TACTIC

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

Workshop 1, Case study Terrorism in Europe

Susan Anson, Hayley Watson, Kush Wadhwa

Trilateral Research & Consulting

Document information

Title	TACTIC REPORT ON WORKSHOP 1, CASE STUDY TERRORISM IN EUROPE
Lead Authors	Susan Anson, Hayley Watson, Kush Wadhwa (Trilateral Research & Consulting)
Contributors	
Distribution	Public
Document Reference	D4.1

Document history

Date	Revision	Prepared by	Organisation	Approved by	Notes
13.03.2015	Version 1	Su Anson Hayley Watson Kush Wadhwa	TRI		
16.03.2015	Version 1.1	Hayley Watson	TRI		
20.03.2015	Version 1.2	Doug Weeks	London Metropolitan University		External review
20.03.2015	Version 1.3	Chloe Begg Annemarie Müller	Helmholtz Centre for Environmental Research		Internal review
31.03.2015	Version 1.4	Su Anson Hayley Watson	TRI		

Acknowledgement

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

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 1, case study on terrorism in Europe.

Contact persons for D4.1:

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

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 report addresses preparedness for a particular type of disaster, terrorism, and provides a case study on effective community preparedness towards an act of terror. Terrorism is a useful case study as it enables the consideration of community preparation that would need to engage with a low-probability, complex and unpredictable situation, where critical infrastructure could be attacked from multiple angles, possibly resulting in a cross-border crisis with cascading effects. This report enables an understanding to be gained on how terrorism is different to other disasters, and what these differences mean for preparedness. The report draws upon the literature, reports and legislation, in addition to data collected during workshop 1, from interviews with workshop participants and during a community preparedness engagement meeting hosted by London Resilience Team in February 2015.

This report is structured into three key chapters. The first chapter introduces terrorism and its changing nature related to the emergence of the Islamic State of Iraq and Syria (ISIS) and the small-scale attacks that took place in early 2015. An analysis of the characteristics of terrorism including its intentionality, high uncertainty, unpredictably, low probability, high complexity and intention to induce fear are examined to understand the implications of these characteristics on community preparedness. However, although terrorism can be considered as just another hazard that may be prepared for as part of a multi-hazard (i.e., generic) approach to preparedness, the characteristics of terrorism mean that preparedness for terrorism is more complex and multi-faceted than for other types of disaster. For terrorism, the focus is predominantly on organisational preparedness with a request for the public's assistance in preventing terrorist attacks through vigilance. An analysis of past terrorist attacks is undertaken to understand the different types of scenario that communities may need to be prepared for and to understand communities' communications needs before, during and after a terrorist attack. The commonalities of these attacks (e.g., multiple co-ordinated attacks, attacks on or using public transportation, the public being part of the response) are used to develop a scenario outlined in Section 3.1 that was the focus of workshop 1. The first chapter concludes with a needs assessment indicating the types of activities and capacities required to deal with a terrorist attack at each stage of the disaster risk management cycle and an examination of the different elements that need to be considered by organisations and communities in preparing for and responding to terrorism.

The second chapter focuses on mapping the networks (actors and relationships), governance structures (laws, roles and responsibilities) and learning needs that exist within London, the case study area. Whilst communities perceive terrorism to be a top risk to London, institutional actors conducting risk assessments consider terrorism to be a lower priority. The laws, actors and guidance addressing public preparedness in London mean that communities may be prepared indirectly for terrorism through a multi-hazard (i.e., generic) approach to preparedness. However, inconsistencies in the approaches to preparedness across the different London boroughs and the focus on prevention, rather than preparedness, for terrorism may result in different levels of community preparedness for this particular hazard. For London, the term "community" encompasses more than members of the public, and also addresses preparing businesses within the area. Guidance and recommendations are provided by actors to prepare communities (e.g., use two-way communication, reach different groups of the public). However, London's diverse population means

that there are complex learning needs that need to be considered when communicating with communities before, during and after a terrorist attack.

The third and final chapter of this report focuses on the outcomes of workshop 1 and participants' feedback and recommendations for the community preparedness audit, the categorisation of good practices and the TACTIC Online Training and Audit Platform (TOTAP). The workshop findings indicate that terrorism is different to other types of disaster and this has implications on the advice you can give to communities on preparedness and the division of responsibility between organisations and communities. Whilst the workshop participants considered the audit, good practices categorisation and TOTAP to be beneficial, feedback focused predominantly on enhancing these tools in terms of; defining their users, making structural and content changes and providing the benefits of using the tools. Participant feedback will be considered, in conjunction with the feedback from the other three case study workshops, to develop the tools before the second workshop on terrorism in Europe in October 2015.

1. Introduction

As highlighted in Deliverable 1.1 (D1.1), definitions of preparedness encompass 'readiness' or 'the state of being prepared' (Shreve et al., 2014). TACTIC has adopted the UN's Office for Disaster Risk Reduction (UNISDR) definition of preparedness as:

> "The knowledge and capacities developed by governments, professional response and recovery organizations, communities and individuals to effectively anticipate, respond to, and recover from, the impact of likely, imminent or current hazard events or conditions." (UNISDR, 2007).

This report examines a case study on effective community preparedness towards an act of terror. It is increasingly recognised that terrorism is a global threat that needs to be prepared for (Lemyre et al., 2006). The impacts of terrorist attacks in recent years, including September 11 (2001) and the bombings in Madrid (2004), London (2005) and Boston (2013), highlight why there is a need for communities to be prepared to respond to future attacks. For instance, nearly 3,000 people from over eighty countries were killed in the 9/11 terrorist attacks (Hoffman, 2006). In Europe, the bombing attacks on the transportation networks of Madrid (2004) and London (2005) resulted in the deaths of 191 people in Madrid and 52 people in London and hundreds of people wounded in both attacks (Hoffman, 2006). In addition to the immediate impacts of terrorism, there are also long-term and far-reaching consequences, including but not limited to, the psychological, social, emotional, economic and behavioural impacts (Lemyre et al., 2005). "To date, the psychological, social, emotional, and behavioural aspects of terrorism have not been fully integrated into preparedness and planning efforts" (Ibid. p.317). The recent emergence of the Islamic State of Iraq and Syria (ISIS) is resulting in a change in the nature of terrorism. In comparison to the larger scale terrorist attacks of 9/11 and the Madrid and London bombings, ISIS have called upon their Western followers to conduct small-scale attacks on the police, soldiers and citizens (Levine and Margolin, 2015). Responding to these calls, in the beginning of 2015, attacks took place in Paris, Brussels, Copenhagen and Tunis (Khindria and Meyers-Belkin, 2015).

The benefits of preparedness are highlighted by Ingleby (2014), in a document covering communication with the public, which outlines how "promoting public awareness and preparedness activity may help reduce the stress to individuals associated with being caught up in a major incident, and assist emergency responders by ensuring responders only have to focus on assisting the most vulnerable in an emergency" (p.18). The public can prepare for all hazards, including terrorism, by (for instance) storing useful resources (e.g., food, water, battery operated radio), by making a family plan for responding to the hazard and by informing themselves of local and regional emergency plans (Redlener and Berman, 2006). Whilst the importance of preventing future terrorist attacks is also recognised, this is not the main focus of TACTIC. Rather, the focus of TACTIC and therefore this report is on the elements of preparedness that are key to ensuring community preparedness for multi-hazards.

This report examines community preparedness for terrorism in order to understand how terrorism is different to other disasters, and what these differences mean for preparedness. First we will introduce terrorism, its unique characteristics and what these characteristics mean for preparedness, before moving on to examine real-life hazard scenarios associated with terrorism and cyberterrorism. Once an understanding of preparedness for terrorism has been gained, we will map the networks (actors and relationships) and governance structures (law, roles and responsibilities, etc.) that exist within London, the case study area. The final section will focus on the first workshop that was held on terrorism in Europe and participant's feedback and recommendations related to the community preparedness audit, the categorisation of good practices and the TACTIC Online Training and Audit Platform (TOTAP). Please note, this report is longer than others due to the need to fully understand the complexities surrounding preparedness for terrorism.

1.1. Understanding terrorism relative to other types of hazards

As outlined in D1.1, despite the long history of terrorism, the meaning and nature of terrorism has frequently changed resulting in a lack of a widely accepted definition (Hoffman, 2006). This difficulty in defining terrorism is related to the media's frequent use of the term to refer to a wide variety of violent acts. This report draws upon the definition of terrorism adopted in D1.1 (Shreve et al., 2014), as "the calculated use of intimidation, coercion, direct violent action or the engenderment of fear to attain goals that are political, religious, or ideological in nature" (United States National Research Council, 2002). For the victims of terrorism, the violence appears to be random (Rodin, 2004).

Recent changes in the nature of terrorism include the emergence of a 'new' type of terrorism in the 1970s, characterised by terrorists increased interest in the use of chemical, biological, radiological and nuclear (CBRN) weapons (Cole, 2011). The 1990s saw terrorist violence become increasingly lethal and an increase in "religious" terrorism whereby the objective of an attack was seen as a combination of political and religious motivations (Cole, 2011). The terrorist attacks of September 11th, 2001 (9/11), on the United States of America were also significant in terms of the changing nature of terrorism. They represented the world formally entering "the era of mass destruction terrorism" (Cole, 2011). Whilst terrorists of the 1970s-1990s were concerned with having a large audience rather than a high death toll, contemporary terrorism is characterised by having both a large audience and a high death toll (i.e., mass casualties) (Barnard-Wills and Moore, 2010). However, whilst there is an established history of research examining preparedness for natural hazards, research investigating preparedness for terrorism is more recent having increased following 9/11 (Kano et al., 2011). As outlined in D1.1, the nature of terrorism is also predicted to change in the future with a UK Ministry of Defence report published in April 2014 highlighting how terrorism in the next 30 years could involve cyber-attacks, the use of robots and fatal viruses as weapons and increased female participation.

It is important to compare terrorism to other types of hazards in order to determine what makes terrorism a unique risk and subsequently, to identify the particular challenges that will need to be addressed in order to increase community preparedness to terrorism. An overview of the characteristics of terrorism is provided in Table 1. More detailed information on these characteristics is available in D1.1.

Table 1 Characteristics of terrorism

Characteristic of terrorism	What this means
Intentional human activity (FEMA, 2003) 9/11 and the subsequent anthrax attacks illustrated how a handful of individuals could significantly disrupt the United States of America (Slovic, 2002)	• Not only is public safety threatened by future acts of terrorism, but attacks on buildings, critical infrastructure and cyber space will impact upon communities indirectly

High uncertainty (i.e., limited or absent knowledge) in terms of the likelihood and consequences of a terrorist attack (Kunreuther, 2002) **Terrorist attacks are designed to be unpredictable** (Alexander, 2003)	• It is difficult to prepare for future terrorist attacks when "we do not know who the perpetrators are, what their motivations are, the nature of their next attack, or where it will be delivered" (Kunreuther, 2002, p.662). • Whilst natural hazards also involve a degree of uncertainty, the data and modelling that can be undertaken for this type of risk enables organisations to more effectively predict when natural hazards will occur and their consequences. Thus, the uncertainty and unpredictability associated with terrorism makes planning and preparing for this type of risk more difficult than preparing for natural hazards.
Low probability In the past, terrorist attacks have been less likely to occur than natural or technological disasters (McEntire, 2007)	• The public may not prepare for terrorism as they believe an attack is unlikely to occur, despite the high consequences of an attack
High complexity The causal chain for terrorism may also be more complex than for other types of disaster (Alexander, 2003).	
The intention to induce fear The fear created by terrorism is argued to be more persistent and intense in creating psychological conditions than other types of disaster due to the characteristics of terrorism, including (Bongar et al., 2007): the human intention to cause harm the unknown threat the difficulty in creating expectations of the incident and that the attack could happen anywhere (i.e., it is ubiquitous) Particular types of terrorism (e.g., suicide terrorism and terrorism involving weapons of mass destruction (WMD) are argued to create the greatest levels of fear in the terrorist' target audience (Hoffman, 2006) As examined in D1.1, the level of fear generated by terrorism may be a result of the way in which terrorism has been communicated by the media in recent years. For instance, a qualitative content analysis of newspaper coverage before and after 9/11 found a significant increase in articles linking fear with terrorism following 9/11 (Altheide, 2006)	• As examined in D1.1, fear of future terrorist attacks has been found to vary based on the characteristics of an individual such as ethnicity, education, income, gender and having observed terrorism (Page et al., 2008; Boscarino et al., 2003; Nellis, 2009; Lerner et al., 2003; Braithwaite, 2013). This suggests that different approaches are required to communicate with and prepare different groups of the public for terrorism • Counter-terrorism policies should educate and reassure the public about the real risk of terrorism (Braithwaite, 2013) • Organisations responsible for managing the risk of terrorism are recommended to "enhance transparency and dialogue, as well as engage the public as an active partner in terrorism risk management" (Lemyre et al., 2006, p.757) • In order to prepare for the psychological impacts of a CBRN attack, Lemyre et al. (2005) recommends: • Integrating psychological elements into emergency preparedness planning within the community • Developing a risk communication strategy • Educating communities concerning emergency preparedness • Building support networks that increase community resilience

Whilst Table 1 examines the unique characteristics of terrorism, it could be argued that terrorism is another type of hazard that should be mitigated and prepared for, responded to and recovered from in similar ways to other hazards. This issue is raised by Stewart et al. (2006, p. 119) who outline how "terrorism may be viewed as simply another hazard that, in principle, should be assessed and treated similarly to other hazards" (i.e., an all hazards approach). For instance, Perry and Lindell (2003) highlight "generic functions" undertaken in the management of disasters that are also required during terrorist incidents, including communications (p.348). The need for organisations to consider planning and communications whether they are preparing for a natural hazard or a terrorist attack suggests that there are similarities in at least organisational preparedness for the different types of risk. A number of parallels have been made between the impacts of the September 11th terrorist attacks and an earthquake in Lisbon in 1755 (Alexander, 2002). Both disasters occurred in commercial cities, involved multiple events and resulted in the collapse of solid buildings. The similar consequences resulting from the different types of risk further supports that terrorism can be treated similar to other types of risk. However, unique aspects of terrorism have been identified, such as the nature of mitigation and the issues that need to be considered associated with law-enforcement (Perry and Lindell, 2003).

Whilst there are aspects of planning and preparedness that are unique to specific types of hazard, there are actions that can be taken to increase preparedness for any hazard (i.e., a multi-hazard approach to preparedness) (Office of Public Health Preparedness and Response, 2014). For example, the Centers for Disease Control and Prevention website outlines how the public can prepare for different types of emergency (e.g., natural disasters, terrorism or outbreak of disease) by creating an emergency supply kit, making a family plan for responding to a disaster and by being informed of the different emergencies that are likely in an area and how each emergency should be responded to (CDC, 2014). Adopting a multi-hazard approach to preparedness means that by undertaking the generic preparedness actions, the public are also preparing themselves for terrorism. Acknowledging terrorism as a hazard that should be prepared for is key within this multi-hazard approach to preparedness. However, there are also unique characteristics of terrorism that may require attention to also be placed on preventing future terrorist attacks. This area will be discussed further in the following sections.

1.2. Preparing for terrorism

Emergency management organisations typically have the responsibility for preparing themselves and the public to respond to different types of incidents, including terrorism. Somers and Svara (2009) outline how "[p]rofessional local managers have a responsibility to ensure that their communities are prepared for any kind of disaster – natural or man-made. They must seek to identify and prepare for all risks…" (p.189). As both organisations and the public will need to respond to future terrorist attacks, and the public are the likely target of an attack, it is important that communities are prepared to respond (Bullock, Haddow and Coppola, 2013). This section will first briefly focus on organisational preparedness for terrorism before moving on to examine how governments and organisations communicate the risk of terrorism to the public. Whilst government authorities are typically responsible for communicating risk information to the public, the term organisations is used to represent the wide variety of institutions that are required to prepare for the different elements of a terrorist attack (i.e., handling intelligence, decontamination, psychological issues).

