TACTIC

TOOLS, METHODS AND TRAINING FOR COMMUNITIES AND SOCIETY TO BETTER PREPARE FOR A CRISIS

Short report on Workshop 2, Case study Terrorism in Europe

Susan Anson, Hayley Watson, Kush Wadhwa

Trilateral Research Ltd

Document information

Title	SHORT REPORT ON WORKSHOP 2, CASE STUDY TERRORISM IN EUROPE
Lead Authors	Susan Anson, Hayley Watson, Kush Wadhwa (Trilateral Research Ltd)
Contributors	
Distribution	Public
Document Reference	D4.2

Document history

Date	Revision	Prepared by	Organisation	Approved by	Notes
21.12.2015	Version 1	Su Anson Hayley Watson Kush Wadhwa	TRI		
22.12.2015	Version 1.1	Hayley Watson	TRI		
22.12.2015	Version 1.2	Su Anson	TRI		

Acknowledgements

The work described in this publication was supported by the European Union (European Commission, FP7, grant agreement no.:608058).

The authors would like to acknowledge the support provided by Cheney Shreve (Northumbria University), Alkiviadis Giannakoulias (European Dynamics), Nuray Karanci (Middle East Technical University) and Anna Donovan (Trilateral Research) in hosting the second workshop on terrorism in Europe.

Preamble

The overall aim of the TACTIC project is to increase preparedness to large-scale and cross-border disasters amongst communities and societies in Europe. This will be achieved through drawing on state-of-the-art literature related to risk perception and preparedness as well as creating a catalogue of good practices in education and communication. This information will be drawn together in the form of a community preparedness audit. The audit will access the risk perception, preparedness and existing capacities of a given community and use this information to point communities towards good practices in communication and education which best reflect their needs. All these findings and outputs will be presented in an online learning platform which aims to ensure the sustainability of the use of the projects outcomes after the project has come to an end.

Rather than taking a top-down approach to preparedness, TACTIC will pursue a collaborative project strategy by including different user and stakeholder groups in the development, testing and validation of tools and materials throughout the project by conducting four case studies focusing on terrorism, floods, pandemics and earthquakes. This ensures that the outcomes of the project reflects the needs of end users and ensures that the project's outcomes have a life span after the project has officially ended.

This document is a short report on workshop 2, case study on terrorism in Europe.

Contact persons for D4.2:

Susan Anson: susan.anson@trilateralresearch.com

Hayley Watson: hayley.watson@trilateralresearch.com

Kush Wadhwa: kush.wadhwa@trilateralresearch.com

Contents

List of Tables

List of Figures

Executive Summary

This report builds on TACTIC Deliverable 4.1, the short report on workshop one, terrorism in Europe, which examined how terrorism is different to other types of disaster, and what these differences mean for preparedness, as well as reporting the findings of workshop one. Deliverable 4.1 examined European terrorist attacks including the 2004 Madrid bombings, the 2005 (7/7) London attacks and the 2011 attacks in Norway by Anders Breivik (Anson, Watson and Wadhwa, 2015). The present report begins by outlining how Europe is becoming increasingly vulnerable to terrorism, as reflected by the 2015 attacks in Paris, Brussels and Copenhagen. It discusses how the second set of attacks in Paris in November 2015 highlighted the cross-border and cascading effects of terrorism and the need for preparedness for terrorism to be considered.

In Chapter 2, the report outlines the different types of organisations that participated in the second workshop on preparedness for terrorism in Europe. Actors from seven European countries and the United States of America participated in the workshop, with participants representing both organisations responsible for risk communication to the general public and organisations that represent the general public.

Chapter 3 outlines the content that was discussed with these representatives during the workshop and their feedback on the self-assessments, feedback reports and good practices categorisation available on the TACTIC Online Self-Assessment Platform (TOSAP). The workshop revealed that while participants could see the potential value of these tools, the feedback that they provided would need to be implemented to increase the likelihood of them actually using the tools. Their feedback on the tools related to:

- Acknowledging that organisations in European Member States are not always allowed to communicate about terrorism
- Reducing the length of the self-assessment(s) and feedback reports
- Including introductions so that the tools tell a story
- Considering the target audience
- Reviewing the terminology and content, which was overwhelmingly described as “too academic”
- Their features (e.g., including a progress bar on the TOSAP rather than page numbers)
- Providing additional explanatory information (e.g., explaining at the start of the self-assessment that there is a feedback process)

This feedback will be discussed and considered, together with the feedback from the other case study workshops, in order to develop and further refine the self-assessments, feedback reports, good practices categorisation and the TOSAP.

1. Introduction

This report builds on Deliverable 4.1 (D4.1), the short report on Workshop 1, Case study Terrorism in Europe (Anson, Watson and Wadhwa, 2015). Since the workshop in February 2015, the TACTIC partners have been using the participant feedback to further develop and refine the self-assessments and good practices categorisation available on the TACTIC Online Self-Assessment Platform (TOSAP). While D4.1 and the first workshop focused on actors preparing for terrorism in London, this report and the second workshop focused on the threat of terrorism across Europe. As outlined in D4.1, many countries across Europe have experienced acts of terrorism, including the 2004 Madrid bombings, the 2005 London bombings and the 2011 attacks in Norway (Anson, Watson and Wadhwa, 2015). These acts of terrorism include large-scale co-ordinated attacks with cross-border and cascading effects. A cascading effect refers to when the impact of an event or incident generates a further sequence of events that result in physical, social or economic disruption (Alexander et al., 2014). The Madrid bombings can be characterized as a large-scale terrorist attack, which involved a series of ten co-ordinated bombs explosions on four commuter trains (Raab and Jones, 2014). The attacks resulted in the deaths of 191 people and more than 1,800 people were injured. Furthermore, the 2004 Madrid bombings resulted in cross-border implications in terms of heightened security alerts in other European countries, including France and Portugal (BBC, 2004). The London bombing attacks on the London Underground and a bus on 7th July (7/7) 2005 resulted in the deaths of 52 people and 770 people injured (London Assembly, 2006). The attacks led to a number of cascading effects, including "chaos" on the transportation network as the London Underground and buses in central London were suspended and mainline trains, airport services and roads were also affected (The Guardian, 2005a). Further impacts of the London bombings included communication issues associated with network congestion and mobile phones being unusable, disruption to the healthcare sector and the closure of schools within London boroughs (London Assembly, 2006; The Guardian, 2005b; Ford, 2005). Since February 2015, there has been a notable increase in the threat of European citizens to acts of terrorism.

