; this is when they begin to ignore subtle signals and messages, and sometimes – very direct threats. It is exactly what had happened in numerous instances of active-shooter scenarios, when the perpetrators were openly "telegraphing" their threats, sometimes giving the exact time and location of the attack. As several of our interlocutors mentioned, the services theoretically responsible for containing such threat were always looking for "reasonable" explanations, usually using the justifications or rationalizations of the otherwise alarming behaviour. No matter how cliché it might sound, the need of raising awareness, educating the police personnel and implementing the thorough training focused on threat detection and containment, as well as making sure that the local patrol officers understand the value of co-operation, establishing and maintaining links with the local communities is one of the most important factors in addressing the threat of violent extremism and terrorism.

COUNTERING LONE-ACTOR TERRORISM: SPECIFICATION OF REQUIREMENTS FOR POTENTIAL INTERVENTIONS

Summary

The author 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 partial results of the research devoted to the preparation of portfolio of lone actor extremism counter-measures requirements based on the findings of the review of existing counter-measures used to defend against lone actor extremist events. The Article concludes with a list of recommendations, which shall be considered in order to prevent, interdict and mitigate the threat of lone actor extremism and terrorism and to support public security and safety. These recommendations are based on the extensive consultations with law-enforcement and security services practitioners and Subject Matter Experts of the PRIME Project domain, representing a wide range of areas (police, intelligence, border protection, military, government, civil defence, non-governmental organizations, and the academic community) and different jurisdictions and law practices (several countries of Europe, United States, Canada, India, Japan, Georgia, Mexico, Australia and New Zealand).

BIBLIOGRAFIA

Almuttaqi A. I., *The „Islamic State" and the rise of violent extremism in Southeast Asia. ASEAN Studies Program*, The Habibie Center, https://thcasean.org/read/articles/171/The-Islamic-State-and-the-rise-of-violent-extremism-in-Southeast-Asia (visited: 12.12.2017)

Gradoń K., *Zabójstwo wielokrotne. Profilowanie kryminalne*, Warszawa 2010

Jenkins B. M., *Stray Dogs and Virtual Armies. Radicalisation and Recruitment to Jihadist Terrorism in the United States Since 9/11*, RAND Corporation 2011

McMahon D. L. (ed.), *Into the Chaos*, Crisis Systems Management LLC, Lebanon, MO, USA 2016

Nicoletti J., *Preventing the next active shooter incident* in The Police Response to Active Shooter Incidents. *PERF*, Washington, D.C. 2014

United States Secret Service & United States Department of Education: „The final report and findings of the Safe School Initiative: implications for the prevention of school attacks in the United States", Washington, D.C. 2004

United States Secret Service & United States Department of Education: „Threat assessment in schools: a guide to managing threatening situations and to creating safe school climates", Washington, D.C. 2004

White J. R., *Terrorism and Homeland Security*, Thomson-Wadsworth, Belmont, CA 2006

KEYWORDS

extremism, radicalization, terrorism, lone actors, lone wolf terrorism, PRIME, counter-terrorism, Police, Intelligence, special services

SŁOWA KLUCZOWE

ekstremizm, radykalizacja, terroryzm, samotni sprawcy, terroryzm samotnych wilków, PRIME, zwalczanie terroryzmu, policja, wywiad, służby specjalne