1.2.1. Organisational Preparedness for Terrorism

Participant feedback from workshop 1 highlighted that whilst community preparedness for terrorism may be low, communities rely on organisations and experts (e.g., airports) to be prepared. This suggests that for terrorism, the responsibility for preparedness is being transferred from communities to organisations and that the two are therefore intrinsically linked.

Planning how best to respond to a terrorist attack is typically undertaken at a national and regional level, despite it being the local level that will primarily respond to the terrorist attack (Alexander, 2003). Whilst areas (e.g., London) that have been the target of terrorist attacks are likely to prepare for future attacks, Coaffee et al. (2008) highlight how many local authorities in the UK may be under-prepared for a terrorist attack, as they are not preparing themselves as they do not consider their area to be at risk of terrorism. The high uncertainty and low probability characterising terrorism may mean that local authorities prefer to focus on known risks that have a higher probability of occurring such as flooding, severe weather, pandemics and industrial accidents. Local authorities not preparing themselves for terrorism may also result in communities not being prepared specifically for terrorism. However, as Chapter 2 illustrates, communities may be being prepared for terrorism indirectly through a multi-hazard approach to preparedness.

Organisational planning and preparedness for terrorist attacks may include exercises involving public participation. For instance, during September 2003, an exercise responding to a chemical attack took place on the London Underground enabling organisations (e.g., London Fire Brigade, London Ambulance Service and University College Hospital) to test their plans (Muir, 2003). The exercise was designed to test "the procedures for mass decontamination in the event of a chemical, biological, radiological or nuclear attack" (Muir, 2003). Following the exercise, the Fire Brigades' Union criticised the conditions of the exercise for being very controlled as the cadets acting as victims had been fully briefed. In a real life terrorist attack, the public would not initially be aware of the nature of the incident.

Additionally, organisations are suggested to have increased their surveillance of the public due to the specific threat of terrorism (Coaffee et al., 2008; Mythen and Walklate, 2006, 2008; Aradau and Munster, 2007). Terrorist activity and an increase in crime levels in the UK in the 1990s is suggested to have resulted in an intensification of the "surveillance approach" (Coaffee et al., 2008). This includes both external forms of observation (government agencies observing various public activities) and a more inward type of surveillance (encouraging the public to report potential terrorist activities) (Mythen and Walklate, 2006). This inward surveillance will be discussed further in the next section.

It is also important to note that for organisations, preparedness is only one element of countering terrorism. For example, CONTEST, the UK's strategy for countering terrorism, includes four main workstreams: pursue, prevent, protect and prepare (HM Government, 2013). Thus, organisations not only have to prepare themselves for terrorism but also have to stop terrorist attacks from occurring, prevent individuals from becoming terrorists and increase protective security (e.g., by increasing the resilience of infrastructure).

1.2.2. Public preparedness for terrorism

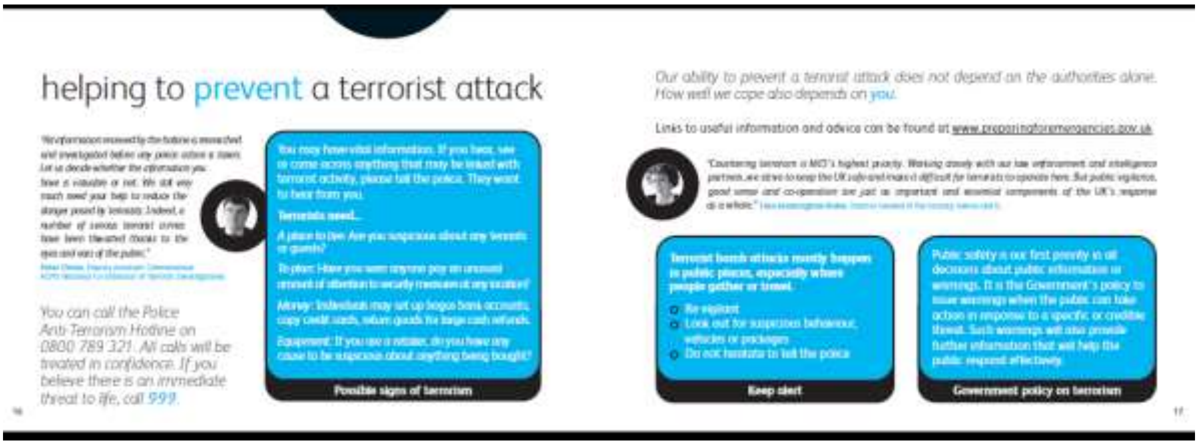
Emergency management organisations are also responsible for preparing the public for different risks. Organisational approaches to public preparedness typically involve education and the communication of preparedness information (Twigg, 2004). For terrorism, this approach is particularly challenging as organisations need to ensure that they do not share information that could assist terrorist groups in threatening national security (Mythen and Walklate, 2006). This sub-section will examine how public preparedness for terrorism can be conceptualised differently to preparedness for other types of risk due to the focus placed on prevention, vigilance and exposure reduction actions. It will also show how research has typically identified low levels of public preparedness for terrorism.

As outlined in D1.1, in 2004, the UK Government distributed the “Preparing for Emergencies: What You Need to Know” booklet to every household. The content included general advice on what to do during an emergency (e.g., ensuring that 999 is called, checking for injuries) and advice for coping with specific emergencies (e.g., chemical, biological or radiological (CBR) incidents) (HM Government, 2004). The booklet also focused on how the public could prepare themselves for an emergency by:

- Identifying where and how to turn off the water, gas and electricity at home
- Identifying the emergency procedures at work and for children at school
- Making a plan for how the family will remain in contact during an emergency
- Identifying vulnerable neighbours that may need support
- Finding out how they tune into their local radio station
- Knowing the items to gather in an emergency (e.g., useful telephone numbers, medication, a battery radio, first aid kit)
- Having useful items ready in case of an emergency (e.g., bottled water, tinned food)

Whilst the booklet was designed to cover general emergency preparedness, the media and political attention focused on the content relating to terrorism (Kearon, Mythen and Walklate, 2007). For example, on the day of its launch, the Guardian featured an article promoting the booklet with the headline; “Terrorism: advice for every household” (Barkham, 2004). Two pages of the booklet (**Error! Reference source not found.**) were dedicated exclusively to preventing a terrorist attack and references to bombs and chemical, biological and radiological incidents were also made (HM Government, 2004). The advice given to the public to help prevent a terrorist attack included:

- Being vigilant
- Reporting anything that could be linked to terrorist activity to the police. The leaflet includes information on the possible signs of terrorism (people paying unusual amounts of attention to security measures, setting up bogus bank accounts)
- Looking out for suspicious behaviour, packages or vehicles



helping to prevent a terrorist attack

"All information received by the hotline is researched and investigated before any police action is taken. Let us decide whether the information you have is valuable or not. We still very much need your help to reduce the danger posed by terrorists. Indeed, a number of serious terrorist crimes have been thwarted thanks to the eyes and ears of the public."
[illegible]

You can call the Police Anti-Terrorism Hotline on 0800 789 321. All calls will be treated in confidence. If you believe there is an immediate threat to life, call 999.

You may have vital information. If you hear, see or come across anything that may be linked with terrorist activity, please tell the police. They want to hear from you.

Terrorists need...

A place to live: Are you suspicious about any tenants or guests?

To plan: Have you seen anyone pay an unusual amount of attention to security measures at any location?

Money: Individuals may set up bogus bank accounts, copy credit cards, return goods for large cash refunds.

Equipment: If you are a retailer, do you have any cause to be suspicious about anything being bought?

Possible signs of terrorism

Our ability to prevent a terrorist attack does not depend on the authorities alone. How well we cope also depends on you.

Links to useful information and advice can be found at www.preparingforemergencies.gov.uk

"Countering terrorism is MI5's highest priority. Working closely with our law enforcement and intelligence partners, we strive to keep the UK safe and make it difficult for terrorists to operate here. But public vigilance, good sense and co-operation are just as important and essential components of the UK's response as a whole." [illegible]

Terrorist bomb attacks mostly happen in public places, especially where people gather or travel.

- Be vigilant
- Look out for suspicious behaviour, vehicles or packages
- Do not hesitate to tell the police

Keep alert

Public safety is our first priority in all decisions about public information or warnings. It is the Government's policy to issue warnings when the public can take action in response to a specific or credible threat. Such warnings will also provide further information that will help the public respond effectively.

Government policy on terrorism

Figure 1 Pages from the Preparing for Emergencies booklet

Kearon et al. (2007) conducted research on the public’s perceptions of the booklet related to its focus on terrorism, the public’s perceptions of the effectiveness of the UK government’s strategy for communicating the risk of terrorism and the public’s concern about the risk of terrorism in the UK. Their findings highlight the challenges associated with preparing the public for terrorism as 34% of respondents reported feeling more at risk after reading the booklet. This was because respondent's believed that the Government had communicated with the public because they had knowledge of a future terrorist attack. The findings also suggest that the UK Government may not be the best source of information concerning terrorism as only 19% of respondents believed that the Government's strategy for communicating about the risk of terrorism had been effective and 66% indicated that they did not trust government communications about terrorism (Kearon et al. 2007). The reasons for the public distrusting government communications on terrorism were related to previous government communications (e.g., on Iraq and its WMD) lacking credibility and the perception that government manipulates information and "spins" the facts. Gender, age and ethnicity were all found to impact upon how the booklet was interpreted with Kearon et al. (2007) outlining how "the diverse responses to emergency advice among our sample demonstrate that a "one size fits" all approach to communicating the terrorist risk should not be the sole strategy implemented by a government wishing to raise awareness of national security issues" (p.93). Instead, they recommend the use of different types of interactive communication, "including workshops, public meetings and citizens' panels" to increase the public's trust and encourage their co-operation (p.93). The booklet is said to be part of a UK government strategy designed to responsibilize the public to manage their own risks (Kearon et al., 2007). However, critically, the booklet did not have a significant impact on preparedness behaviours, as 68% of respondents did not undertake any of the preparedness actions outlined in the booklet (Kearon et al., 2007).

Following the bombings in Bali in October 2002, which resulted in the deaths of 202 people (88 of which were Australian), the Australian Government launched a 'National Security Public Information Campaign' focussing specifically on terrorism (Mcdonald, 2005). The campaign included television advertisements and an anti-terrorism kit including a "Let's Look out for Australia" booklet which was sent to all Australian homes (Mcdonald, 2005). Instead of focusing on preparedness, the booklet outlined how the public could prevent terrorism by identifying suspicious activity (Mcdonald, 2005). The anti-terrorism kit also included a fridge magnet including the number for a 24-hour hotline to report suspicious activity, a list of suggested items to store in case of an emergency (e.g., food, drink, battery-powered radio) and a letter from the Prime Minister (BBC, 2003). However, the campaign was criticised for predominantly being concerned with justifying the introduction of new anti-terror legislation (Mcdonald, 2005). A national campaign calling on the public to return the kits, as they were a form of 'propaganda', resulted in approximately 100,000 kits being returned in one month to Australia's largest mail centre (Mcdonald, 2005).

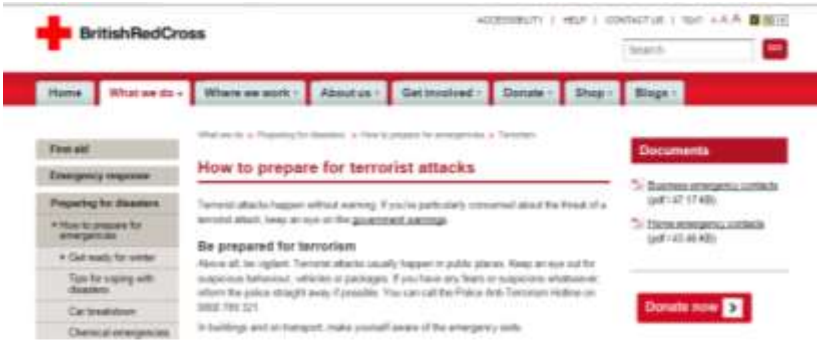
Thus, for terrorism, the focus of government communication strategies is not only on encouraging the public to undertake preparedness actions but is predominantly on requesting the public's assistance in preventing terrorist attacks through vigilance. This suggests that community preparedness is more complex and multi-faceted for terrorism than it is for other types of hazard.

The counter-terrorism week launched nationally by the UK police on the 24th November 2014 (as this report was being written,) demonstrates the focus on prevention (City of London Police, 2014). The campaign was the largest ever to focus on alerting the public of the risk of terrorism and involved 6,000 police officers across Britain (Morris, 2014). Crowded places (e.g., railway stations, airports) were patrolled and advice on strengthening their security measures was provided to staff at shopping centres, cinemas and sports stadiums (Morris, 2014). The week focused on encouraging the public to be vigilant and informing them of “simple measures they can take to make it harder for terrorists to attack the UK” (City of London Police, 2014). Five key areas for preventing terrorism were addressed, including:

1. Crowded places (Monday 24 November) – terrorists typically target crowded places and the City of London Police highlighted the role of businesses in spotting the first signs that something is wrong
2. Transport hubs (Tuesday 25 November) – as Section 1.3 shows past terrorist attacks have targeted transport hubs. The City of London Police requested that the public be vigilant and report any suspected threats
3. Preventing violent extremism (Wednesday 26 November) – A request was made for “parents, carers, friends and colleagues to be alert to the signs of extremism” (City of London Police, 2014)
4. Terrorist financing (Thursday 27 November) – The City of London Police highlighted how the public should use registered charities to make donations as terrorists can pose as charity fundraisers
5. Terrorist tools (Friday 28 November) – The public were provided with information on the tools terrorist use in attacks and how different tools are regulated (e.g., EU legislation requiring a permit to purchase particular chemicals)

The National Policing Lead for Counter-Terrorism, Assistant Commissioner Mark Rowley was “keen to stress that we can all be doing more to ‘protect’ and ‘prepare’ – ensuring security in crowded places, monitoring out borders and being ready to respond to a terrorist attack” (Mayor’s Office for Policing and Crime, 2015b). However, the campaign was criticised for potentially being used as a cover up for removing civil liberties by retaining more data on each member of the public (Morris, 2014)

A review of approaches communicating information on terrorism to the public further supports how the focus on prevention is more common than campaigns focusing on community preparedness. Approaches to terrorism typically request that the public be vigilant to potential terrorist attacks. For example, the British Red Cross website (**Error! Reference source not found.**) advises that to prepare for terrorism, the public should “above all, be vigilant”.


BritishRedCross
ACCESSIBILITY | HELP | CONTACT US | TEXT A A A
Search
Home
What we do
Where we work
About us
Get involved
Donate
Shop
Blogs
First aid
Emergency response
Preparing for disasters
How to prepare for emergencies
Get ready for winter
Tips for coping with disasters
Car breakdown
Chemical emergencies
What we do > Preparing for disasters > How to prepare for emergencies > Terrorism
Documents
Business emergency contacts (pdf : 47.17 KB)
Home emergency contacts (pdf : 43.46 KB)
Donate now

How to prepare for terrorist attacks

Terrorist attacks happen without warning. If you're particularly concerned about the threat of a terrorist attack, keep an eye on the government warnings.