According to reports, Europe is becoming increasingly vulnerable to the rising threat of terrorism (Barnato, 2015). While 2014 saw a low number of terrorist attacks in EU Member States (Europol, 2015), in early 2015 attacks took place in Paris, Brussels and Copenhagen (Khindria and Meyers-Belkin, 2015). The October 31st crash of a Russian charter plane over Egypt's Sinai desert, claimed the lives of 224 people and has since been confirmed as a terrorist attack that resulted in hundreds of British tourists being stranded in Sharm el-Sheikh (Steafel, Lawler and Millward, 2015). On 13 November 2015, Paris faced a second terrorist attack, which has been considered by some as the worst terrorist attack in Europe since the 2004 Madrid bombings (Odell, 2015). Seven co-ordinated attacks, involving bomb explosions and shooting attacks, claimed the lives of at least 129 people, critically injured 99 people and injured 352 people (Steafel et al., 2015). More than 20 people from a number of countries outside of France lost their lives in the attack (BBC, 2015) and there is evidence that the attacks will have cascading effects in terms of policies related to the refugee crisis and the closing of borders across Europe (Hewitt, 2015). For instance, following the attacks, France has introduced temporary border controls and multiple countries, including Germany, have suspended the Schengen agreement which enables passport free movement across the countries that participate in the agreement (Ibid). Highlighting the cross-border implications of a terrorist attack, the attacks in Paris resulted in the "lockdown" of Brussels, as the suspected gunman from the Paris attacks was rumoured to have travelled to Brussels (BBC News, 2015b). Eight days following the Paris attacks, the terror alert in

Brussels was raised to level four, indicating that there was a "serious and immediate threat" and that members of the public should avoid visiting areas where groups gather, including airports and train stations, concerts, major events and commercial districts (Sehmer, 2015). Following the terror alert being raised, schools, universities, the metro system, shops, museums, restaurants and bars were closed for days (Matharu, 2015). The large-scale nature of terrorist attacks and the resulting cross-border and cascading effects highlights the importance of examining community preparedness towards an act of terror.

As outlined in D1.1 and D4.1, the nature of terrorist attacks may also change as future terrorism could include cyber-attacks (Shreve et al., 2014). The increasing threat of cyber terrorism is reflected in the creation of the UK's first "cyber force" designed to combat the online threat from terror groups (Wright, 2015). Groups such as ISIS are reported to be "developing increasingly sophisticated cyber capabilities" which could be used to target electricity supplies, air traffic control or hospitals online (Ibid). While there are no known fatalities directly resulting from a cyber-attack, future cyber-terrorism attacks targeting air traffic control and the Highways Agency's and hospital's networks have the potential to have a similar impact as the Paris attacks (Starling, 2015).

The increasing threat of terrorism requires communities to prepare themselves to respond to future terrorist attacks (Bullock, Haddow and Coppola, 2013). While there are elements in relation to preparedness for terrorism that are similar to preparedness for other types of crises (e.g., the restoration of critical services, the development of response aids/training and the empowerment of community leaders), D4.1 examined how terrorism is different to other disasters, and what these differences mean for preparedness. The key findings highlighted in D4.1 include that:

- Terrorism is characterised as being the result of deliberate human activity, high uncertainty, unpredictability and complexity, the low probability of an attack occurring and terrorist's intention to induce fear
- The characteristics of terrorism typically mean that communities are prepared indirectly through a multi-hazard approach
- For terrorism, the focus is on requesting the public's assistance to prevent, rather than prepare for, an attack through vigilance
- The responsibility for preparing for a terrorism is viewed as predominantly belonging to organisations, who undertake a range of activities to prevent, prepare for, respond to and recover from a terrorist attack

The findings from D4.1 were used to further develop and refine the self-assessments, feedback reports, good practices categorisation and TOSAP, that were presented to participants during the second workshop on terrorism in Europe. This report focuses on the second workshop. First it provides an overview of the different types of actors that are preparing for terrorism and that participated in the workshop. It then moves on to outline the second workshop on terrorism in Europe, including the agenda for the workshop, the scenario presented to workshop participants, and the key findings related to the self-assessments, feedback reports and good practices categorisation that are available on the TOSAP. The second workshop on terrorism in Europe was held on 3 November 2015, before the attacks in Paris. It is important to note that if the workshop had been held following the attacks, the findings may be different. For instance, while the workshop participants indicated that politically countries across Europe do not want to communicate with the public concerning terrorism, following the attacks, the French Government

published a poster (Figure 1) informing the public what to do in response to a terrorist attack. Furthermore, in the UK in December 2015, the National Police Chiefs' Council released a video informing the public of how to respond to a firearms or weapons attack (Krol, 2015). Thus, the attacks may act as an impetus for countries across Europe to review how they communicate with their public about preparedness for terrorism.

Figure 1 - Poster by the French Government on how to respond to a terrorist attack[1]

2. Actors responsible for preparing for terrorism across Europe

As examined in Section 1, countries across Europe have experienced acts of terrorism. While the first workshop on terrorism in Europe (Task 4.3) focused on London, the second workshop (Task 4.4) focused on terrorism across Europe. Seven European countries, including Belgium, the Czech Republic, Greece, Malta, Spain, Turkey and the United Kingdom, and the United States of America were represented during the second workshop on terrorism in Europe. The participants included both actors responsible for communicating risk information to the public and actors that work directly with or comprise the general public. Table 1 provides a brief overview of the different categories of organisation that workshop participants belong to. In order to protect participant's identity, detailed information is not provided.

[1] Gouvernement.fr, Reagir-en-cas-d-attaque-terroriste, 2015. [Online] http://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2015/12/reagir-en-cas-d-attaque-terroriste.pdf (Accessed 21 December 2015).

Table 1 - Organisations participating in Workshop 2 on Terrorism in Europe

Type of organisation	Relevance to the Case Study on Terrorism in Europe
Non-Governmental Organisations	These organisations aim to increase community preparedness by providing organisations, businesses and/or the general public with information and resources related to disaster preparedness and resilience.
National, regional and local level government authorities responsible for communicating risk information to the general public	In many European countries, there is a (legal) requirement for authorities to provide risk information to the general public. However, this does not specifically cover terrorism and as outlined below in some countries there are restrictions on communicating with the public about terrorism.
Academic institutions	Academics with expertise in cross-cultural and multi-hazard preparedness and radicalization participated in the workshop.
The emergency services (police, fire and ambulance)	All three emergency services that would respond to a terrorist attack were represented during the workshop.
Representatives from related research projects	Representatives from the following European Commission funded projects participated in the workshop: 1) THREATS focusing on increasing the resilience of EU hospitals to terrorist attacks 2) eVACUATE focusing on ICT-enabled emergency evacuation processes 3) ZONeSEC focusing on the security of Widezones (i.e., large area facilities).
Independent organisation's working with communities to counter extremism	The workshop included a representative from an organisation working on programmes designed to tackle the different drivers of extremism. In addition to the high-level strategic interventions, the organisation engages directly with civil society.
Volunteer rescue organisations	This voluntary organisation was created to protect and preserve human life. The organisation is comprised of a number of units, including: First Aid and Ambulance, Search and Rescue and Disaster Response. In addition, the organisation raises safety awareness amongst school children and the private sector.
Government psychology experts	A government psychologist specialising in security threats participated in the workshop.

It is important to note that while organisations responsible for communicating risk information to the general public participated in the workshop, the communication of information specifically for terrorism is more complex. Workshop participants outlined how there are restrictions in some European countries that prohibit organisations responsible for risk communication from communicating about the threat of terrorism due to political reasons. This was related to specific information for terrorism having restricted access and the concern that communicating about terrorism would result in fear in the public. As highlighted in D4.1, communication for terrorism is predominantly part of a multi-hazard approach.

In addition to the external organisations that participated in the workshop, TACTIC partners (Cheney Shreve from Northumbria University, Alkiviadis Giannakoulias from European Dynamics SA and Nuray Karanci from Middle East Technical University) participated in and supported the workshop by giving presentations and using the evaluation methodology to elicit feedback. The workshop was organised by Trilateral Research.

3. Workshop 2 on terrorism in Europe

Trilateral Research hosted the second workshop on preparedness for terrorism in Europe on 3 November 2015 in London. In order to enable participants to test the self-assessments, the workshop was held in a computer suite. Twenty-five representatives participated in the workshop from eight countries. A full list of participating organisations can be found in Appendix A. Table 2 provides an overview of the agenda for the workshop. The full agenda is provided in Appendix B.

Table 2 – Overview of the workshop agenda

Session	Description
1	An overview and background to the TACTIC project, including the objectives and structure of the project, TACTIC's focus on preparedness and risk communication and an introduction to the self-assessments and catalogue of good practices of communication and education for preparedness. During this session, workshop participants introduced themselves and their role.
2	Presentation on the terrorism case study, including how terrorism is different to other types of hazard and the cyber-terrorism scenario. During this session, participants were asked a number of questions to understand the different elements of preparedness for terrorism before, during and after an attack and the potential cascading effects and cross-border communication resulting from a terrorist attack.
3	Presentation of the TACTIC Online Self-Assessment Platform (TOSAP).
4	Completing and assessing the TOPSAP. Participants worked in groups to complete the self-assessment. As they were doing so, a facilitator asked them a series of questions comprising the evaluation methodology.
5	Discussion and feedback on the feedback reports.
6	Presentation and discussion of the good practices categorisation.
7	Next steps and information on the TACTIC conference.

3.1. The terrorism scenario

When comparing terrorism to other types of disaster, there are elements that are unique to terrorism, such as the focus on vigilance. The second workshop on terrorism included a scenario in order to enable participants to consider the different elements that need to be taken into consideration to prepare for, respond to and recover from a terrorist attack. Trilateral Research presented the scenario to encourage participants to think about the different issues that need to be considered in how organisations communicate preparedness information for terrorism to the public and how the public can prepare themselves to respond to a terrorist attack.

As future terrorism may include cyber-attacks that have the potential to cause as great an impact across Europe as a bomb or firearms attack, the scenario involved a cyber-terrorism attack. In order to ensure that the scenario would have implications for workshop participants from a number of European countries, it was decided that the scenario would focus on a cyber-terrorism attack affecting airport operations in two countries, the UK and Denmark but that would have wider implications for other European countries. The development of the scenario involved phone calls with a crisis management expert with experience of managing security incidents in the aviation sector and conducting an online review of cyber-attacks that have impacted on an airport's operations.

The final scenario drew on the cyber-attack experienced by Polish airline LOT on 21 June 2015. The attack on the airline's ground computer systems that are used to issue flight plans resulted in 10 national and international flights being cancelled and 1, 400 passengers grounded (The Guardian,

2015). In order for the scenario to comprise a large-scale attack, the scenario also involved a fire-arms attack in central London at King's Cross railway station and St. Pancras International where the Eurostar is located. This element of the scenario was introduced following a recommendation from one of WP 4's Practical Case Study Partners (PCSP) to include a firearms attack. The addition of the fire-arms attack to the scenario would also result in cascading effects primarily in terms of the availability and functioning of the public transportation system. For instance, the shutting down of the Eurostar service and train stations in the vicinity would result in congestion in the transport network. Highlighting how social media can be used to spread rumours during a crisis, the last element of the scenario involved rumours on social media concerning someone with a gun at Luton airport. Figure 2 features the key scenario slides presented during the workshop.

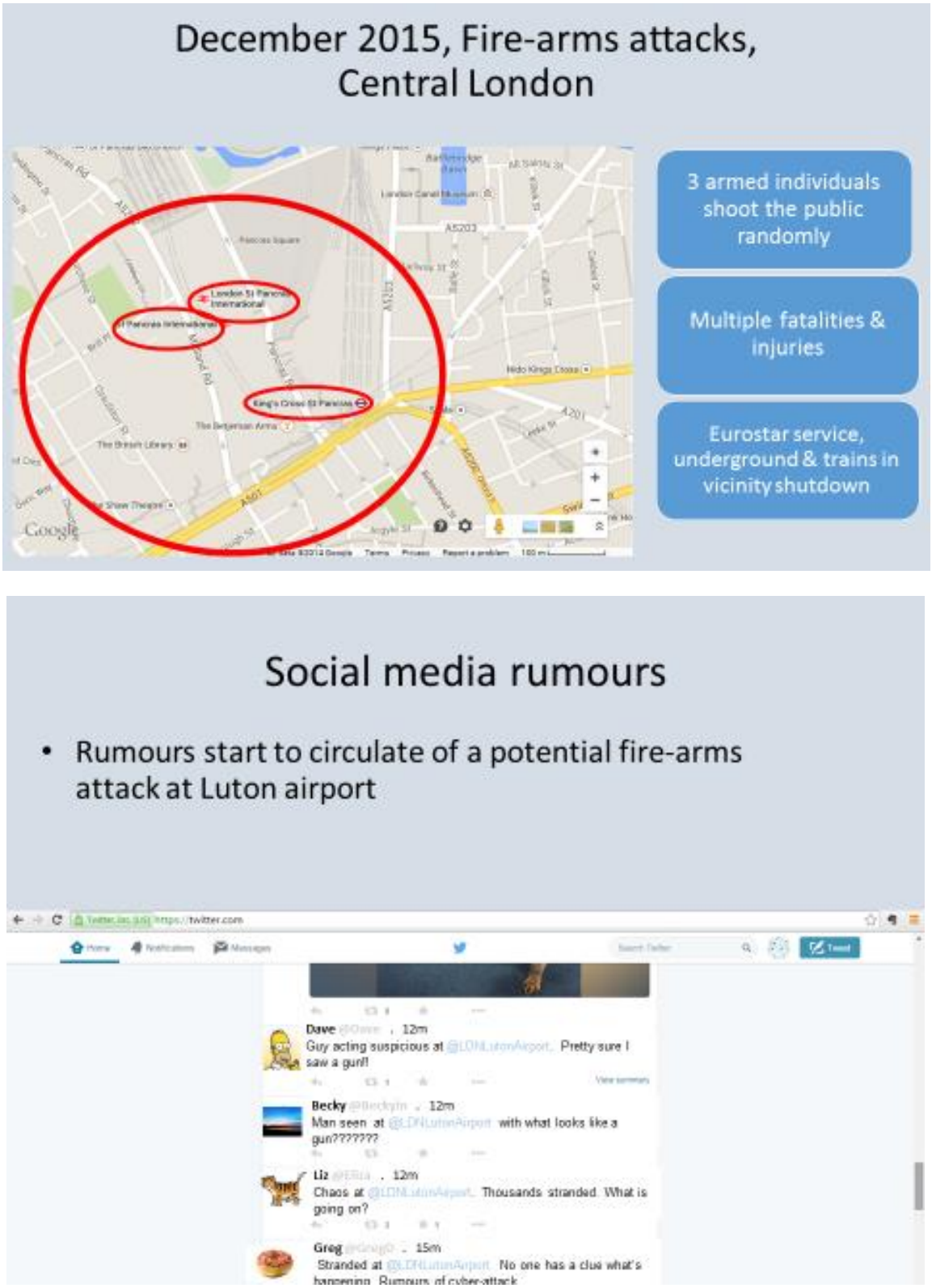

Figure 2 - Scenario slides from workshop 2

In order to encourage participants to consider community preparedness for large-scale and cross-border terrorist attacks with cascading effects, a series of questions were asked following the scenario presentation. The questions and participant responses are highlighted in Table 3.