Be prepared for terrorism

Above all, be vigilant. Terrorist attacks usually happen in public places. Keep an eye out for suspicious behaviour, vehicles or packages. If you have any fears or suspicions whatsoever inform the police straight away if possible. You can call the Police Anti Terrorism Hotline on 0800 789 321.

In buildings and on transport, make yourself aware of the emergency exits.

Figure 2 The UK Red Cross Website

A website[1] by the French Government concerned with preventing major risks also advises the public to remain vigilant to the threat of terrorism. Campaigns such as these that include "an instruction for responsible individuals to remain on the lookout for suspicious activity and to immediately convey relevant information to authorities" are termed "public vigilance campaigns" by Larsen and Piché (2009, p.188). Examples of public vigilance campaigns in New York City, Ottawa and London are discussed by Larsen and Piché (2009). These campaigns requested that the public report any suspicious activity, packages or persons to the authorities and included the "If you see something, say something" campaigns ran by the New York City Metropolitan Transportation Authority and Ottawa's OC Transpo and the "If you suspect it, report it" campaign ran by the Metropolitan Police Service and partners (the British Transport Police, the City of London Police, Transport for London, and the Mayor's Office of London) (Larsen and Piché, 2009). Campaigns such as these suggest to the public that not being vigilant is irresponsible and a risky option (Larsen and Piché, 2009).

A small number of examples were found in the United States of America of communication strategies focusing predominantly on preparedness for terrorism. The US Ready.Gov website focuses on how the public can prepare themselves for different types of terrorist attack, including; biological threats, chemical threats, cyber-attack, explosions, nuclear blast and radiological dispersion device (RDD). With the exception of cyber-attacks, the actions Ready.Gov recommends that the public undertakes to prepare for the different types of terrorist attack include building an "emergency supply kit" and making a "family emergency plan". Items that Ready.Gov recommend that the public include in their emergency kit include "non-perishable food, water, a battery-powered or hand-crank radio, extra flashlights and batteries". Making a family emergency plan is considered important as family members may not be together when the disaster occurs. The public are advised to include information in their plan on:

- How family members will contact each other (e.g. meeting points, telephone numbers)
- The emergency plans of places where the family spends time (e.g. work, school)
- The community's warning systems and plans
- The plans for pets

Tailored preparedness advice is also provided for the different types of terrorist attack. For example, for biological threats, Ready.Gov advises the public to check that their immunisations are up to date and to consider installing a High-Efficiency Particulate Air (HEPA) filter to prevent biological agents from entering their home. The U.S. Centers for Disease Control and Prevention website outlines how the public can prepare for anthrax emergencies. In addition to the advice of creating an emergency kit, plan and staying informed about different types of emergency, the public would "also need to know how to get antibiotics, how to create a family medical history, and how to recognize the symptoms of anthrax" (Centers for Disease Control and Prevention, 2013).

Approaches such as the one by Ready.Gov, are designed to influence the public to undertake actions to prepare themselves to respond to a terrorist attack. However, research based in the United States has found that similar to public preparedness for natural hazards, there are low levels of public preparedness for terrorism. For example, Kano et al. (2011) found that whilst individuals in the

[1] République Française, Prévention des Risques Majeurs, 2012. [Online] http://www.risques.gouv.fr/. (Accessed: 02 December 2014).

United States had become more vigilant following September 11th (83%), only a minority of respondents had stockpiled supplies (34%) and had developed an emergency plan (29.5%). As outlined in D1.1, research by Bourque et al. (2012) found differences in preparedness across gender and income.

The research by Bourque et al. (2012) and Kano et al. (2011) also highlighted a key difference between the impacts of terrorism and natural hazards on the public's behaviour. In response to September 11th, individuals were found to have taken exposure reduction actions. This included individuals avoiding certain cities (19.8%), reducing their plane travel (18.2%), changing how their mail is handled (15.4%) and avoiding tall buildings (10.8%). The public taking exposure reduction actions (e.g., limiting their outside activities and choosing another form of transport) and having low levels of preparedness following September 11th is also supported by research by Torabi and Seo (2004).

1.3. Terrorism: Hazard scenarios

This section provides an overview of the characteristics of past terrorist attacks and the resulting different elements that need to be considered when preparing for, responding to and recovering from a terrorist attack.

Table 2 summarises the characteristics of past terrorist attacks taken from a detailed analysis of past attacks that can be found in Appendix A. Past terrorist attacks were analysed in order to understand the different scenarios that communities may need to be prepared for. This analysis was used to develop the scenario that was the focus of workshop 1 and that is outlined in Section 3.1. However, it is important to acknowledge the limits of developing hazard scenarios for planning and preparing for terrorism. The unique characteristics of terrorism examined in Section 1.1, means that "planning scenarios to counteract future terrorist outrages usually are contentious… The problem is that terrorism offers too many potential scenarios, and, according to experience, too many discrepancies between the scenarios that have been worked out and the reality on the ground" (Alexander, 2003, p. 168). Even when scenarios are used for training, governments and the public could still be overwhelmed by a terrorist attack (Sloan, 2002). Whilst these limits are recognised, the past attacks examined in Table 2 and Appendix A provide lessons for planning, preparing and communicating about terrorism that were discussed during workshop 1.

Characteristics Past terrorist attacks	Type of attack	Timing of the attacks	Multiple attacks	Fatalities (F) & injuries (I)	Intelligence or previous attacks	Longer term impacts	Prepared or Unprepared	Communication issues before (b), during (d) and/or after (a)	Public part of the response	Evaluation and/or lessons learnt for preparedness
1995 Tokyo subway sarin attacks	Chemical	Morning rush-hour	✓	F – 10 I – 5,000	✓	✓	Unprepared	b, d, a	✓	✓
11th September 2001 attacks in the USA	Plane hijackings	Morning rush-hour	✓	F – 2,981+ I – Thousands	✓	✓	Unprepared	d	✓	✓
2001 anthrax attacks in the USA	Bioterrorist	Over a number of weeks	✓	F - 5 I - 17						✓
2004 Madrid bombings	Bombing attack on the transportation network	Morning rush-hour	✓	F – 191 I – 1,800+	✓		Unprepared		✓	
2005 London bombings	Bombing attack on the transportation network	Morning rush-hour	✓	F – 52 I - 770		✓	Authorities prepared	d	✓	✓
2008 Mumbai terrorist attacks	Bombing and shooting attacks	Lasted four days	✓	F – 166 I – 300+			Unprepared			✓
2011 Anders Brevik attacks	Bombing and shooting attack	Afternoon	✓	F – 77						
2013 Boston Marathon bombings	Bombings	Afternoon		F – 3 I - 264	✓		Prepared		✓	✓

Table 2 An overview of the characteristics of past terrorist attacks

The review of past attacks highlighted the characteristics shared by many of the attacks. These characteristics were used to develop the terrorism scenario that was used in the first workshop to understand preparedness and communities' communication needs before, during and following a terrorist attack. This information will also be used to consider a multi-hazard scenario in the second workshop. The common characteristics of past terrorist attacks identified include;

- **Multiple coordinated attacks** – with the exception of the Boston Marathon bombings (2013), where there was the intention to commit multiple attacks, each act of terrorism included multiple attacks at different locations
- **Attacks on or using transportation** – the attacks in Japan (1995), Madrid (2004), London (2005) and Mumbai (2008) were on or included attacks on the transportation network (e.g., the tube, a bus and a train station). In the USA (2001), planes were used as the weapons to carry out the attacks
- **Attacks carried out at peak times** – the attacks in Japan (1995), USA (2001), Madrid (2004) and London (2005) were all carried out during the morning rush hour when higher numbers of people would be travelling to work and using the transportation network
- **The public being part of the response** – during many of the attacks, the public supported organisations in the response effort (e.g., donating blood, providing information on suspects). Preparing communities for terrorism may enable them to effectively support the official response
- **The importance of communication** – communicating effectively with the public following an attack was considered important. Additionally, communication issues experienced during an attack (e.g., a lack of mobile network) heightened the impact
- **Wider long term impacts** – in addition to the immediate impacts of a terrorist attacks (e.g., fatalities), long term impacts include stress and behaviour change

1.4. The needs assessment

Undertaking Task 4.1 and reviewing the literature to understand terrorism, its unique characteristics and the characteristics of past terrorist attacks enabled Trilateral Research & Consulting to conduct a needs assessment of the types of activities and capacities that are required to deal with a terrorist attack at each stage of the disaster risk management cycle. As

Table 3 illustrates, for terrorism, organisational preparedness involves a wide range of activities to prevent, prepare for, respond to and recover from an attack. However, whilst the participants of workshop 1 suggested that for terrorism the focus may be on organisational preparedness, rather than community preparedness, Table 3 highlights how there are actions communities can undertake to both prevent and prepare for a terrorist attack. Communities undertaking actions such as those outlined in Tables 3 and 4 may support organisational preparedness efforts, highlighting how organisational and community preparedness are interlinked.

In addition, Table 4 highlights the various elements that organisations and communities need to consider in preparing for and responding to terrorism.

Table 3 Needs assessment of the organisational and public activities and capacities required for the different phases of a terrorist attack

	Mitigation/Prevention	Preparedness	Response	Recovery
Organisational	Physical protection of infrastructure	Assessing the capacity to respond at different levels (e.g., organisational, regional)	Initial assessment of the scene to confirm the incident is a terrorist attack Police investigation of the crime scene	Treating PTSD and providing psychological support
	Gathering, acting on and sharing intelligence between different agencies	Multiagency and multidiscipline planning covering the different elements of the response (e.g., information to the public, mass fatality plans)	Tightening security at other potential targets (e.g. airports, ports, train and bus stations, cities) to prevent further attacks	
	Increased security measures (e.g., tighter security at potential high risk targets, CCTV/ high resolution cameras, police patrols, security scanners, sniffer dogs)	The existence of Standard Operating Procedures	Communication with the public (e.g., to provide updates, request help and that the public be vigilant). Establishment of communication centres	
		Training and exercises covering different types of terrorist attack	Response at the scene (e.g., decontamination, creating a field hospital, victim transportation to hospital)	
		Established systems of command and control	Interagency cooperation and communication	
		Communication systems with the capacity to cope with the demand (i.e., do not overload), that are compatible across different response agencies and can work underground	Human resources required for the response – emergency services, psychologists, volunteers	
		Mutual aid agreements	Establishing a morgue and process for identification of victims	
		Sourcing resources and equipment (e.g., decontamination equipment, antibiotics)	Establishing a survivor reception centre	
		Established triage procedures and systems for handling the non-injured		
		Institutional mindset (i.e., motivation) – identification of the need to prepare for terrorism		

	Mitigation/Prevention	Preparedness	Response	Recovery
Communities	Responsibilization campaigns requesting the public to report suspicious activity (i.e., vigilance)	Creating an emergency kit	Providing support and help (e.g., donating blood, information and images to the investigation, helping paramedics)	Returning to normal behaviour (pre-disaster behaviour) e.g., using public transport again
	Avoidance of certain activities	Storing useful resources	Panic and shock (this response is minimal when compared to the public providing support)	
		Making a Family Emergency Plan		
		Informing themselves of likely emergencies and how to respond (e.g., identifying evacuation exits)		
		Taking responsibility for their own preparedness		
		Psychological preparedness		

Table 4 Elements for organisations and communities to consider to prepare for and respond to terrorism

Elements to consider to respond and prepare against terrorism	Description & Examples
Related to communities	
Communications related to preparedness	Campaigns requesting the public to prepare by storing resources (e.g., creating an emergency kit) and developing a family emergency plan
Communications related to prevention and public vigilance	Campaigns requesting the public to be vigilant and assist authorities in preventing terrorist activities by reporting suspicious activity (e.g., suspicious packages)
Community engagement	To prevent radicalisation
Fear-arousing nature of terrorism	Communicating with the public about terrorism may heighten their levels of fear and result in anxiety. Thus, it is important for organisations to explain to communities why they are communicating with them concerning terrorism
Diversity of the population	Tailored approaches are required to prepare different groups of the public
Public involvement in the response	Providing help and support to responding agencies Providing information and evidence to criminal investigators (e.g., phone images) Donating blood
Recovery and the return to normal	Identifying ways to limit the influence of terrorist attacks on public behaviour
Related to Organisations	
Multi-agency planning and cooperation	The different responding agencies will need to establish procedures for working together during the response to a terrorist attack
Training and exercises	International learning and exercises for terrorism
Roles and responsibilities	Identification of the organisations that may be involved in the response (e.g., police, fire, healthcare, transportation, psychologists). Determining the incident response command structure. Presence of standard operating procedures
Intelligence sharing	Between different levels of government and agencies before and during terrorist attacks
Security measures	Technology to prevent and monitor terrorist activity (e.g., biometrics that identify if a person is carrying a bomb, CCTV) Physical protection of infrastructure (e.g. concrete blocks to protect buildings) Heightened security at airports, train, tube and bus stations
Communication	Interoperability between responding agencies Capacity of the cell phone network Difficulty in communicating in particular locations (e.g., underground) Secure radio bandwidth The dissemination of information to the media and public
Resources	Mutual aid agreements between areas Sourcing specialized equipment (e.g., chemical suits, breathing apparatus) The coordinated deployment of resources during the attack
Support for the victims	Psychological services Victim reception and assistance centres
Preservation of the crime scene	Ensuring the crime scene is protected Searching for clues

2. Preparing for terrorism in London - mapping network and learning needs

This section addresses Task 4.2 and examines preparedness for terrorism in London in relation to: the legislation governing emergency preparedness, the actors responsible for preparedness and the potential learning needs that exist within communities. It will highlight London's complex governance structure and the diverse learning needs that exist. The section draws upon literature, reports and legislation, in addition to data collected during workshop 1, interviews with workshop participants and during Trilateral Research & Consulting's participation in a community preparedness engagement meeting hosted by London Resilience Team on 26 February 2015 in London.

2.1. Legislation – The 2004 Civil Contingencies Act

This section first focuses on the CCA as it provides an overview of the networks (i.e., actors and relationships) and governance structures (i.e., laws, roles and responsibilities) related to emergency preparedness in the UK.

The fuel crisis and severe flooding in 2000 and the Foot and Mouth Disease outbreak in 2001 prompted a review of the existing arrangements for emergency planning, which indicated how "existing legislation no longer provided an adequate framework for modern civil protection efforts and that new legislation was needed" (Cabinet Office, 2009). The new legal framework for emergency planning in the UK was established in 2004 in the form of the CCA. The Act updated the existing definition of an emergency to cover modern risks including the threat of terrorism (Cabinet Office, 2009). The CCA (2004) defines an emergency as:

- "an event or situation which threatens serious damage to human welfare;
- an event or situation which threatens serious damage to the environment; or
- war, or terrorism, which threatens serious damage to security" (Cabinet Office, 2009).

There are two parts to the CCA with Part 1 focusing on the roles and responsibilities for civil protection at a local level and Part 2 addressing the emergency powers required to respond to serious emergencies (Cabinet Office, 2013). In terms of roles and responsibilities, the CCA includes two categories of local responder based on the degree of involvement in civil protection activities. Category 1 responders, listed in **Error! Reference source not found.**, are organisations key to the response to an incident (e.g., emergency services, local authorities) and as part of their responsibilities are required to:

- Undertake risk assessments that inform planning
- Create emergency plans
- Establish Business Continuity Management arrangements
- "Put in place arrangements to make information available to the public about civil protection matters and maintain arrangements to warn, inform and advise the public in the event of an emergency"
- Share information and co-operate with other local responders to facilitate co-ordination and efficiency
- Provide businesses and voluntary organisations with advice and assistance covering business continuity management (Cabinet Office, 2013).

The requirement for Category 1 responders to provide the public with information and advice about risks and the planned response to emergencies and to warn the public when an emergency has occurred is "based on the premise that a well-informed public is better able to respond to an emergency and able to help to minimise the impact of an emergency" (Cabinet Office, 2011, p.30). Category 1 responders are reminded of "the need to avoid unnecessary public alarm" but also how research indicates that when the public have insufficient information, they are more likely to be alarmed (Cabinet Office, 2011, p.30). For terrorism in particular, the need to balance the risk of alarming the public with providing sufficient information is key.

However, the data collected by Trilateral Research & Consulting highlighted how the CCA does not necessarily mean that communities will be provided with information specifically about terrorism. An interviewee described the CCA as a "*catch all*", meaning that to fulfil the legal requirement, Category 1 responders could provide the public solely with generic emergency preparedness advice. The data also indicated the potential for inconsistent approaches to community preparedness for terrorism across different areas of London. Whilst some Category 1 responders provide their community with information specifically on preparing for terrorism, others may not. Reviewing the websites of different local authorities across London highlighted the different approaches used.

Category 2 organisations (e.g. transport and utility companies) are "co-operating bodies" who although less likely to be involved heavily in planning, will be heavily involved in the incidents affecting their sector (Cabinet Office, 2013). The CCA legally obligates Category 1 and 2 responders to form 'Local Resilience Forums' designed to facilitate co-ordination and co-operation between local level responders.

"Emergency Preparedness" provides statutory guidance to responders on implementing Part 1 of the CCA, in the form of a series of chapters covering different topics. These chapters are relevant to TACTIC and the case study focusing on preparedness for terrorism in Europe. For example, Chapter 4 of Emergency Preparedness focuses on "local responder risk assessment duty" and, related to terrorism, outlines how Counter Terrorism Security Advisors (CTSAs) can be found in all UK police forces (Cabinet Office, 2012). Their role is to identify 'local critical sites' that would be vulnerable to a terrorist attack and to develop plans to minimise the impact to both the site and the local community. This involves delivering Project Argus, a three hour multimedia simulation designed to raise awareness of the threat of terrorism and that provides advice on preventing, responding to and recovering from an attack (City of London Police, 2014). Project Argus is designed for businesses, including the following sectors: office and retail, night time economy, hotels, education, health, designers, planners and architects. Thus, it is not only the public in London that are being prepared for terrorism, but also businesses operating within the community.

Another chapter of Emergency Preparedness that is highly relevant to TACTIC is Chapter 7 on "Communicating with the Public". This chapter includes guidance for local responders on informing the public about terrorism:

> "Information relating to events, particularly terrorist events, where the consequences would include mass fatalities and casualties could be unsettling and upsetting. However, there is a clear need to strike a balance between not causing public alarm and providing necessary information to enable people to understand the threat and respond in an appropriate

> manner in the event of an incident occurring. There is no evidence to suggest the public panics when receiving information. They want to feel they have the relevant facts so that they can take informed decisions. Communication needs to be handled sensitively. Responders should use clear terminology, providing factual information which avoids sensationalism or emotive language. The content should not be overly negative or graphic, and should be as brief as possible to avoid confusing or overwhelming readers" (Cabinet Office, 2012).

The CCA provides context to the next section, focusing in more detail on the actors who are responsible for planning, preparing for, responding to and recovering from emergencies in London. Whilst these actors had responsibilities prior to the 2004 CCA, the CCA legally enforced these roles and responsibilities.

2.2. London's Emergency Management Actors

As this section demonstrates, the different phases of emergency management in London involves a range of actors and complex governance structures.

Table 5 provides an overview of the different actors with roles and responsibilities related to managing emergencies, including terrorism, in London. Detailed information on these roles and responsibilities is provided in Appendix B.

Examining the legislation governing emergency preparedness and the actors with roles and responsibilities for managing emergencies, highlights how:

- Existing legislation means that communities in London may be prepared indirectly for terrorism through generic (i.e., multi-hazard) approaches to preparedness
- The inconsistency of preparedness strategies across the 33 London boroughs may result in different levels of preparedness for terrorism across different communities in London
- London is characterised by a complex governance structure with a multitude of actors responsible for preparing for, responding to and recovering from emergencies. However, many actors focus on preparedness for multi-hazards, rather than community preparedness specifically for terrorism. It is the Metropolitan Police who holds responsibility for counter-terrorism, however, the focus is on preventing rather than preparing for terrorism
- The focus is not only on preparing members of the public for terrorism, but also businesses that are part of the community
- There is a need to balance the risk of alarming the public with providing sufficient information that enables the public to understand the threat and respond appropriately to an incident
- Responders are advised that communication regarding terrorism should be handled sensitively (e.g., clear terminology, factual information) and should avoid sensationalism, emotive language and being overly negative or graphic

Table 5 Overview of London's Emergency Management Actors and their roles and responsibilities

Organisation/network and key points	Roles and responsibilities
The London Emergency Services Liaison Panel (LESLP) Created 1973 Consists of the Metropolitan Police Service, City of London Police, British Transport Police, the London Fire Brigade, the London Ambulance Service, local authorities, the Port of London Authority (PLA), Marine Coastguard, RAF and Military and voluntary sector	• The various organisations have different roles and responsibilities during the response to an emergency, which are outlined in a Major Incident Procedure Manual discussed in Section 2.3.3
The Metropolitan Police The Counter Terrorism command is known internally as SO15 The Metropolitan Police Service website requests the public's help in preventing, rather than preparing for, terrorism by reporting suspicious activity	• Protecting London and the UK from the threat of terrorism • Preventing the threat of terrorism • Engaging, building and maintaining working relationships with local communities to jointly combat the threat of terrorism. For instance, the Metropolitan Police delivers advice, guidance and briefings to individuals, groups of individuals and large businesses (e.g., the media, councils, football stadiums, banks) on the things that they can do to make themselves more resilient to a terrorist attack • Working with communities to provide advice and tackle extremism • Responsible for the PROTECT strand of CONTEST
London Resilience Team (LRT) Established in early 2002 The 2004 CCA further broadened LRT's responsibilities and work Includes representatives from Local Authorities, the Emergency Services, utility companies and transport organisations LRT was part of the Greater London Authority but was transferred to the London Fire and Emergency Planning Authority (LFEPA), who run the London Fire Brigade in early 2015	• Supporting the role of the London Resilience Partnership in order to make London more resilient • Developing and coordinating multi-agency plans and procedures for responding to an emergency in London • Facilitating London Local Resilience Forum meetings • Acting as a liaison point between the London Resilience Partnership, central government and Local Resilience Forum areas • Raising awareness of risks and internationally promoting preparedness for emergencies • Maintaining and updating the London Prepared web pages and Twitter account
London Resilience Partnership Created in 2002 Coalition of over 170 organisations (Table 15) involved "in preparing, responding and recovering from emergencies in London" (London Resilience	• Assessing the risks to London's resilience and publishing a public version of the London Risk Register[2] • Prevention and mitigation to build resilience • Preparing for, responding to and recovering from emergencies

[2] London Resilience Partnership, London Risk Register, February 2015. [Online]. http://www.london.gov.uk/sites/default/files/London%20Risk%20Register%204.0.pdf. (Accessed 23 March 2015).

Partnership, 2013)	• Communicating with the public to ensure that people who live, work and visit London are aware of the risks in London and how they can prepare for these risks • Increasing social media followers and website visitors • Encouraging communities to prepare • Promoting initiatives designed to increase community resilience • Ensuring that the London business community are risk aware and have developed business continuity plans
Greater London Authority (GLA) Established 2000 Form of government consisting of the Mayor of London, the London Assembly and non-political staff Categorised as a Category 1 responder	• Participating in high-level discussions and decision making relating to managing emergencies in London • Chairing the London Resilience Forum (or appointing a deputy) • Locally and nationally, contributing to the pre-informing of Londoners about emergency plans, the correct behaviour during an emergency and preparedness • Warning and informing the public in London during an emergency • Civil protection issues related to managing Parliament and Trafalgar Squares
Local Resilience Forums 2004 CCA resulted in the creation of 42 Local Resilience Forums across England and Wales	• Developing a Community Risk Register • Addressing policy related to: risk, emergency planning, business continuity management, publishing information on risk assessments and plans, warning and informing the public and other civil protection duties (e.g., promoting business continuity management) • Supporting the preparation of multi-agency plans, protocols and agreements and the co-ordination of multi-agency exercises
London Resilience Forum A pan-London Local Resilience Forum covers all of London and incorporates the Metropolitan Police and City of London Police areas. However, the data highlighted inconsistences in the preparedness strategies across the 33 London boroughs	• Providing strategic high level direction for multi-agency planning in London • Ensuring that London is prepared to respond to a variety of different incidents including terrorist attacks, the impacts of climate change and pandemics • Agreeing strategic and policy approaches concerning London's preparedness and response • Producing and maintaining the London Risk Register • Enabling information on risk management, threats and hazards to be shared across local, sub-national and national organisations • Ensuring that plans, procedures, training and exercises are in place • Improving co-ordination across London • Reviewing and recommending the key members of the Borough Resilience Forums • Approving the Borough Resilience Forums Risk Registers
Borough Resilience Forums For each borough of London, a Borough Resilience Forum meets a minimum of once every six months for more local level planning	• Multi-agency emergency planning based on the local risks and needs

2.3. London's key emergency planning procedures

This section examines the relevant documents and procedures underpinning emergency preparedness in London.

2.3.1. Communicating with the Public Framework

The "Communicating with the Public Framework" was published by the London Resilience Partnership in 2014. "Communicating with the public is a core element of the London Resilience Partnership Strategy, and a capability which is required in all incidents" (Ingleby, 2014, p.4).

Whilst the Framework predominantly provides responders with recommendations for communicating with the public during an incident, the lessons can also be applied to communicate preparedness information. For example, the Framework outlines how diversity within a community can create a barrier to communicating with the public in terms of the various communications needs. Different needs will exist during all stages of an emergency, requiring responders to also implement the recommendations to prepare communities. Areas covered by the framework that can be considered when preparing communities, include (Ingleby, 2014):

- The role of trust in influencing risk perceptions. Factors that influence public trust are argued to include: message source, communications channels trusted by particular audiences, the use of clear language and ensuring consistency across multiple sources of information. The relationship between trust and preparedness was discussed in D1.1
- Communication tools that responders can use to communicate with the public (e.g., press and broadcast media, social and digital media, traditional communication channels)
- How to reach particular groups and networks (e.g., faith groups, volunteer organisations, schools)
- How to communicate with particular groups (e.g. visually impaired, deaf/hard of hearing, older people, non-English speakers, transient population)

The Framework acknowledges the importance of preparedness by outlining how "the public should be given information about local risks, the desired response and the method and style of message prior to the incident to ensure that when they receive a message for an incident they understand the message and respond" (Ingleby, 2014, p.8). Thus, preparedness is important in order for communities to be able to respond effectively when an incident occurs.

Roles and responsibilities for communicating with the public pre-incident and during the response and recovery phases are documented in the Framework. The responsibility of Emergency Planning Officers pre-incident is to work in conjunction with the communications team to provide information and advice to the public on specific risks. The role of the lead responder, pre-incident, is to consider whether specific risk(s) should be communicated to the public, if required to provide the public with information and advice on specific risks, to engage with the public in order to raise awareness, and to inform partners of publicly available information (Ingleby, 2014). The Lead Responder(s) for each risk is outlined, including, but not limited to; Public Health England for human diseases and human health incidents; the Environment Agency for flooding; the Met Office, Public Health England, the Environment Agency, Defra and local authorities for severe weather and DEFRA and local authorities for animal diseases. However, whilst seven pages of risks are included, significantly, the risk of terrorism is not included. Although there are speculative reasons why terrorism may have been excluded (e.g., fear of scaring the public, preferring to focus on organisational, rather than public, preparedness for terrorism), it is the implications of not including terrorism that is significant.

Terrorist attacks are suggested to be a bottom-up incident that affect one or more specific locations (Ingleby, 2014), however, if no one has responsibility or is accountable for communicating pre-incident, local communities affected by terrorism are unlikely to have been prepared in advance to respond to an attack.

During a terrorist attack, or an incident suspected to be a terrorist attack, the Counter Terrorism Command must first authorise information before it can be provided to the news media.

2.3.2. Strategic Coordination Protocol

The Strategic Coordination Protocol "details the escalating strategic coordination arrangements for London's response to a disruptive incident (Brown, 2014, p.10). The Protocol covers the procedures for responding to an incident from notifying the London Resilience Team Duty Officer of the incident to the strategy for responding to and recovering from the incident. There are eight guiding principles of the Protocol, of which three are relevant to TACTIC (Brown, 2014):

- **Preparedness –** All individuals and organisations that might need to respond to an emergency should be prepared. This includes having clear roles and responsibilities, both generic and specific plans and regularly rehearsing the response
- **Communication –** Two-way communication, including with the public, is viewed as critical to the response. Advice for organisations to prepare their communications with the public during the response includes: managing public expectations of what responders will be able to do and when, holding public meetings and press conferences and using and monitoring what is being said in all forms of media, including social media. During an emergency, the Mayor of London acts as the 'voice of London' providing the public with clear information and guidance (Brown, 2014, p.25).
- **Anticipation –** Planners should identify risks and understand the direct and indirect consequences. As examined in Section 1.1, the uncertainty associated with terrorism makes understanding the consequences more difficult

Whilst the Strategic Coordination Protocol focuses on response, it enables individuals and organisations to prepare themselves to effectively respond to an incident and to prepare their communications with the public.

2.3.3. The LESLP Major Incident Procedure Manual

As LESLP was discussed in Table 5 and Appendix B, this section will briefly focus on the LESLP Major Incident Procedure Manual which summarises the responsibilities and responses of the emergency services at a major incident and the supporting role that local authorities have (LESLP, 2012). Concerning terrorism, the manual outlines how "[t]he threat from a CBRN device is significant, not only as a result of its activation but also in the fear and panic that it would create within the public and media and the considerable resources that would be required in the decontamination and restoration to normality following such an attack" (LESLP, 2012, p.64). Terrorist attacks and suspected CBRN attacks require a specific multi-agency response that is supported by the Government (LESLP, 2012). For example, during a CBRN attack, the London Ambulance Service and London Fire Brigade have extra responsibilities related to decontamination. Thus, there are a wide range of roles and responsibilities related to terrorism.

The LESLP Manual also covers liaising with the media and providing the public with information during an incident. The media and social networking sites are recommended as tools for communicating advice to the public about the incident and the actions they should take. When a major incident occurs in London, a Gold Communication Group is established, as occurred during the 7/7 bombings. This group should include the heads of communication from the emergency services and other agencies involved. During 7/7, the Gold Communication Group included "senior representatives from the Met, TfL, the Mayor's office, the Association of London Government and the emergency services" (PR Week, 2005). This group has responsibility for managing and coordinating media and communication issues.

The interviews with workshop participants highlighted how LESLP is being succeeded by the Joint Emergency Services Interoperability Principles (JESIP). JESIP "aims to improve the ways in which police, fire and ambulance services work together at major and complex incidents" (JESIP, n.d.). JESIP has only been briefly mentioned here as it is not directly related to TACTIC.