Table 3 - Questions and findings emerging from the terrorism scenario

Question	Participant responses
How could authorities have prepared the public to respond to this type of terrorist attack in advance of the incident?	• In the UK, information is provided on the threat level for terrorism which is currently at severe. However, the public are not given any additional information and are not told what to do with this information. There is also the potential for threat levels to instil more fear in people or for it to create complacency. For example, in London there has become a desensitisation to threats. As there is always a threat in London, it has become normal. • Organisations and businesses are very well advised of what to do when there is an incident. • We cannot expect the public to respond immediately. Preparedness and changing awareness is a "long game" requiring a culture change. The public should not rely on the emergency services so much and there needs to be more individual responsibility. • Small scale incidents such as fires, gas leaks and snow could be used to train and prepare the public. For example, by encouraging them to think about meeting points in the event of an incident. • In countries/cities where there is a bomb every week, people are alert. In London there hasn't been a bomb for ten years so people don't feel constantly under threat. This is different to the situation in Belfast and Israel where there is a high state of alert.
What information needs will the public have during the response to this type of incident?	• How it's going to affect them and their family. • Where to go. • What to do.
What are the potential cascading effects of this type of incident?	• Civil unrest. • The uncertainty can cause panic such as during the 2011 London Riots. Workshop participants recognised the power of social media to create panic and confusion for the emergency services and the public. It was suggested that the public need to see an authoritative response on social media that curbs the panic and that offers official and factual reports.
How would you coordinate with organisations in neighbouring countries?	• As part of the Benelux Union, Belgium has contacts in the Netherlands and France that they would co-ordinate with. In terms of the January 2015 terror attacks in Paris, a cross-border contact shared information that rumours being spread on social media about the planned transport route of the two men were untrue. • Best practice is often circulated. • In Spain, information is shared with other Member States. For terrorism, there is a cross-border communications office. • The Red Cross has a central coordination body. Within each national society, there is an emergency response unit. The Federation will coordinate relevant countries and deploy skills from the entire pool.
How can the public be prepared to support their recovery from this type of incident?	• The discussion around this question focused on whether there is a definition of how to prepare the public and what we want them to do. • There is uncertainty with terrorism and an increased focus on prevention rather than response. Authorities request that the public report any suspicious activity. • In the United States, information is provided to the public on what to do before, during and after different types of attack. • People will assist during the response as citizens are the first responders. In line with this, there is a need for first aid training. • There is a conflict between raising the terrorism alert level and then not wanting people to respond or saying, "don't worry about it".

3.2. Key findings from the workshop

Following Trilateral's presentation of the terrorism scenario and the subsequent discussions, European Dynamics presented a high-level overview of the TOSAP to the workshop participants. Following the presentation, participants were asked three questions comprising the first part of the evaluation methodology. These questions are outlined together with participant's responses in Table 2.

Table 4 - Participant feedback

Question	Responses
What do you expect from the tool?	**Organisational Self-Assessment** • To be able to identify risks and vulnerabilities. • To identify the organisational and community's responsibilities. • To identify the communication gaps between organisations and the public (e.g.., what does the public need to know, how can information be delivered to communities with cultural diversity). • To understand cultural differences (e.g., in the use of CCTV). • To be provided with tailored tools and resources (e.g., geotagged resources). • To be directed to resources (e.g., where to go to learn about first aid). • To learn about communicating with social media. Everyone has problems with social media. Participants would like guidance on how to best use it. **General Public Self-Assessment** • To identify the threats and risks that would affect them as a community. • To identify the information that the general public can expect from authorities. • To identify the actions and things that they can do (e.g., creating a grab bag). • To know what communication they should expect from authorities (e.g., should they have a basic understanding of threats?).
Do you have any experience with similar tools?	The American Red Cross provides the online Ready Rating[2] service that assists businesses schools and organisations in becoming better prepared for a disaster. Participants did not mention any tools similar to the TOSAP that are available in Europe.
How important is receiving feedback on your risk communication/suggestions how you can improve your risk communication for you?	• Motivation is a challenge as people rarely start thinking about preparedness until something goes wrong. Then there is the window of opportunity (i.e., the event), however interest drops off. • In some instances, it is not important whether something really works in practice, but rather it is a case of boxes being ticked. Organisations should be asked whether they have the will to be resilient. • Events will always drive the level of importance placed on preparedness. • Denial plays a role as people cannot live in fear of an attack, which affects levels of interest and perceived importance.

3.2.1. Feedback on the self-assessments

Following the completion of the first part of the evaluation methodology, the workshop participants were split into groups of approximately five people, with two members of each group registering to use the TOSAP. Three groups then worked through the organisational self-assessment, with a further two completing the general public self-assessment. A facilitator worked with each group asking questions that comprised the second part of the evaluation methodology. Questions included whether each question and response option was understandable, reasonable and relevant, and whether there was anything missing. Additionally and highlighting the participant's engagement with TACTIC and the project's tools, Trilateral received further e-mail feedback on the self-assessments from four workshop

[2] American Red Cross, Ready Rating, 2015. [Online] http://www.readyrating.org/ (Accessed 18 December 2015).

participants. The Appendix contains participant feedback by question (Appendix C) and also general feedback on the self-assessments (Appendix D). A high-level overview of the key feedback on the self-assessments is highlighted in Table 5. While participants could appreciate the potential value of the self-assessments, their feedback would need to be addressed in order for them to actually use them.

Table 5 - Participant feedback on the Self-Assessments

Organisational Self-Assessment	General Public Self-Assessment
As the self-assessment is too long in terms of the number of pages and amount of content, the content should be condensed.	Clarify terms that are vague or confusing (e.g., the terms "community" and "voluntarily").
Organisations are not always allowed to communicate with the public about terrorism. For example, emergency plans have restricted access.	Provide detailed information on the self-assessment in order to correctly set the general public's expectations.
Enable all nationalities to register on the TOSAP, not just the TACTIC countries.	The self-assessment is too long.
Include introductions to sections so that the self-assessments tell a story.	Explain the feedback process at the beginning of the self-assessment.
The audience is too broad. Consider use cases to narrow the audience down.	Explain what is meant by community.
Consider audiences that might not have Internet access.	Consider the use of the term "preventing".
Provide detailed information on the purpose of the self-assessment.	Provide descriptions of emergency kits and emergency plans.
For some questions, the scales are unclear.	
Be consistent in the use of terminology.	
There is overlap between questions.	
Include a progress bar instead of page numbers.	
Reorder the questions (e.g., in terms of the organisational self-assessment, the questions on the aims of risk communication (Questions 34-37) should come earlier).	
Simplify questions that are too wordy and academic and provide clarification for questions that are unclear. In some instances, it may be necessary to delete questions.	