2.3.4. Key points summarised from London's key emergency planning documents and procedures

- Public preparedness is important in terms of people understanding the message and responding appropriately when there is an incident
- Guidance enables actors and organisations to prepare their communications with the public ready for when an incident occurs
- Two-way communication with the public is critical
- There are different factors to consider when communicating with communities (e.g., the influence of trust on risk perceptions, the different communication tools that can be used, how to reach particular networks and communicating with groups of the public with different communication needs)
- Not addressing the risk of terrorism in documents may result in communities not being prepared to respond to future terrorist attacks
- There is a need to consider the fear and panic an act of terrorism may generate in the public and media
- For terrorism, actors have additional responsibilities in addition to communicating with communities (e.g., decontamination)

2.4. The London Risk Register

As outlined in Section 2.1, the 2004 CCA requires Category 1 responders to conduct a risk assessment and to arrange for all or parts of the risk assessment to be published (Cabinet Office, 2012). In London, risk assessments are coordinated by the London Resilience Team (LRT) and involve representatives of the "emergency services, local authorities, health services and other emergency responders" reviewing the risk of emergencies every few months (London Resilience Team, 2013). The resulting London Risk Register includes an assessment of the likelihood and impact of each risk that could affect London and is updated annually (Hogan, 2013). The purposes of the London Risk Register are to (London Resilience Team, 2013, 2014, 2015; Hogan, 2013):

- provide emergency responders, individuals, businesses and communities with a shared understanding of the risks local communities face. This is to improve the effectiveness of their response to an emergency.
- "provide a basis for proportionate resilience planning" (London Resilience Team, 2013)
- act as a basis for developing planning assumptions and evaluation
- determine the prioritisation of activities towards risks rated higher on the scale

The London Risk Register includes three different categories of risk as highlighted in Table 6 (London Resilience Team, 2015).

Table 6 Categories of risk included in the London Risk Register

Category of risk	Risks
Natural Hazards	Human health incidents, flooding, volcanic hazards, severe weather, severe space weather, severe wildfires, animal health incidents
Major accidents/incidents	Major industrial accidents/environmental pollution, infrastructure technical failures, major structural accidents, major transport accidents, disruptive industrial action, public disorder
Malicious attacks	Attacks on crowded places, attacks on infrastructure, attacks on transport system, unconventional attacks, cyber security

Whilst this case study focuses on community preparedness for malicious attacks (i.e., terrorism), it is important to highlight that terrorism is only one of multiple risks communities in London are facing. Whilst risks including pandemics, flooding (inland, fluvial and coastal) and technical failure (e.g., electricity failure) are categorised as very high risk, the different types of malicious attack are categorised differently as shown by Table 7 (London Resilience Team, 2015).

Table 7 The categorisation of different types of terrorism

Malicious Attacks	Risk Rating	Risk Rating Definition
Attacks on crowded places	High	Significant risk
Attacks on infrastructure	High	Significant risk
Attacks on transport system	High	Significant risk
Small Scale Unconventional Attacks	High	Significant risk
Catastrophic Unconventional Attack	Very High	Requires immediate attention
Cyber security (Infrastructure)	Medium	Less significant risk
Cyber security (Data Confidentiality)	Low	Unlikely to occur and not significant impact

The London Risk Register outlines how "[w]hile terrorists can be expected to continue to favour high-profile physical attacks, the possibility that they might also use cyber space to facilitate or mount an attack is growing" (London Resilience Team, 2015, p.34).

The London Risk Register is made available to the public annually in order to encourage communities and businesses to develop arrangements for an emergency and business continuity plans (London Resilience Team, 2015). This is "[o]n the basis that risk-aware Londoners will be better able to respond to emergencies (and therefore reduce the overall impact)" (London Resilience Team, 2013). The Greater London Authority website (2013) also includes suggestions for the public, businesses and London residents to use the Risk Register to enhance their preparedness and resilience. For example, people who live in London are informed that they can think about the local risks that apply to them, how the risk might affect them and to consider whether they and their family are prepared for these risks.

However, the data gathered highlighted how London based community groups perceive the risk of terrorism differently to organisations. The London Resilience Partnership invited community groups from across London to a "Community Engagement Meeting: Community Resilience and Preparedness in London" on 26 February 2015. On arrival, participants were given three stickers[3] and asked to mark on the board the top three risks for London. In contrast to organisations, for the public, both terrorist attack and flooding were the top risks. Thus, assessments of risk may vary between organisations and communities.

2.5. Understanding potential learning needs in London

This section concludes by examining the potential learning needs that exist within London, characterised by its population diversity.

> "London is home to a hugely diverse population; forty-two percent of Londoners identify themselves as from a group other than White British and more than 300 community languages are spoken in London's schools. In addition, more than a million people commute into London to work, and as an international tourist destination and centre of finance and business, London attracts a huge number of foreign visitors" (Ingleby, 2014, p.6).

This diversity means that there is a complex and wide variety of learning needs to consider when communicating information before, during and after an emergency (Ingleby, 2014). For instance, the Communicating with the Public Framework outlines how differences between communities lead to differences in the agencies that are trusted and in the ways that members of the public receive information (Ingleby, 2014). It is recommended that messages should consider the target audience in order to ensure that the public can understand the message. In order to overcome the barriers associated with a variety of learning needs, Ingleby (2014) recommends "[t]he provision of clear and simple messages, and where appropriate, use of appropriate images facilitates message understanding. Messages should be disseminated though a wide variety of channels and platforms to ensure individuals have the greatest chance of receiving and believing the message". Table 8 highlights demographic groups and trends for London and the potential implications for TACTIC and the learning framework.

Table 8 The different demographic groups in London and their implications for TACTIC

Demographic group/trend	Potential implications for TACTIC and the learning framework
Lower income groups – 28% of Londoners are in poverty[4]	This group may not have access to computers or the internet This group may be best reached through community based organisations
Commuters – approximately 80,000 people commute into London each day[5]	Commuters may not be part of any community Employers may be used as a source of preparedness information Apps available on mobile phones or tablets may be used to reach this group
Younger age groups – 24.5% of the population of London is made up of people aged 19 or under[6]	This group may only access particular communications channels (e.g., social media) Apps available on mobile phones or tablets may be used to reach this

[3] Please note that there was no difference attached to the different coloured stickers

[4] Trust for London and New Policy Institute, London is still England's poverty capital, 13 October 2013. [Online]. http://www.londonspovertyprofile.org.uk/test/news/london-is-still-englands-pover/. (Accessed:05 March 2015).

[5] Jones, Alexandra, What challenges face London's next mayor?, 7 July 2014. [Online]. http://www.theguardian.com/local-government-network/2014/jul/07/challenges-next-mayor-london-building-homes (Accessed: 05 March 2015).

[6] London Councils, London Key Facts, (no date). [Online]. http://www.londoncouncils.gov.uk/londonfacts/default.htm?category=3 (Accessed: 05 March 2015).

	group There is the potential for the TOTAP to be used with this group in schools
Older people – 11% of Londoners are 65 years old or over[7]	Older people are more likely to have a disability that may require the TOTAP to be tailored to their specific needs There may be older people unfamiliar with using a computer who require a simplified version of the TOTAP
Languages spoken – Over 300 languages are spoken in London schools[8]	The learning framework and TOTAP may be inaccessible to groups who do not speak the languages that the materials are available in Images may be used to overcome language barriers
Disabled people – 14% of Londoners are disabled[9]	The blind and partially sighted may require the TOTAP to be available in audio or large text
Different faith groups – 52.9% of Londoners are Christians, 13.5% are Muslim, 5.5% are Hindu, 2% are Jewish, 1.7% are Sikhs and 1.1% are Buddhists[10]	The different faith groups across London provide "communities" in which the TOTAP could be promoted and implemented

Thus, the learning framework and TOTAP need to account for the diverse learning needs that exist within communities in London.

[7] Mayor of London and Tranport for London, Understanding the travel needs of London's diverse communities. A summary of existing research, August 2014. [Online]. *https://www.tfl.gov.uk/cdn/static/cms/documents/understanding-the-travel-needs-of-london-diverse-communities.pdf* (Accessed: 05 March 2015).

[8] London Councils, London Key Facts, (no date). [Online]. *http://www.londoncouncils.gov.uk/londonfacts/default.htm?category=3* (Accessed: 05 March 2015).

[9] Mayor of London and Tranport for London, Understanding the travel needs of London's diverse communities. A summary of existing research, August 2014. [Online]. *https://www.tfl.gov.uk/cdn/static/cms/documents/understanding-the-travel-needs-of-london-diverse-communities.pdf* (Accessed: 05 March 2015).

[10] Greater London Authority Intelligence,2011 Census Snapshot: Religion, December 2012. [Online]. *https://londondatastore-upload.s3.amazonaws.com/c0A%3D2011-census-snapshot-religion.pdf* (Accessed: 05 March 2015).

3. Workshop 1 on terrorism in Europe

On 10 February 2015, Trilateral Research & Consulting hosted the first workshop on preparedness for terrorism in Europe (Task 4.3), with a particular focus on London. Due to the scenario discussed during the workshop and in Section 3.1, the workshop was held within a one mile radius of King's Cross, London. There were 17 workshop participants from 12 organisations (Appendix C), including 9 TACTIC partners and 8 representatives from a non-governmental agency, the police, a community group, the media, business and academia. Difficulties were experienced in recruiting participants for this workshop focusing on terrorism. The workshop was heavily promoted from November 2014 with approximately 60 individuals/organisations directly invited by email or telephone, in addition to the workshop being promoted on the TACTIC website and Twitter account. Difficulties related to recruiting participants included organisations not responding to multiple emails, not having the resources to attend, withdrawing their participation days before the workshop due to having to respond to an emergency and registering for the workshop and then not attending. Table 9 provides an overview of the agenda for the workshop. The full agenda can be found in Appendix D.

Table 9 An overview of the workshop agenda

Session	Description
1	An overview and background to the TACTIC project, the community preparedness audit and catalogue of good practices and how these feed into the long-term framework for improving community preparedness and the web-based platform
2	A demonstration of the web-based platform (i.e., the TOTAP)
3	A case study examining how terrorism is different to other types of hazard and presenting a terrorism scenario
4	Group work discussing and developing the audit
5	An overview of the catalogue of good practices for education
6	Group work discussing and developing the catalogue of good practices for education
7	Next steps

3.1. The terrorism scenario

A scenario involving a terrorist attack was developed for the workshop in order to understand how terrorism is different to other types of disasters and what these differences mean for preparedness and risk communication. The hypothetical scenario was developed based on the analysis of past terrorist attacks in Section 1.3 and focused on the different phases of a terrorist attack to understand both preparedness and communities' communication needs before, during and after an attack. **Table *10*** highlights the information that was provided to workshop participants for each phase of the hypothetical scenario.

Table 10 Information provided to workshop participants

Phase	Available information and issues to consider
Before: preparedness	**Information available before the attacks** • Single hazard incident – terrorist attack by lone wolves • Co-ordinated bombing and shooting attacks • Early morning rush hour with implications for commuters **The possible scenario area** • One mile radius of Kings Cross Station (**Error! Reference source not found.**) • Multiple potential targets including St Pancras International (including the Eurostar), the British Library, museums, colleges and theatres

	• Heavily populated and diverse community
During: the response	**The impacted area** • 8.35am – bomb explosions at St Pancras International and Kings Cross Station • 8.45am – shooting attacks at a local renowned hotel and the British Library **Impact** • Fatalities and hundreds injured • Wide impact on transport network and wider community • Community volunteering and support (e.g., donating blood) • Need to coordinate with national and local media to prevent rumours
After: the recovery	• Wide psychological impact (e.g., stress) • Community fears of further attacks • Community tension • Behaviour change (e.g., people not visiting London)

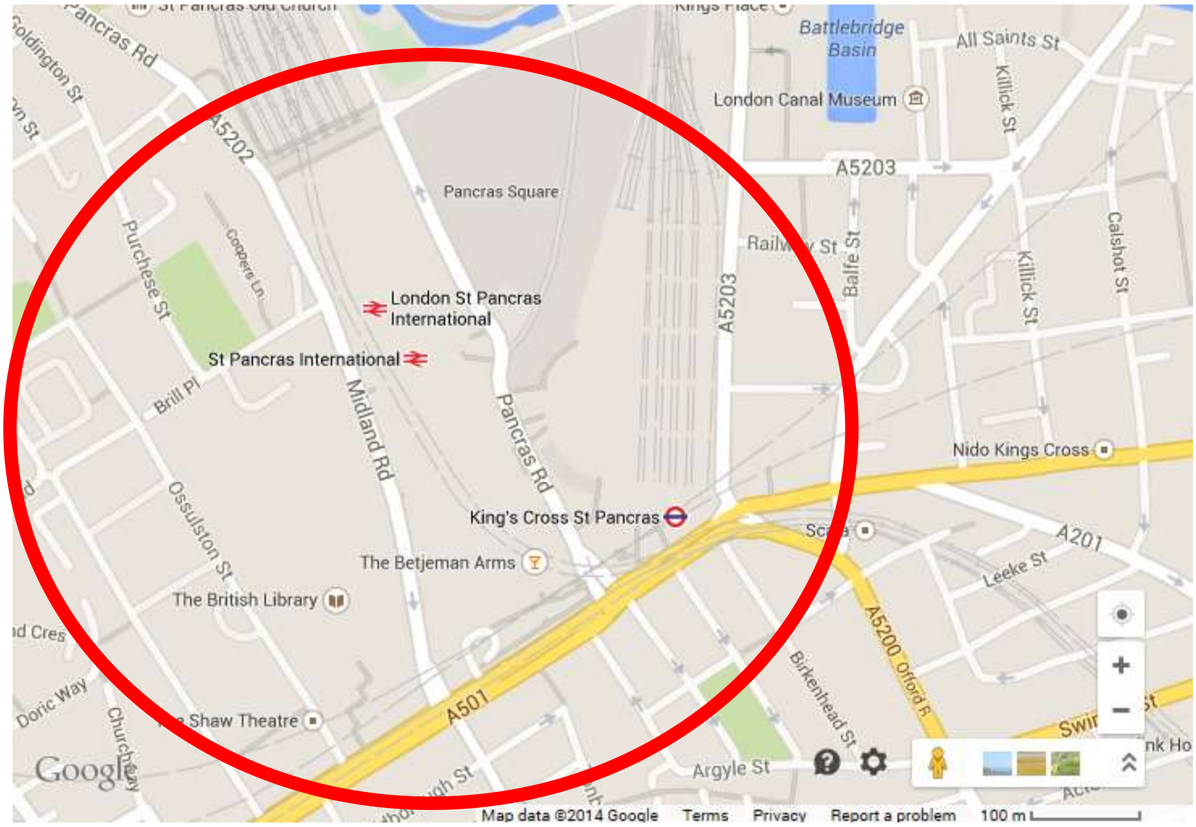


Figure 3 The terrorism scenario area

During the session focusing on the terrorism scenario, participants were asked to discuss in groups "*Is terrorism different to other types of disaster? If so, how?*" and "*What do these differences mean for preparedness?"* The feedback from participants suggests that terrorism is different to other types of disaster, which has implications for preparedness. The key points discussed in response to these questions, include:

- Terrorism differs in terms of how you prepare and what advice you can give to people and businesses. For hazards such as earthquakes, fires and flooding, preparedness advice is clearer (e.g., insurance, grab bags) than it is for terrorism
- The geographical spread is different for terrorism. Earthquakes have a certain reach but terrorism can occur anywhere and can take different forms and shapes
- Terrorism is a deliberate attack on life and critical structure rather than an act of god