3.2.2. Feedback on the feedback reports

Once participants had finished reviewing the self-assessments, they were provided with hard copies of the long and short versions of the feedback reports and were able to view PDF copies on the computers. European Dynamics also demonstrated the feedback reports for flooding on the TOSAP to participants. The lack of time meant that it was not possible to go through the feedback reports in detail, however some general feedback is provided in Appendix D. Participants stressed the importance of not having a long feedback report. One participant recommended that there should be a one-page feedback report providing recommendations and practical advice. Additionally, it was suggested that the feedback report could provide a comparison between the user and other organisations.

3.2.3. Feedback on the good practices categorisation

In the penultimate session, participants were provided with examples of different practices that had been categorised by UFZ. Feedback provided on the categorisation is summarised in Figure 3 and is included in more detail in Appendix D. Again, while participants found the good practices interesting,

Figure 3 includes recommendations that can increase the value that the good practices will provide to users of the TOSAP.

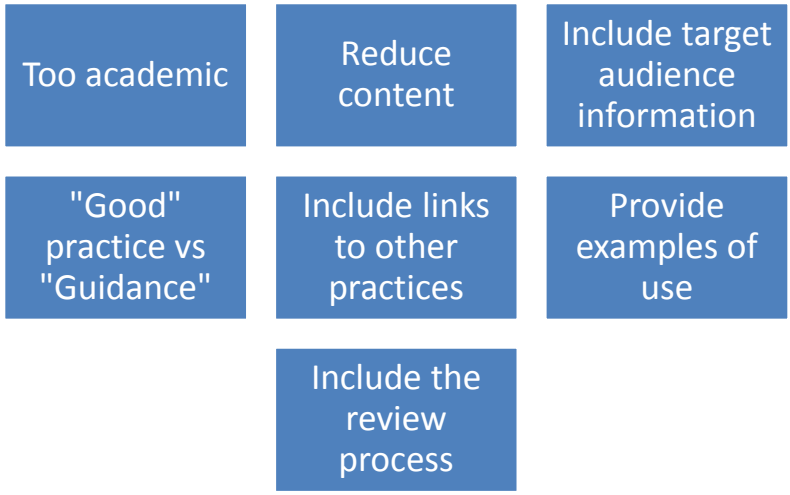

Figure 3 - Feedback on the good practices categorisation

4 Workshop summary and next steps

At the end of the workshop, participants were presented with an evaluation form to provide feedback on the workshop. The amount of information, the quality of the presentations, the time for discussion, the workshop venue and the organisation of the workshop were consistently rated as good. Nearly all of the participants expressed an interest in evaluating the final version of the TOSAP at a later date and in attending the TACTIC conference in March 2016.

A lot of useful data was gathered during the workshop that will be used to further develop and refine the self-assessments, feedback reports and good practices categorisation before they are presented at the TACTIC conference. Trilateral will work with the relevant TACTIC partners to discuss and implement the recommendations outlined in Appendices C and D (where appropriate and possible). If further clarification is needed in developing the tools hosted by the TOSAP, Trilateral will seek guidance from the Practical Case Study Partners and workshop participants as required.

References

Alexander, D., Bartels, M., Hagen, K., Hahne, M., Hempel, L., Kreissl, R., Pelzer, R., Pescaroli, G., Ritchey, T., Tzanetakis, M., Wadhwa, K., and Watson, H. "Interdependencies and Cascading Effects in Crisis Situations", Deliverable 1.1 of the FORTRESS project, 31 July 2014.

Anson, S., Watson, H., and Wadhwa, K., "Workshop 1: Case Study Terrorism in Europe", Deliverable 4.1 of the TACTIC project, 31 March 2015.

Barnato, Katy, Europe, Canada, Australia face rising terror threat: Report, 25 May 2015. [Online] http://www.cnbc.com/2015/05/25/europe-canada-australia-face-rising-terror-threat-report.html (Accessed 17 November 2015).

BBC News, France raises alert to 'orange', 12 March 2004. [Online] http://news.bbc.co.uk/1/hi/world/europe/3505094.stm (Accessed 17 November 2015).

BBC News, Paris attacks: Who were the victims?, 27 November 2015. [Online] http://www.bbc.co.uk/news/world-europe-34821813 (Accessed 17 November 2015).

BBC News, Brussels lockdown: How is city affected by terror threat?, 24 November 2015b. [Online] http://www.bbc.co.uk/news/world-europe-34900353 (Accessed 25 November 2015).

European Law Enforcement Agency (Europol), European Union Terrorism Situation and Trend Report, 2015. [Online] https://www.europol.europa.eu/content/european-union-terrorism-situation-and-trend-report-2015 (Accessed 16 November 2015).

Hewitt, Gavin, Paris attacks: Impact on border and refugee policy, 15 November 2015. [Online] http://www.bbc.co.uk/news/world-europe-34826438 (Accessed 17 November 2015).

Krol, Charlotte, 'Run, hide and tell': Watch what to do in a firearms or weapons attack, 18 December 2015. [Online] http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/12057122/Run-hide-and-tell-Watch-what-to-do-in-a-firearms-or-weapons-attack.html (Accessed 22 December 2015).

Matharu, Hardeep, Brussels lockdown: State of emergency has created 'Islamic regime' in Brussels, says city's mayor, 24 November 2015. [Online] http://www.independent.co.uk/news/world/europe/brussels-lockdown-islamic-regime-state-of-emergency-a6746956.html (Accessed 25 November 2015).

Odell, Mark, Paris attacks: What we know so far, 16 November 2015. [Online] http://www.ft.com/cms/s/0/2a018474-8c63-11e5-a549-b89a1dfede9b.html#axzz3rg2WSqDd (Accessed 16 November 2015).

The Guardian, Transport chaos after London blasts, 7 July 2005a. [Online] http://www.theguardian.com/travel/2005/jul/07/travelnews.terrorism.transportintheuk (Accessed March 2015).

The Guardian, Hospitals treat hundreds of blast casualties, 7 July 2005b. [Online] http://www.theguardian.com/society/2005/jul/07/hospitals.terrorism (Accessed March 2015).

The Guardian, Hackers ground 1,400 passengers at Warsaw in attack on airline's computers, 21 June 2015. [Online] http://www.theguardian.com/business/2015/jun/21/hackers-1400-passengers-warsaw-lot (Accessed 23 October 2015).

Sehmer, Alexander, Brussels terror threat: Special forces arrest four people after warnings of 'imminent threat', 21 November 2015. [Online] http://www.independent.co.uk/news/world/europe/paris-attacks-brussels-raises-terrorism-alert-to-highest-level-warning-of-serious-and-immediate-a6743076.html (Accessed 25 November 2015).

Shreve, C., Fordham, M., Anson, S., Watson, H., Hagen, K., Wadhwa, K., Begg, C., Müller, A., Kuhlicke, C., and Karanci, N., "Report on risk perception and preparedness", Deliverable 1.1 of the TACTIC project, 31 December 2014.