- Terrorism is a dynamic threat in that multiple events can occur over a period of hours or days
- Other hazards can be more predictable or one-off events
- Terrorism is intelligent whereas other types of hazard are passive
- Communities rely on authorities and expect that they are prepared (e.g., airport security). A participant commented that their personal preparedness level isn't very high but hope that other agencies have the situation under control
- A participant outlined how the public are either prepared or not prepared and very few are. Those who do prepare were suggested to typically prepare for all-hazards which was considered as the best way to prepare by the participant. The reliance upon government to do more or be better prepared for a particular hazard was viewed as problematic as it sectionalises terrorism to a degree that it becomes unhealthy. Terrorism was viewed as representing a small percentage of what goes wrong in the world and when people die. This participant believed that there are nuances that need to be considered for terrorism but that government preparedness is government preparedness
- For terrorism, governments across the globe are taking a law focused approach and are trying to get communities to police themselves. This can become a difficult area when the messaging becomes too overt (e.g., what are your neighbours/family/kids doing?). However, there was a discussion amongst participants concerning where you draw the line
- Governments can only do so much in terms of communication. They are relying on communities and organisations to percolate the message down. They cannot do it just by a single organisation sending the message out
- There has to be a consensus around accepted levels of preparedness
- The public perception is heightened by terrorist incidents and there was the view that you cannot expect the government to do nothing. There is a balance between alert and alarm and preparedness
- In comparison to other types of hazard, people acknowledge that all the information cannot be made available for terrorism

In order to validate and supplement the information collected for Chapter 2 on preparing for terrorism in London, participants and interviewees were asked an additional four questions concerning communicating preparedness information to communities. The questions and the key responses are outlined in **Table *11***:

Table 11 Key findings stemming from the terrorism scenario

Question	Key Findings
Who is responsible for communicating with the community before the situation unfolds?	• All Category 1 responders (e.g., emergency services, local government) under the CCA have a legal responsibility to warn and inform the public generally for emergencies • The government's CONTEST strategy is designed to counter-terrorism and has four strands (prepare, pursue, protect, prevent) • The government recently held the Counter-terrorism awareness week (CTAW) which was a week of stranded information communicated through a variety of channels. This was connected with transport, rail, businesses and advising them on the heightened level of threat. There are plans to promote the CTAW campaign every month • Every borough in London has a counter-terrorism advisor • As part of Operation Fairway, the Metropolitan Police provide counter-terrorism briefings
What information are these actors obligated to provide?	• Advice is provided on what individuals, groups of individuals and businesses can do to make themselves more resilient • People are informed that they may not be within the immediate direct impact of a

/ What information is provided?	terrorist attack but they may suffer consequences (e.g., be part of crime scene) • Information on the threat level change was communicated to the public, however, a participant questioned how this should affect them and what they can do to prepare? There was a perception that the government believe that if you tell the public too much, it will worry them or prevent them from going into London • Information is communicated to businesses on what the response level should be
What tools do you use for communication purposes?	• The messages promoted during the CTAW were published in newspapers and on the tube (e.g., posters) • There is a mechanism that enables messages to be sent from the police to businesses that reaches 8 million people • Presentations to employees within large businesses. This involves showing a DVD
Would this information be sufficient to prepare the community for this type of situation?	• An interviewee believed that the information that they delivered was sufficient to prepare communities. For them, the biggest battle they face is complacency so they ensure that they redeliver various type of messages and find new audiences all the time. • For the same interviewee, it is about targeting and making sure that they deliver messages in the right fashion to that specific group. Face to face communication was viewed as very important as there are normally questions following the presentation. If they had sent a leaflet or PowerPoint presentation, it would not be possible to address the questions. Face to face communication also enables them to ensure that the message that they wanted to deliver has been delivered appropriately

However, whilst an interviewee believed that the information provided is sufficient to prepare the community, participation in the community engagement meeting hosted by the London Resilience Partnership suggested that communities in London do not feel that they have been prepared to respond to any type of risk. During the meeting, many community representatives outlined how they had not been briefed and did not know what to do in response to an emergency in London such as a CBRN attack.

The scenario outlined in this section was used to encourage the workshop participants to consider the variety of areas that the audit, categorisation of good practices and TACTIC Online Training and Audit Platform (TOTAP) may need to address. Whilst participants considered the three tools to be beneficial with the potential to add value, the first workshop focused on participant's feedback and recommendations in order to further develop the tools. The strengths of each tool will be further examined in the second workshop on terrorism in Europe (MS6).

3.2. Key findings: The participatory community preparedness audit

In the week before the workshop, participants were e-mailed a copy of the organisational audit to read in order to facilitate discussions during the workshop on how it could be further developed. During the workshop, participants were asked to work in groups to consider: 1) What should be included/and or removed from the audit? (e.g., what information do you need?) 2) How could you benefit from the audit? 3) What were your expectations of the audit? And 4)What are the strengths and weaknesses of the audit? However, due to this being the first time the participants had encountered the audit, their focus was on question 1 and providing feedback and recommendations to improve the audit. The key findings related to the audit are outlined in **Table *12***[11]:

[11] More detailed recommendations and feedback related to the audit will be provided to the partners responsible for developing the audit

Table 12 Feedback and recommendations on the audit

General feedback and recommendations	
Participant feedback	**Examples and recommendations where provided**
Define the user of the audit. Who is completing the audit will influence the framing of the audit	There could be a filter question to help people to decide which audit they should complete The audit might not be useful for governments in regards to terrorism preparedness but it could be useful to businesses and NGOs
The audit could be structured into 3 stages: Communicating preparedness Embedding preparedness Measuring preparedness	
As the audit focuses only on communication, participants questioned how we know how the public interpreted the message and whether people are prepared or took action	For communities, they could be asked the question “have you got a grab bag?” and if no, they could be provided with a list of what a grab bag could contain
The goal of the audit should not only be to improve communication but also to provide information about what actions could be undertaken to improve preparedness (e.g., content of the communication practice)	A scale could provide a score that encourages organisations to want to do more
There is a need to understand how we motivate people to act and why people are not preparing and link them together	
The use of terminology and consistent terminology should be considered	Whether it is titled an “audit” or “course” “You” and “your community” were used interchangeably
There is the need to provide people with an incentive to complete the audit and contextualise why they should complete it	The benefits of completing the audit should be clear and to the point at the beginning of the audit.
There is the need to consider how TACTIC adds value for organisations	TACTIC could be further refined to support small businesses
A discussion forum could be used to share best practices	
The audit was considered too long, detailed and time consuming	
Is there potential for the audit to be a stand-alone tool that is separate to the overall TOTAP?	The audit could be a stand-alone tool that others want to link to. Having the audit as a stand-alone tool would make it more transferable
An interviewee expressed concern over the potential for mixed messaging in terms of what is delivered by the audit and what they are able to do. They are unable to prescribe one guidance or route to follow and as an organisation, they have to stay within their remit and expertise	Provide general guidance
Recommendations related to the questions	
Participant feedback	**Examples and recommendations where provided**
Change the ordering of questions	Include question 14 on the aim of the communication strategy earlier Separate the advice-related questions and the practice-related questions
Link questions together	Link question 10 to question 12

Include additional questions	Include the question: "Do you have a communications strategy?" Include a question on business continuity
Questions should not only focus on the existence of the communications strategy but also on the methods used, behaviour change, and barriers	Include a question on barriers to preparedness
Delete questions that are not relevant as this increases confusion. It was also considered that there were too many questions	Delete question 20
Reword questions to make them clearer and less confusing in terms of what is being asked	For question 4, specify who the lessons were shared with
Emphasize key words in a question	For similar questions focusing on different phases of a terrorist attack, emphasize the phase the question is referring to
Some questions were highlighted as being organisational specific and if not relevant to a specific organisation would be based on personal opinion	
Recommendations related to the responses	
Participant feedback and recommendations	**Examples and suggestions where provided**
Reduce the number of response options available for a question	
Increase the number of response options available for a question.	Include hands on practice (e.g., training, drills, practice) to the communication and education practices used to prepare the community for terrorism
Ensure that there is a clear link between the question and the answers	
There was debate surrounding the use of the "Don't know" response option because if people don't know, then they probably shouldn't be completing the audit. Alternatively, the option of "non-applicable" could be added to all questions as the question might not be relevant to an individual's role or to the organisation	

Thus, whilst workshop participants could see the potential of the audit for increasing preparedness, at this stage their feedback focussed on how the audit could be further improved. Suggested improvements were related to more clearly defining the user of the audit, making structural changes, editing the content and providing the incentives/benefits of completing the audit.

3.3. Key findings: Categorisation of preparedness communication and education material and practices

The second session of group work focused on the categorisation of good practices. In the week before the workshop, participants were asked to think about and bring to the workshop any good practices that they had developed or come across focusing on preparing communities for terrorism. During the workshop, participants were provided with a document which explained the relationship between the audit and "good" practices and that included a draft version of the categorisation of good practices. Participants were asked to work through the document to categorise the practice that they were familiar with. This process revealed how the categorisation was viewed as an opportunity to create a channel for expert conversation and active feedback on the practices. Detailed feedback and recommendations related to the draft categorisation are highlighted in Table 13.

Table 13 Feedback and recommendations on the "good" practices categorisation

Feedback	Recommendations
Participants discussed how the practices should be evaluated. It was suggested that the categorisation was subjective and that it should be completed by trusted sources in order to be treated as a trusted source by the end users. There needs to be transparency in the reputability of the source - who decides whether something is a "good" practice	• Create a peer-review process for all the practices included in the library. • Enable users to provide feedback and comments about the practices using a rating system and comments that are pre-moderated (e.g., similar to TripAdvisor) • Include a category on whether the good practice has been evaluated • Talk to trusted organisations such as ReliefWeb and UNHCR to identify what processes they go through to upload documents
The issue of the credibility of good practices was raised One participant would prefer to look at the original source of information rather than use someone else's analysis of the practice as it would not have enough authenticity	• Practices could be rated using an expert authority or through a crowd sourced mechanism. The practices that were rated 5* could then be searched for • A question could be added asking whether users found the practice useful • Information on how many times the practice was used or cited could be included
The practices should encourage feedback and discussion and provide the community with a voice. Engagement was considered important.	• There should be the facility for two-way communication • There should be a conversation and engagement about the practices rather than it being "top down"
Avoid the use of jargon as this may prevent people from using the categorisation	
Can tangible outputs be included? (e.g., communication templates, business continuity plan, an example of a community group using the practice)	• Including case studies of how the practices have been used may add life to the documents. There is a need to make a bridge to the practical realty
The categorisation in its existing form is very desk-based	• Is there the ability to use it onsite? (e.g., mobile, app)
Refine the category related to the target audience (i.e., who was the practice developed for? e.g., local community groups, ambulance workers)	
Participants questioned who should add the practices to the database and who would own the database of practices	
Crisis response organisations that have an authority and are recognised as a go to resource for disaster preparedness (e.g., the Red Cross) could host the website and good practices	

In summary, for the workshop participants, the key issue that needs to be addressed going forward is the credibility and evaluation of the good practices. Additionally, the good practices should facilitate conversation and engagement between those categorising the practices and the users of the web-based platform.

3.4. Key findings: The TACTIC Online Training and Audit Platform

At the end of the first introductory session, partners provided a demonstration of the TACTIC Online Training and Audit Platform (TOTAP). During this demonstration and the remainder of the workshop, participants provided feedback and recommendations for the development of the TOTAP. These are highlighted in **Table *14***.

Table 14 Participant feedback and recommendations on the TOTAP

Feedback	Recommendations
- Greater consideration needs to be given when using the terms "community" and "organisations" - There is a need to define what is meant by community. For example, business is only interested in their community and not the wider community or public - The terms used should "speak to" and be of relevance to the users of the TOTAP. The language and pitch has to be tailored to the different users	- The audit could be structured so as to filter the questions based on the type of organisation that is conducting the audit. For example, not all questions included in the audit are relevant for NGOs. Instead of a general audit for all users, the organisational audit and community audit should become more specific based on the needs of the individual user. This would also address the length of the audit as participants were concerned that the length may put some people off completing the audit
- The term "audit" was also suggested to be off-putting and the language considered to technical	
- The feedback from the community should be tailored to the organisation, however, how does the platform know which "community" members to base its results on?	
- Participants questioned whether users would be able to add content to the TOTAP and if so, what type of content?	
- In terms of accessibility, there was considered to be too many menus/options. The TOTAP needs to be easy to use.	
- It was suggested that making the case study audits context specific may attract people to complete the audit	
- The audit should not be limited to the website itself. It should also be available as a mobile application	
- The images currently used should be changed as the visual representation of the platform is important	- Make the TOTAP visually appealing and accessible to a wider audience - Avoid word clouds - Use a community-based image
- Related to trust, is there potential for the TOTAP to be hosted by other reputable organisations e.g., the Red Cross?	
- The use of leading information in the self-assessment was discussed. The italicised text may help the user to understand the question but could also lead them to what the correct/desirable answer is	- Include the pop-up explanation after they have completed the question - Include a click here option for guidance - Include the context/rationale to the questions (e.g., there is research out there and the trends are as follows and you can contribute by providing a response. At the end of completing the audit, the TOTAP could show how the response fits into the wider context). However, this would depend on the purpose of asking the question - Only the question could be included and then the user click on the explanation if they want

	more information
• Have one default setting for the community and a different default setting for organisations	• Have defaults created by the TACTIC consortium not the user • There should be different options for different users • On the registration page request information on whether it is an organisation or individual registering and identify their level of experience of IT systems. Based on this there could be different configurations
• For the community audit, collect demographic information and experience as part of the registration process rather than the audit	
• Explain the purpose of the audit	
• Include a timeline/bar showing the progress that has been made	
• Enable people to get something from using the TOTAP	• The italicised text could be provided as outputs at the end to teach people something
• Include keywords at the beginning of the question	
• The audit being anonymous provides the opportunity to be honest	

The findings suggest that firstly, the users (i.e., communities and organisations) of the TOTAP need to be more clearly defined before the TOTAP can be structured and redesigned accordingly. The redesign would involve considering the content and terminology used, the accessibility and usability of the TOTAP, the visual appearance of the TOTAP and the functions that are provided.

3.5. The second workshop on terrorism in Europe

The feedback collected from the workshop participants will be used to further develop and enhance each tool. This will involve:

- Using the feedback from the first workshop on terrorism in Europe and the first workshops on floods, earthquakes and pandemics/epidemics to create an improved and multi-hazard version of the audit
- Continuing to collect good practices and refine the categorisation
- Enhancing the TOTAP in line with participant's feedback and recommendations across the four case studies

In October 2015, a second workshop on terrorism in Europe will be held in order to discuss and validate each of the tools. The second workshop will be developed based on feedback and recommendations from participants of the first workshop. During this workshop, a similar setup will be used in the form of a multi-hazard scenario to validate the audit and the education and communication materials and practices. This will involve a more complex and unfamiliar multi-hazard scenario, and thus will consider both physical and cyber terrorism. The participation of the second workshop will also be broadened to include emergency management representatives from across Europe.

4 Conclusion

This report has examined community preparedness for terrorism in order to understand how terrorism is different to other disasters, and what these differences mean for preparedness. Both the literature and workshop findings indicate that terrorism is different in terms of; being the result of deliberate human activity, the high uncertainty, unpredictability and complexity associated with terrorism, the low probability of a terrorist attack occurring and the intention of terrorists to induce fear. These differences result in preparedness for terrorism being different to preparedness for other types of hazard, which has implications for TACTIC and the long-term learning framework for improving community preparedness to multi-hazards. For instance, the characteristics of terrorism means that communities are typically prepared indirectly for terrorism through a multi-hazard approach. Whilst authorities are not preparing communities specifically for terrorism, they are requesting the public's assistance in preventing terrorist attacks through vigilance. This focus on prevention for terrorism may need to be considered in the development of the learning framework. Additionally, the responsibility for preparedness for terrorism being transferred from communities to authorities, may limit the extent to which communities can be prepared specifically for terrorism. Whilst communities may be accepting more responsibility to prepare for other types of hazard, for terrorism it is more complex and relies predominantly on organisations undertaking a range of activities to prevent, prepare for, respond to and recover from a terrorist attack.

Reviewing the literature, reports and data collected highlighted many challenges and recommendations related to preparing communities for terrorism that should be considered during the development of the audit, the categorisation of good practices, the learning framework and the TOTAP. For instance, communicating about terrorism can potentially alarm communities and make them feel more at risk if they believe that government is withholding information about a future attack. Thus, a multi-hazard approach to preparedness, that encompasses a request for the public to be vigilant, may be most suitable for preparing communities for terrorism. Whilst this report focused specifically on the risk of terrorism, London is preparing for multiple hazards including flooding and pandemics.

The need to clearly define 'who' the users of the audit, good practices categorisation and the TOTAP are was a key recommendation from workshop 1. For emergency management actors and the workshop participants based in London, the term "community" was broader than members of the public, but also included businesses that are part of the wider community. Going forward, there is a need to more clearly define how the term community is used in TACTIC as this will have implications on the design of the audit, good practices categorisation and TOTAP.

The literature, government guidance and data collected also highlighted the diversity of communities and how different approaches are required to communicate with different groups. The differences across different community groups in terms of the agencies that are trusted and the preferences for receiving communication (e.g., communications tools used, languages that materials are available in) may present a challenge for authorities in terms of reaching all members of a community. For instance, limited resources may prevent authorities from providing preparedness communications material in the 300 languages that are spoken in London schools[12]. Thus, TACTIC needs to consider the challenges authorities may face in terms of reaching different groups within a community.

Whilst the workshop 1 participants could see the benefits and value of developing the community preparedness audit, the good practices categorisation and the TOTAP, there is a need to further develop and enhance these tools based on this report and the findings of the additional workshops focusing on preparedness for flooding, earthquakes and epidemics/pandemics. The key recommendations, from workshop 1 on terrorism in Europe, for enhancing the tools include; clearly defining the user/s of the tools, further enhancing their structure and content and providing incentives/benefits for using the tools.

[12] London Councils, London Key Facts, (no date). [Online]. *http://www.londoncouncils.gov.uk/londonfacts/default.htm?category=3* (Accessed: 05 March 2015).

References

9/11 Commission, National Commission on Terrorist Attacks Upon the United States. (2004). The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States, US Government Printing Office, Washington, DC, 2004.

9/11 Commission, National Commission on Terrorist Attacks Upon the United States. (2004). The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. Executive Summary, US Government Printing Office, Washington, DC.

Alexander, D. (2002). Nature’s impartiality, man’s inhumanity: reflections on terrorism and world crisis in a context of historical disaster. *Disasters*, 26(1), 1-9.

Alexander, D. (2003). Terrorism, disasters, and security. *Prehospital and disaster medicine*, 18(03), 165-169.

Alexander, D.E. (2014). Social media in disaster risk reduction and crisis management. Sci Eng Ethics, 20, 717-733.

Altheide, D. L. (2006). Terrorism and the Politics of Fear. *Cultural Studies↔ Critical Methodologies*, *6*(4), 415-439.

Aradau, C., & Van Munster, R. (2007). Governing terrorism through risk: Taking precautions,(un) knowing the future. *European journal of international relations*, 13(1), 89-115.

Archer, E.M. (2014). Crossing the Rubicon: Understanding Cyber Terrorism in the European Content. *The European Legacy,* 19(5), 606-621.

Barkham, P. (2004, July 26). *Terrorism: advice for every household*. Retrieved from http://www.theguardian.com/media/2004/jul/26/advertising.britishresponsetoseptember11

Barnard-Wills, D., & Moore, C. (2010). The terrorism of the other: towards a contrapuntal reading of terrorism in India. *Critical Studies on Terrorism*, 3(3), 383-402.

BBC. (2003, October 6). Terror test exercise criticised. *BBC News*. Retrieved from http://news.bbc.co.uk/1/hi/england/london/3167030.stm

BBC. (2012, August 13). Norway police ‘could have stopped Brevik sooner’. *BBC News.* Retrieved from http://www.bbc.co.uk/news/world-europe-19241327

BBC. (2004, March 11). Many die as bombs destroy Madrid trains. *BBC News*. Retrieved from http://news.bbc.co.uk/onthisday/hi/dates/stories/march/11/newsid_4273000/4273817.stm

Bellanova, R. (2014). ‘Resilience in the US: cyber security and critical infrastructure protection’. In Wright, D. and Rodrigues, R. *Deliverable D6.1 – A report on resilience in “democratic” surveillance societies*, *D6.1 of the IRISS project*. http://irissproject.eu/?page_id=9

Bongar, B. M., Brown, L. M., Beutler, L. E., Breckenridge, J. N., & Zimbardo, P. G. (2007).*Psychology of terrorism*. New York: Oxford University Press.

Boscarino, J. A., Figley, C. R., & Adams, R. E. (2003). Fear of terrorism in New York after the September 11 terrorist attacks: implications for emergency mental health and preparedness. *International journal of emergency mental health*, *5*(4), 199-209.

Bourque, L. B., Regan, R., Kelley, M. M., Wood, M. M., Kano, M., & Mileti, D. S. (2012). An examination of the effect of perceived risk on preparedness behavior. Environment and Behavior, 0013916512437596.

Braithwaite, A. (2013). The logic of public fear in terrorism and counter-terrorism. *Journal of police and criminal psychology*, *28*(2), 95-101.

Brown, G. (2014). Strategic Coordination Protocol. London Resilience Partnership. Retrieved from https://www.london.gov.uk/sites/default/files/Strategic%20Coordination%20Protocol%20v6.1%20Apr%202014.pdf

Buchanan, R.T. (2012, July 22). Norway massacre: A timeline of the attacks that horrified a nation. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/news/worldnews/europe/norway/9495025/Norway-massacre-A-timeline-of-the-attacks-that-horrified-a-nation.html

Bullock, J., Haddow, G., & Coppola, D. P. (2013). *Homeland Security: The Essentials*. Butterworth-Heinemann.

Bux, S. M., & Coyne, S. M. (2009). The Effects of Terrorism: The Aftermath of the London Terror Attacks1. *Journal of Applied Social Psychology*, *39*(12), 2936-2966.

Campbell, D. and Laville, S. (2005, July 13). British suicide bombers carried out London attacks, says Police. *The Guardian*. Retrieved from http://www.theguardian.com/uk/2005/jul/13/july7.uksecurity6

Davis, Edward F. III, *Testimony Before the Senate Committee on Homeland Security*, US Senate, July 10, 2013.

Day, T. G. (2003). The autumn 2001 anthrax attack on the United States Postal Service: the consequences and response. *Journal of contingencies and crisis management*, *11*(3), 110-117.

Drury, J., Cocking, C., & Reicher, S. (2009). The nature of collective resilience: Survivor reactions to the 2005 London bombings. *International Journal of Mass Emergencies and Disasters*, *27*(1), 66-95.

Cabinet Office. (2009). Civil Contingencies Act 2004: a short guide (revised). Civil Contingencies Secretariat. Retrieved from http://www.essex.gov.uk/Your-Council/Local-Government-Essex/Documents/15mayshortguide.pdf

Cabinet Office. (2011). The role of Local Resilience Forums: A reference document. The Civil Contingencies Act (2004), its associated Regulations (2005) and guidance, the National Resilience Capabilities Programme and emergency response and recovery. Civil Contingencies Secretariat.

Cabinet Office. (2012). Chapter 9 London: Revision to Emergency Preparedness. Civil Contingencies Act Enhancement Programme. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61032/Chapter-9-London-revised-March-2012.pdf

Cabinet Office. (2012). Chapter 4 Local responder risk assessment duty. Revision to Emergency Preparedness. Civil Contingencies Act Enhancement Programme. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61027/Chapter-4-Local_20Responder-Risk-assessment-duty-revised-March.pdf

Cabinet Office. (2013). Preparation and planning for emergencies: responsibilities of responder agencies and others. Retrieved from https://www.gov.uk/preparation-and-planning-for-emergencies-responsibilities-of-responder-agencies-and-others

Centers for Disease Control and Prevention (CDC). (2014). Emergency Preparedness and You. Retrieved from http://emergency.cdc.gov/preparedness/index.asp

City of London Police. (2014, November 27). National Counter Terrorism Awareness Week. Retrieved from https://www.cityoflondon.police.uk/news-and-appeals/campaigns-and-initiatives/counter-terrorism-awareness-week/Pages/default.aspx

Coaffee, J., Murakami Wood, D., & Rogers, P. (2008). The Everyday Resilience of the City: how cities respond to terrorism and disaster.

Cole, B. (2011). *The Changing Face of Terrorism: How Real is the Threat from Biological, Chemical and Nuclear Weapons*. London: I.B. Tauris & Co Ltd, London.

Corrigan, D. (2004, March). Madrid Bombings, March 11 2004 – A Timeline of Events. *About.com*. Retrieved from http://gospain.about.com/od/spanishlife/a/madridbombtime.htm

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. *Networks and netwars: The future of terror, crime, and militancy*, *239*, 288.

Eligon, J. and Cooper, M. (2013, April 15). Blasts at Boston Marathon Kill 3 and Injure 100. The New York Times. Retrieved from http://www.nytimes.com/2013/04/16/us/explosions-reported-at-site-of-boston-marathon.html?pagewanted=all&_r=1

(FBI) The FBI Federal Bureau of Investigation. (no date). Amerithrax or Anthrax Investigation. Retrieved from http://www.fbi.gov/about-us/history/famous-cases/anthrax-amerithrax

Ford, L. (2005, July 7). Schools to close Friday. *The Guardian*. Retrieved from http://www.theguardian.com/education/2005/jul/07/schools.uk

Greater London Authority. (2014). Introducing…the London Resilience Team. Retrieved from http://www.london.gov.uk/mayor-assembly/mayor/london-resilience/london-prepared-blog/2012/10/introducingthe-london-resilience-team

Griffiths, E. (2006, July 5). Is London ready for another 7/7? BBC News. Retrieved from http://news.bbc.co.uk/1/hi/england/london/5133210.stm

Gunaratna, R., & Haynal, C. (2013). Current and Emerging Threats of Homegrown Terrorism: The Case of the Boston Bombings. *Perspectives on Terrorism*, *7*(3).

Heickerö, R. (2014). Cyber Terrorism: Electronic Jihad. *Strategic Analysis*,*38*(4), 554-565.

HM Government (2004). Preparing for Emergencies: What You Need to Know. Retrieved from http://www.monmouthshire.gov.uk/app/uploads/2013/06/Preparing_for_Emergencies-_Eng.pdf

HM Government. (2013). CONTEST. The United Kingdom's Strategy for Countering Terrorism. Annual Report. The Stationery Office. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/170644/28307_Cm_8583_v0_20.pdf

Hoffman, B. (2006). *Inside Terrorism*. New York: Columbia University Press

Hogan, M. (2013). London Risk Register. A brief overview of the London Risk Register. Prezi Presentation. Retrieved from https://prezi.com/ghza5vj7_0wu/london-risk-register/

Hua, J., & Bapna, S. (2012). How Can We Deter Cyber Terrorism?. *Information Security Journal: A Global Perspective*, *21*(2), 102-114.

Ingleby, A. (2014). Communicating with the Public Framework. London Resilience Partnership. Retrieved from https://www.london.gov.uk/sites/default/files/Communicating%20with%20the%20Public%20Framework%20v1.0%20web.pdf

Jenkins, B., (2007). The terrorist threat to surface transportation. National Transportation Security Center. Mineta Transportation Institute.

Joint Emergency Services Interoperability Principles (JESIP). (no date). About. Retrieved from http://www.jesip.org.uk/about/

Johnstone, B. (2005). New Strategies to Protect America: Terrorism and Mass Transit after London and Madrid. Center for American Progress Retrieved from https://www.americanprogress.org/issues/security/news/2005/08/10/1592/new-strategies-to-protect-america-terrorism-and-mass-transit-after-london-and-madrid/

Kano, M., Wood, M. M., Bourque, L. B., & Mileti, D. S. (2011). Terrorism preparedness and exposure reduction since 9/11: the status of public readiness in the United States. *Journal of Homeland Security and Emergency Management*, *8*(1).

Kearon, T., Mythen, G., & Walklate, S. (2007). Making Sense of Emergency Advice: Public Perceptions of the Terrorist Risk. *Security Journal*, *20*(2), 77-95.

Khindria, C. and Meyers-Belkin,H. (2015, March 20). Terror attack in Tunis: Arab Spring poster child targeted (part 1). *France24*. Retrieved from http://www.france24.com/en/20151903-the-debate-tunisia-terrorist-attack-part-one/

Kreissl, D. (2014). 'The Boston bombing'. In Wright, D. and Rodrigues, R. *Deliverable D6.1 – A report on resilience in "democratic" surveillance societies, D6.1 of the IRISS project*. http://irissproject.eu/?page_id=9

Kristof, N.D., (1995, March 21). Hundreds in Japan Hunt Gas Attackers After 8 Die. *New York Times*. Retrieved from http://www.nytimes.com/learning/general/onthisday/big/0320.html#article

Kunreuther, H. (2002). Risk Analysis and Risk Management in an Uncertain World. *Risk analysis*, *22*(4), 655-664.

Laqueur, W. (1996). Postmodern terrorism. *Foreign Aff.*, *75*, 24.

Larsen, M., & Piché, J. (2009). Public vigilance campaigns and participatory surveillance after 11 September 2001. In S. P. Hier and J. Greenberg (Ed.), *Surveillance. Power, Problems, and Politics* (187-202). Vancouver: UBC Press.

Lemyre, L., Turner, M. C., Lee, J. E., & Krewski, D. (2006). Public perception of terrorism threats and related information sources in Canada: implications for the management of terrorism risks. *Journal of Risk Research*, *9*(7), 755-774.

Lemyre, L., Clément, M., Corneil, W., Craig, L., Boutette, P., Tyshenko, M., & Krewski, D. (2005). A psychosocial risk assessment and management framework to enhance response to CBRN terrorism threats and attacks.*Biosecurity and bioterrorism: biodefense strategy, practice, and science*, *3*(4), 316-330.

Lerner, J. S., Gonzalez, R. M., Small, D. A., & Fischhoff, B. (2003). Effects of Fear and Anger on Perceived Risks of Terrorism A National Field Experiment. *Psychological science*, *14*(2), 144-150.

Levine, M. and Margolin, J. (2015, January 11). ISIS Renews Previous Calls for Attacks in West as Police Remain Vigilant. abc News. Retrieved from http://abcnews.go.com/US/isis-renews-previous-calls-attacks-west-police-remain/story?id=28151629

Lewis, S. (2012). Emergency preparedness – working in partnership. Journal of Terrorism Research, 3(1). Retrieved from http://ojs.st-andrews.ac.uk/index.php/jtr/article/view/413/372

London Assembly. (2006). Report of the 7 July Review Committee. Greater London Authority. Retrieved from http://www.london.gov.uk/sites/default/files/archives/assembly-reports-7july-report.pdf

London Elects. (2012). The Greater London Authority, the Mayor of London, and the London Assembly. Retrieved from http://www.londonelects.org.uk/download/file/fid/228

London Emergency Services Liaison Panel (LESLP). (2012). Major Incident Procedure Manual. Eighth Edition. The Stationery Office. Retrieved from http://www.leslp.gov.uk/docs/major_incident_procedure_manual_8th_ed.pdf

London Regional Resilience Forum. (2006). Looking back, moving forward. The Multi-Agency Debrief. Lessons identified and progress since the terrorist events of 7 July 2005. Retrieved from https://www.london.gov.uk/sites/default/files/LRRF-7July-debrief-report.pdf

London Resilience Partnership. (2013). London Resilience Strategy. Retrieved from https://www.london.gov.uk/sites/default/files/London%20Resilience%20Partnership%20Strategy%20v1%20web%20version_1.pdf

London Resilience Team. (2013). London Risk Register: The risks you need to know about. Greater London Authority. Retrieved from http://www.london.gov.uk/mayor-assembly/mayor/london-resilience/london-prepared-blog/2013/06/london-risk-register-the-risks-you-need-to-know-about

London Resilience Team. (2014). London Risk Register. Greater London Authority.