Starling, Boris, How close could Britain be to a cyberterrorist attack?, 22 November 2015. [Online] http://www.telegraph.co.uk/technology/12008964/How-close-could-Britain-be-to-a-cyberterrorist-attack.html (Accessed 25 November 2015).

Steafel, Eleanor, Rory Mulholland, Rozina Sabur, Edward Malnick, Andrew Trotman and Nicola Harley, Paris terror attack: Everything we know on Saturday afternoon, 21 November 2015. [Online] http://www.telegraph.co.uk/news/worldnews/europe/france/11995246/Paris-shooting-What-we-know-so-far.html (Accessed 17 November 2015).

Steafel, Eleanor, David Lawler and David Millward, Terrorists 'boasted' to Isil leaders about bombing plane, stranded Brits 'could face ten day delays' - as it happened on Saturday November 7, 08 November 2015. [Online] http://www.telegraph.co.uk/news/worldnews/europe/russia/11981239/Russian-plane-crash-sharm-el-sheikh-stranded-British-tourists-missile-latest-updates.html (Accessed 21 December 2015).

Wright, Oliver, Isis plotting cyber warfare to kill people in UK, claims George Osborne, 17 November 2015. [Online] http://www.independent.co.uk/news/uk/politics/paris-terror-attack-uk-government-to-invest-2bn-in-cyber-force-to-combat-online-terror-threats-a6737071.html (Accessed 18 Nvember 2015).

Appendix A – Workshop: list of participating organisations

Organisation	Type	Country
British Red Cross	Non-governmental organisation	UK
Emergency Response and Rescue Corps	Non-governmental organisation	Malta
European Dynamics	Industry	Greece
DG Centre de crise du SPF Intérieur	Government	Belgium
Global Disaster Preparedness Center / American Red Cross	Non-governmental organisation	United States of America
Government of Catalonia	Government	Spain
Hanover Associates	SME	UK
Institute for Strategic Dialogue	Non-governmental organisation	UK
Islington Borough (Local Authority)	Government	UK
London Ambulance Service	First responder	UK
London First	Non-governmental organisation	UK
London Metropolitan University	Academia	UK
Mersey Fire	Government	UK
Middle East Technical University	Academia	Turkey
Ministry of Interior	Government	Czech Republic
Northumbria University	Academia	UK
Policia de la Generalitat- Mossos d'Esquadra	Government	Spain
Telesto Technologies	Industry	Greece
Thrivespring	Non-governmental organisation	UK
Total Resilience Ltd	Non-governmental organisation	UK
Trilateral Research Ltd	SME	UK
University College London	Academia	UK

Appendix B – Workshop agenda

TACTIC

TOOLS, METHODS AND TRAINING FOR COMMUNITIES AND SOCIETY TO BETTER PREPARE FOR A CRISIS

Workshop 2 for Case Study 1: Terrorism in Europe

London, 3 November 2015

Agenda

Timings	**Session**
9.00-9.30	Registration
9.30-9.40	**Trilateral Research & Consulting** • Welcome • Participant introductions
9.40-10.00	**Northumbria University** • Overview and background to the TACTIC project • Introducing the organisation's and general public's self-assessments and catalogue of good practices of communication and education for preparedness and how these feed into the long-term framework for improving community preparedness and the online platform
10.00-10.30	**Trilateral Research & Consulting** • Overview of the case study on terrorism and how is preparing for terrorism different to preparing for other types of hazard in Europe? • The cyberterrorism scenario
10.30-11.00	**European Dynamics** • Presentation of the online platform and the self-assessments
11.00-11.20	Tea and coffee break
11.20-12.45	Completing and assessing the self-assessments • Participants will work in groups and complete either the organisational or general public self-assessment • Group feedback will be provided on the structure, questions and design of the self-assessment
12.45-13.30	Lunch
13.30–15.00	Assessing the self-assessments continued • Group evaluation of the self-assessments • Introduction and discussion of the feedback reports
15.00-15.20	Tea and coffee break
15.20-16.20	**Middle East Technical University / Trilateral Research & Consulting** The catalogue of good practices • Presentation of the good practices categorisation • Feedback on the catalogue of good practices
16.20-16.30	**Trilateral Research & Consulting** • Next steps and discussion surrounding the conference

Appendix C – Feedback on the self-assessments by question

Number of question	Original question	Problem description	Suggested changes
Organisational self-assessment			
T4	Has your community/city/region ever experienced a terrorist attack?	Terrorism can be interpreted differently. For example, participants discussed whether the attack on Lee Rigby constituted a terrorist attack.	Provide clear guidance at the beginning of the terrorism self-assessment on how the self-assessment defines terrorism.
T5	If you answered yes to Question 4, when did a terrorist attack last occur in your community?	Does this question refer to a completed or attempted terrorist attack or a small or a large terrorist attack? Participants also questioned why seven years is used in the response options.	Provide clear guidance at the beginning of the terrorism self-assessment on how the self-assessment defines terrorism. Include information in the question that indicates why seven years is important in terms of awareness.
T6	If you answered yes to Question 4, have you or your organisation drawn out lessons from the most recent terrorist attack?	Participants did not think that this question was needed. If it stays in the self-assessment, more detail is required related to what the actual lessons were.	
T7	What lessons have you drawn?	There needs to be multiple options to this question.	
T1-9	1. Where is your organisation based? 2. What type of organization are you working for? 3. How many people are working in your organisation?	Participants were not sure about the purpose of this questions and commented that the questions could be narrowed down to one. They would prefer more precise	Include questions 1-3 as part of the registration process.

	8. Did you or your organisation share your lessons learned with others? 9. With whom your organisation shared your lessons?	questions, for example on the actions (e.g., meetings) taken to share lessons.	
T10	Is the risk of terrorism taken voluntarily or involuntarily by people living in areas considered at higher risk of terrorism (e.g., cities)?	Participants did not understand the question and commented that it needs to be stated clearly. The scale is also not obvious as only two boxes are required. The users do not understand why there are so many options. In addition, participants did not consider this question to be applicable to an organization and thought that it would be impossible to answer from an organizational standpoint.	Reword or remove the question. Reconsider the scale.
T11	Is the risk of terrorism natural or human-made?	This question is unclear. Is it the risk of terrorism that is natural or human-made or terrorism itself?	Reword or remove the question.
T13	Is the risk of terrorism familiar or unfamiliar?	This question is unclear.	Reword or remove the question.
T15	Is the risk of terrorism distributed fairly or unfairly within the community?	This question is difficult to understand. It should be the threat of terrorism rather than the risk.	Reword or remove the question.
T16	Is knowledge about the community's risk of terrorism certain or uncertain?	This question cannot be answered.	Reword or remove the question.
T10-16	12. Is the risk of terrorism threatening or not threatening? 14. Is the risk of terrorism manageable or unmanageable?	These questions were considered obscure and inappropriate as they were too personal and participants did not understand	Participants suggested including one question: "How at risk do you think you are of a terrorist attack?" to compare the risk perceptions of organizations and the general public.

		what the questions were referring to. The answers provided would be very subjective. In addition, they were considered “way too academic”. Participants wanted simple questions that can be understood by all.	Simplifying or removing the questions. Reconsider the scale. If the questions are left in, preface all questions with “in your opinion”.
T17	Have the challenges of preparing for terrorism, in relation to other types of risk, been considered?	There was a mixed response from different groups. One group would prefer for it to be kept in as terrorism is different. For another group, the response would be based on opinion.	Keep this question in. Preface with “in your opinion” and provide an explanation of how terrorism is different to other types of risk.
T18/19	18. How often do you collaborate with the following organisations in your day-to-day business? 19. In case of an emergency, which organisations do you collaborate with?	It is not clear what organised community of interests are or administrative organisations. Organisations communicating with the public could refer to all of the organisations that are listed. There is an inconsistent use of organization and institutions. Actors from the health sector is too broad. Religious organisations and the media are not included. Housing corporations does not translate across all societies.	Remove/reword some options or provide examples of each category. Narrow down the option e.g., organisations communicating with the public could be replaced with the media. Be consistent in the use of the terms organizations and institutions.
T18-23	20. Some hazards require that outside support must be brought in to support the local or regional disaster response.	The questions are asking the same question but in three different ways.	Participants suggested including one question covering “Who do you work with?”.

	Does your organisation have plans in place to coordinate with these groups? 21. Is your organisation in contact with organisations from neighbouring countries? 22. How regularly are you in contact with organisations from neighbouring countries? 23. Do you have communication plans with organisations from your neighbouring countries that might be affected by a terrorist attack?		
T29	In your opinion, how well are you and your organisation equipped with resources to prepare for the risk of terrorism in your community/city/region?	The definition of skills needs to be clearer. Participants think that the question can be included but the options removed.	Include the question but not all the different options (e.g., finances, staff, knowledge).
T30	Now we are proceeding with asking more specific questions about your risk communication activities…	This text should be more direct and user-faced and include information about why answering the questions are useful for the user (i.e., what will the list of questions do for the user).	Develop text that explains the purpose of answering the questions.
T31	How regularly do you internally talk about your risk communication activities?	This question needs to be clearer as it was unclear whether the question related to internal communication or external communication. The response would also depend on business size and who has responsibility.	Reword the question.
T34-37	Please specify which of the following aims are relevant for your organisation's risk communication activities related	One group of participants commented that raising risk awareness (Q.34) and warning in	Reorder the questions and provide additional information to make each option easier to

	specifically to the risk of terrorism. Please tick all that apply. 34. Raising risk awareness (i.e. informing people about risks) 35. Strengthening capacities to act (knowing what to do in case of emergency, knowing how to prevent terrorism, etc.) 36. Warning in case of emergency (what is known about an impending attack, what needs to be done by the population etc.) 37. Joint problem solving and conflict resolution (e.g. disputes about appropriate measures, tensions between different groups of the community, etc.)	case of emergency (Q.36) were the same. Instead of splitting by aim, they thought it would be more useful to split the questions by stage of the attack (i.e., before, during and after). These aims may change based on changing public risk perceptions. If the risk is low, sometimes no information is provided. These questions should come earlier in the assessment (or at least before questions 30-33).	understand. The text "At present…" could be added for further clarification.
T38	Do you provide detailed information about the risk of terrorism to your community/city/region?	It is not clear what the term detailed means. It is also not clear whether the question refers to on a daily basis or just in the event of an emergency. Participants also suggested that the response scale for this question should be changed to: sometimes, often, never, etc.	Remove the word detailed and provide further clarification in the wording of the question Change the response scale.
T39	Do you provide your community/city/region with general information on terrorism as part of a multi-hazard approach?	The term multi-hazard is not well understood.	Explain the term or alternatively use a different term.
T41	Did conflicts arise out of this difference in risk perception?	The use of 'conflict' is confusing here. The question needs to be more simply stated.	Better explain what is meant by conflict or provide an example so participants understand what we mean.

T43	How often on a scale from 1-5 do you use simple, graphical, and factual materials which avoid technical or specialised language when raising awareness of the risk of terrorism?	The wording is unclear and this question was not considered relevant for this hazard.	Reword to “How often on a scale from 1-5 do you use vivid, real images, examples, and anecdotes that communicate [to others] on a personal level when communicating the risk of terrorism?” or delete the question.
T46/T47	46. Do you think that the information you share concerning terrorism is well understood by your intended audience? 47. Are you actively collecting feedback on your communication practices related to the aim of raising awareness of the risk of terrorism?	The answer will depend on the delivery method. Question 46 should come after question 47.	Reorder question 46 and 47.
T51	How regularly does your organisation inform your community/city/region about the following issues?	Emergency plans for terrorism are restricted.	Remove this option.
T52/53	52. How well on a scale from 1-5 do you communicate the costs and benefits of taking specific actions to prepare for terrorism? 53. How well on a scale from 1-5 do you actively involve members of the general public in discussions about how to improve preparedness for terrorism?	This question needs to be clearer as it is not clear who the costs and benefits are communicated to. The wording of the questions also needs to be improved as participants thought that they were unclear and wordy. The questions were also suggested to not reflect how organisations communicate with the public.	Reword the questions. For example, question 52 could be reworded to “When you communicate with the public, does your organisation emphasize the potential benefits of taking these actions to the public?”.
T54	How do you provide your community/city/region with information about the risk of terrorism?	This question is duplicative as it was covered by the same question for raising awareness.	
T55	How clearly on a scale from 1-5 do you communicate your roles and responsibility for managing the risk of terrorism?	Roles and responsibilities should not be communicated for terrorism.	Delete the question.

T54/57	57. How do you communicate the general public's responsibilities with regards to terrorism?	These questions are too similar.	Consider whether these two questions can be merged.
T59	Are you actively collecting feedback on your communication practices related to the aim of strengthening the public's capacity to respond to a terrorist attack?	This question needs to be grouped with the other questions about collecting feedback.	
T63	In your opinion, what were the reasons that your warning was successful or unsuccessful? 63. The warning was very precise (e.g. time and location) 64. The warning provided no contradictory information 65. The warning was very timely 66. People have received a false warning in the past and therefore did not trust our last warning 67. We are continuously informing the public 68. We have used multiple channels to reach out to the public 69. We did not reach our audience since our communication channels were insufficient	These are confusing questions. It should not be about whether it was successful or unsuccessful.	Ask about what plays a role in warning the public and the degree of success.
T70	Which methods do you use for warning the population?	Too much repetition for every aim gets boring.	
T74	Are you aware of any conflicts concerning the risk of a terrorist attack in your community/city/region?	This question is too broad. Who is it referring to conflicts between?	Reword the question.
T87	Different target audiences have different communication needs. Are you interested in learning more about	The question is a yes/no question but then a list of different target audiences is provided.	Reword the question.

	communicating with certain groups of the public about the risk of terrorism?	Is gender important to an organization? The 4th grouping needs a header. The list is too long and there is overlap between the different categories. Tourists and travellers need to be included.	
General public's self- assessment			
T1	Now we would like to gain a brief overview about how you perceive the risk of terrorism and your involvement in community life	The location of this text is confusing.	Move the text to somewhere else.
T11	Please describe how often you: Think about terrorism Talk about terrorism	Who does the term "you" refer to? Is it you as the community or you as the individual?	Provide further clarification on who "you" refers to.
T14	The risk of terrorism is taken voluntarily or involuntarily by people living in areas considered at higher risk of terrorism (e.g., cities)	Participants do not like this question and the wording of this question (e.g., the use of the word voluntarily).	Delete or reword the question.
T15	The risk of terrorism is natural or human-made	What is meant by the word "natural"?	Reword the question.
T16	The risk of terrorism is threatening or not threatening	Participants questioned the use of the word "threatening". The use of the word "risk" was also considered inappropriate.	Reword the question.
T19	The risk of terrorism is distributed fairly or unfairly within the community	Participants questioned the wording of this question.	Reword the question. Participants suggested changing the wording of the question to "The risk of terrorism is distributed equally within the community".

T14-20	17. The risk of terrorism is familiar or unfamiliar 18. The risk of terrorism is manageable or unmanageable 19. The risk of terrorism is distributed fairly or unfairly within the community	These questions were considered too academic in nature.	Delete or reword the questions.
T23	Have you informed yourself in the past about the risk of terrorism in your community?	Participants questioned the wording of this question.	Participants suggested that the wording be changed to “Have you been informed in the past about the risk of terrorism in your community?”

Appendix D – General feedback on the self-assessments, the feedback reports and the good practices categorisation

Issue	Proposal for its solution
Organisational self-assessment	
Group: 46 pages is too long and the users would switch off before completing the self-assessment. They would prefer a version that is ten pages maximum.	Reduce the number of pages by reducing the content. Participants recommended a maximum of 10 pages. Condense the 4-5 questions on the same theme into 1. Alternatively, workshop participants suggested removing the page numbers and including a progress bar instead.
TRI_SA: Communicating about terrorism is difficult and depends on the political party in power. In some countries, organisations are unable to communicate about terrorism.	Include a question in the self-assessment about whether the user is responsible for / allowed to communicate with the public about preparedness for terrorism.
TRI_SA: As the user has already registered, the answers for the first three questions should already be completed.	Link the registration process to the first three questions.
Group: The TOSAP should provide the ability for all nationalities to register, not just limit it to the "TACTIC" countries.	Add additional countries to the registration options.
Group: The use of "organization" is too broad as it could cover a small business or an international NGO.	The participants suggested the inclusion of different "use cases" within the self-assessment.
TRI_AD: The questions need to be reordered and introductions added to the different sections (e.g., at the beginning of each section on the different aims).	The ordering of questions and the overall "story" that the self-assessment is telling needs to be considered. Participants requested a well-structured survey with introductions to different sections from the user perspective, that guide the user through the process.
METU_NK: The whole community does not have access to the Internet.	
Group: Some questions need to be simplified as they are too wordy, academic and cannot be understood.	Reword questions to simplify them and make them easier to understand.
E-mail feedback: Detailed information on the purpose of the self-assessment needs to be provided before the user starts it.	Provide detailed information on the purpose and format of the self-assessment before the user starts taking it.

E-mail feedback: The need for a different self-assessment for each hazard was questioned. Instead, the commonalities across the different hazards could be exploited.	Discuss this with the TACTIC partners in line with the feedback from the other workshops.

General public's self-assessment

Group: The assessment was not what they were expecting as they were expecting to receive a risk matrix informing them of what their risks are.	Provide detailed information on the purpose, format and outputs of the self-assessment.
UoN_CS: Users would like a banner notifying you that the self-assessment skips questions or the question numbers to be automatically updated.	Include a progress bar and explanation that the self-assessment will not include all questions.
UoN_CS: The self-assessment is too long.	Reduce the length of the self-assessment.
UoN_CS: The questions need to be reordered as there is some overlap.	Review the questions and remove/merge questions when appropriate.
UoN_CS: Some of the questions were too academic and wordy and could be condensed. The self-assessment felt like completing a research survey. In particular, the wording on the questions relating to the outrage factors needs to be addressed. For example, participants did not like the use of "involuntarily" and "voluntarily".	Reword the questions and simplify the questions where possible.
UoN_CS: The feedback process needs to be explained at the beginning of the self-assessment. Users were disappointed to not receive something (e.g., how well they were doing in terms of their preparedness).	Provide clear information on how the user will receive feedback on the self-assessment once they have completed it before they start answering any questions.
UoN-CS: The participants expected a risk assessment/risk matrix.	At the beginning of the self-assessment, provide detailed information on the content of the self-assessment and the feedback process.
UoN-CS: Explain at the beginning of the self-assessment what is meant by "community". Is a community a neighbourhood or geographically based?	Provide a detailed definition of community at the beginning of the self-assessment. Alternatively, participants suggested that a question could be included asking participants "what is your community"? in order to address who they are filling it in as or on behalf of?
UoN-CS: Participants discussed the use of the term "preventing" vs the term "protecting". Individuals do not feel that they can prevent a terrorist attack. They would prefer the use of being	Examine how the term "preventing" is used in the self-assessment and consider whether this can be replaced with "protecting", "vigilant" and/or "alert".

vigilant and alert. However, another participant commented how “preventing” is the term used by authorities.	
UoN-CS: Provide a description of the emergency kits and the emergency plan in the guidance.	
Organisational feedback report	
Group: Both feedback reports were considered too long. Participants would prefer a one-page summary of recommendations and advice.	Discuss the potential for a one-page feedback report with the TACTIC partners.
Group: Consider including a comparative result in a diagram or a spider web that acts as a quick visual indication of where the user sits in comparison with other organisations.	Discuss this with TACTIC partners based on the feedback from the other case study workshops.
General public’s feedback report	
UoN-CS: Provide a description of the emergency kits and the emergency plan in the feedback report.	Add a description of the recommended content for emergency kits and the emergency plan to the general public’s feedback report.
Categorisation	
Group: The categorisation was viewed as really academic and not accessible for people. Participants would prefer the sentences to be simplified (e.g., replace visualisation with image).	Review the wording of the categorisation and simplify where possible.
Group: There was mixed feedback on the description. Some participants liked the description of the practice at the beginning so that they could decide whether they wanted to keep reading, while others thought that it should be moved to the bottom due to its length.	Review in line with the feedback from the other TACTIC workshops.

Group: The content could be reduced as empty sentences are used.	Review the sentences and take out any redundant content.
Group: Include information on the target audience on the left hand side of the document.	
Group: Several participants commented on who determines what a good practice is. The participants found the idea of a good practice difficult to accept and commented that the use of good practice is risky. For example, good practice varies from common practices. In the case of earthquakes, an expert would say to climb on the roof terrace during an earthquake but common practice is to run from the building.	Participants suggested the use of “idea bank” or “guidance”. They enquired about whether the guidance can be given a rating.
Group: Include information on the TOSAP on whether the practice goes through a committee.	
Group: Include more links to other practices in terms of increasing the diversity of the document.	
Group: Include examples of use. For instance, that a practice has been handed out at a community event.	