Mayor's Office for Policing and Crime (2015a). Counter Terrorism Command. Metropolitan Police. Retrieved from http://content.met.police.uk/Article/Counter-Terrorism-Command/1400006569170/specialistoperations

Mayor's Office for Policing and Crime (2015). Major counter terrorism awareness operation launches in London. Metropolitan Police. Retrieved from http://content.met.police.uk/News/Major-counter-terrorism-awareness-operation-launches-in-London/1400027993456/1257246745756

Mcdonald, M. (2005). Be alarmed? Australia's anti-terrorism kit and the politics of security. *Global Change, Peace & Security*, *17*(2), 171-189.

McEntire, D. A. (2007). Local emergency management organizations. In H. Rodríguez, E. L. Quarantelli and R. R. Dynes (Ed.), *Handbook of disaster research* (168-182). New York: Springer.

Morris, N. (2014, 26 November). Counter-terrorism awareness drive denounced as cynical political PR. *The Independent*. Retrieved from http://www.independent.co.uk/news/uk/politics/counterterrorism-awareness-drive-denounced-as-cynical-political-pr-9885727.html

Muir, H. (2003, September 5). London Tube test for terror gas attack. *The Guardian*. Retrieved from http://www.theguardian.com/society/2003/sep/05/terrorism.disasterresponse

Mythen, G., & Walklate, S. (2008). Terrorism, risk and international security: The perils of asking'what if?'. *Security Dialogue*, *39*(2-3), 221-242.

Mythen, G., & Walklate, S. (2006). Communicating the terrorist risk: Harnessing a culture of fear?. *Crime, Media, Culture*, *2*(2), 123-142.

Nellis, A. M. (2009). Gender differences in fear of terrorism. *Journal of Contemporary Criminal Justice*. *25*(9), 322-340.

New York Times 2011, http://www.nytimes.com/2011/10/10/science/10anthrax.html?_r=1 Accessed 05.11.2014

Office of Public Health Preparedness and Response (OPHPR). (2014, September 30). Preparedness for All Hazards. Retrieved from http://emergency.cdc.gov/hazards-all.asp

Page, L., Rubin, J., Amlôt, R., Simpson, J., & Wessely, S. (2008). Are Londoners prepared for an emergency? A longitudinal study following the London bombings. *Biosecurity and bioterrorism: biodefense strategy, practice, and science*, *6*(4), 309-319.

Pangi, R. (2002). Consequence Management in the 1995 Sarin Attacks on the Japanese Subway System (Report ESDP-2002-01 / BCSIA-2002-04). Retrieved from http://belfercenter.ksg.harvard.edu/files/consequence_management_in_the_1995_sarin_attacks_on_the_japanese_subway_system.pdf

Papadimitriou, A., Yannopoulos, A., Kotsiopoulos, I., Finn, R. L., Watson, H., Wadhwa, K. and Baruh, L. (2013) Case studies of communication media and their use in crisis situations. Deliverable 2.2 of the COSMIC project.

Perry, R. W., & Lindell, M. K. (2003). Preparedness for emergency response: guidelines for the emergency planning process. *Disasters*, *27*(4), 336-350.

PR Week. (2005, September 29). Putting crisis theory into practice. Retrieved from http://www.prweek.com/article/519174/7-july-putting-crisis-theory-practice

Jones, R. and Raab, C. (2014). The London bombings, 2005 ("7/7"). In Wright, D. and Rodrigues, R. *Deliverable D6.1 – A report on resilience in "democratic" surveillance societies*, *D6.1 of the IRISS project*. http://irissproject.eu/?page_id=9

Ready.Gov. (no date). Terrorist hazards. Retrieved from http://www.ready.gov/terrorist-hazards

Redlener, I. E., & Berman, D. A. (2006). National Preparedness Planning: the Historical Context and Current State of the US Public's Readiness, 1940-2005.*Journal of International Affairs*, *59*(2), 87-103.

Rodin, D. (2004). Terrorism without Intention*. *Ethics*, *114*(4), 752-771.

Rodrigues, R. (2014). The Mumbai terrorist attacks 2008 ("26/11"). In Wright, D. and Rodrigues, R. *Deliverable D6.1 – A report on resilience in "democratic" surveillance societies*, *D6.1 of the IRISS project*. http://irissproject.eu/?page_id=9

Rubin, G. J., Brewin, C. R., Greenberg, N., Simpson, J., & Wessely, S. (2005). Psychological and behavioural reactions to the bombings in London on 7 July 2005: cross sectional survey of a representative sample of Londoners. *Bmj*,*331*(7517), 606.

Schwartz, Kurt N., *Testimony before the Senate Committee on Homeland Security & Governmental Affairs: The Boston Marathon Bombings*, US Senate, 10 July 2013, p. 7.

Sciolino, E. (2004, March 11). Spain Struggles to Absorb Worst Terrorist Attack in Its History. The New York Times. Retrieved from http://www.nytimes.com/2004/03/11/international/europe/11CND-TRAI.html

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.

Simon, J. D. (2013a). *Lone Wolf Terrorism: Understanding the Growing Threat*. Prometheus Books.

Simon, J.D. (2013b, April 17). An Army of One. What makes lone-wolf terrorists so dangerous? Foreign Policy. Retrieved from http://foreignpolicy.com/2013/04/17/an-army-of-one/

Sky News. (2003, September 6). Mass Evacuation Plans for London. Retrieved from http://news.sky.com/story/210661/mass-evacuation-plans-for-london

Sloan, S. (2002). Meeting the terrorist threat: The localization of counter terrorism intelligence. *Police Practice and Research*, *3*(4), 337-345.

Slovic, P. (2002). Terrorism as hazard: A new species of trouble. *Risk analysis*, *22*(3), 425-426.

Somers, S., & Svara, J. H. (2009). Assessing and managing environmental risk: Connecting local government management with emergency management.*Public Administration Review*, *69*(2), 181-193.

Stewart, M. G., Netherton, M. D., & Rosowsky, D. V. (2006). Terrorism risks and blast damage to built infrastructure. *Natural Hazards Review*, *7*(3), 114-122.

The Guardian. (2004, March 26). 'We must learn lessons from Madrid'. Retrieved from http://www.theguardian.com/society/2004/mar/26/spain.internationalnews

The Guardian (2005a, July 7). Transport chaos after London blasts. *The Guardian*. Retrieved from http://www.theguardian.com/travel/2005/jul/07/travelnews.terrorism.transportintheuk

The Guardian. (2005b, July 7). Hospitals treat hundreds of blast casualties. *The Guardian*. Retrieved from http://www.theguardian.com/society/2005/jul/07/hospitals.terrorism

The Washington Post. (2006, September 11). Timeline of Events From September 11, 2001. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2006/09/11/AR2006091100450.html

Torabi, M. R., & Seo, D. C. (2004). National study of behavioral and life changes since September 11. *Health Education & Behavior*, *31*(2), 179-192.

Twigg, J. (2004). *Disaster risk reduction: mitigation and preparedness in development and emergency programming*. Humanitarian Practice Network, Overseas Development Institute.

UNISDR. (2007, August 30). Terminology. http://www.unisdr.org/we/inform/terminology

United States National Research Council (US). Committee on Science, & Technology for Countering Terrorism. (2002). *Making the nation safer: the role of science and technology in countering terrorism.* National Academies Press.

Warrick, J. (2010, February 20). FBI investigation of 2001 anthrax attacks concluded; U.S. releases details. *The Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2010/02/19/AR2010021902369.html

Weimann, G. (2004). Cyberterrorism. How Real Is the Threat? United States Institute of Peace Special Report. Retrieved from http://www.usip.org/sites/default/files/sr119.pdf

Appendix A – An examination of past terrorist attacks

As outlined in Section 1.3, past terrorist attacks were examined in order to understand the different scenarios that communities may need to be prepared for and to develop the scenario used in workshop 1. The analysis of each attack will outline their impacts and where appropriate highlights issues related to mitigation, preparedness, response and recovery.

The sarin attacks on the Tokyo Subway, Japan, 1995

In March 1995, the Aum Shinrikyo cult carried out an attack using the nerve gas sarin in the Tokyo subway (Laqueur, 1996). This attack represented "the first significant terrorist attacks with weapons of mass destruction to occur in modern times" (Pangi, 2002, p.1). Chemical attacks such as this are different to the more conventional attacks examined in this appendix as quick intervention (e.g., decontamination) can mitigate the impact of chemical attacks by saving lives and preventing further exposure (Pangi, 2002)). The attacks "came at the peak of the Monday morning rush hour in one of the busiest commuter systems in the world" as the Tokyo subway transports 5.8 million people per day (Kristof, 1995). The attacks were coordinated, using a minimum of five packages to simultaneously release poisonous gas on three different subway lines (Kristof, 1995). Highlighting the devastating impact desired by the Aum Shinrikyo cult, the release of sarin is particularly effective in enclosed spaces such as subways and tunnels as it cannot rise and dissipate (Kristof, 1995). Ten people died from the attack and 5,000 people were injured (Kristof, 1995). Police officers and subway workers cleaning up the spills of liquid sarin were amongst those injured (Kristof, 1995).

"The historical and cultural reluctance among Japanese officials to prepare for or even discuss terrorism…hindered the response effort" (Pangi, 2002, p.9). Due to the unprecedented nature of the attack, there had been no training or plans to prepare personnel for a WMD attack (Pangi, 2002). This is despite Aum Shinrikyo carrying out a sarin attack in Matsumoto in June 1994 (Pangi, 2002). Whilst the 1994 attacks killed seven people and hospitalized 500, no significance was attached to them (Pangi, 2002).

A news article by The New York Times highlights how the initial response to the attacks included a request from the Prime Minister for "'all the Japanese people to cooperate by reporting any suspicious objects at public meetings or in trains or buses'" (Kristof, 1995). A more detailed analysis of the response to the attacks highlights issues, including (Pangi, 2002);

- Initial delays in identifying the nature of the attacks, caused by transit workers being the first to respond and a lack of communication between government agencies. This resulted in trains continuing to run for an hour and a half after the public first reported the incident, potentially increasing the public's exposure to the sarin
- Inadequate communication with the public during and following the attacks. Confusing messages were disseminated during the attacks and insufficient information was provided after the attacks causing fear in the public and victims
- Hospitals and their communications systems being overwhelmed. This was heightened by the "worried well" seeking medical treatment (p.30). Approximately 5,510 people who visited the hospital were "psychological casualties" (Lemyre et al., 2005, p.317)

The long-term effects experienced by the population of Tokyo included a fear of commuting, absenteeism from work, a lack of trust in authorities, depression, anxiety, insomnia and uncertainty over the long-term health impacts (Lemyre et al., 2005).

Many preparedness related lessons were learnt and subsequently, recommendations were implemented following the sarin attacks, including (Pangi, 2002);

- Changes in government attitudes towards terrorism (e.g., in 1999 the Japanese government held their first bioterrorism conference)
- Training volunteers on the response to chemical and biological weapons
- Conducting large-scale disaster drills
- Improving inter-agency cooperation and communication
- The established of the Tokyo National Disaster Center which operates as an educational facility until a crisis occurs. In response to a crisis, the center can provide and accommodate hospital beds.
- Training emergency responders and physicians to treat the symptoms of posttraumatic stress disorder.

It is interesting to note that following the attacks “there has not been a strong focus on building a public affairs strategy that would enable the government to communicate effectively with the public” (Pangi, 2002, p.24). This suggests that for terrorism, the focus is on improving organisational preparedness and response, rather than the public’s. This is an issue that is discussed further in section 3.1 in relation to the findings of workshop 1.

11th September attacks in the USA (9/11), 2001

The attacks in the USA on the 11th September 2001 (9/11) involved multiple attacks, coordinated and carried out during the early morning rush-hour. Four attacks “were planned and carried out by al-Qaida operatives, and were based on the coordinated hijacking of commercial flights and their use as weapons” (Bellanova, 2014, p.89). At 8.46am, the first plane crashed into the north tower of the World Trade Center (WTC) (The Washington Post, 2006). This was followed by a second plane striking the south tower of the WTC at 9.03am (The Washington Post, 2006). The impact of these crashes resulted in the south and north towers collapsing at 9.59am and 10.28am respectively (The Washington Post, 2006). In addition to the attacks on the WTC, a hijacked plane crashed into the Pentagon at 9.37am and a hijacked plane targeting the United States Capitol or the White House was forced down by passengers into a field in Pennsylvania at 10.03am (9/11 Commission Executive Summary, 2004). “More than 2,600 people died at the…[WTC]; 125 died at the Pentagon; 256 died on the four planes” (9/11 Commission Executive Summary, 2004, p.1-2).

Whilst the attacks “were a shock...they should not have come as a surprise” (9/11 Commission Report Executive Summary, 2004 p.2). There had been many warnings that Islamist extremists were intent on killing large numbers of Americans indiscriminately (9/11 Commission Report Executive Summary, 2004). For example, in 1993, a bomb attack on the World Trade Centre resulted in the deaths of six people and left thousands wounded (9/11 Commission Report Executive Summary, 2004). Further attacks between 1993 and October 2001 clearly revealed this intention to the U.S. government, Congress, media and public (9/11 Commission Report Executive Summary, 2004).

However, despite earlier attacks providing warnings, America was not prepared for 9/11; 9/11 "was a day of unprecedented shock and suffering in the history of the United States. The nation was unprepared" (9/11 Commission Report Executive Summary, 2004, p1). The 9/11 Commission was established in November 2002 with the aim of providing a detailed accounting of the attacks and to provide recommendations on how to prevent future attacks (Bellanova, 2014). Their report provides many lessons for planning and preparing for future terrorist attacks. In New York, as the attacks were an "unimaginable catastrophe", the Fire Department of New York (FDNY), New York Police Department (NYPD), "the Port Authority, WTC employees, and the building occupants…did their best to cope with the effects…for which they were unprepared in terms of both training and mindset" (9/11 Commission Report, 2004, p.315).

Discussing the public's preparedness for 9/11, the 9/11 Commission Report (2004) outlines how "[o]ne clear lesson of September 11 is that individual civilians need to take responsibility for maximizing the probability that they will survive, should disaster strike" (p.318). The report also recommends that the public should identify the locations of every stairwell where they work and always have access to flashlights (ibid.). The 9/11 Commission Report Executive Summary (2004) also proposed a strategy to: "(1) attack terrorists and their organizations, (2) prevent the continued growth of Islamist terrorism, and (3) protect against and prepare for terrorist attacks" (p.17).

The anthrax attacks in the USA, 2001

Shortly after 9/11, "letters laced with anthrax began appearing in the U.S. mail. Five Americans were killed and 17 were sickened in what became the worst biological attacks in U.S. history" (FBI Website, no date). A maximum of six letters containing anthrax were posted on 18 September and a further two on 9 October (Day, 2003). However, there is uncertainty over the exact number of letters sent as only four letters containing anthrax were discovered (Day, 2003). The first two people were identified as being infected with anthrax on 4 and 5 October and testing indicated that the exposure had been through the mail at their workplace in Florida (Day, 2003). This resulted in the death of one of the two people that had been exposed (Day, 2003). Between 12 and 19 October, two letters with anthrax were found and seven individuals infected with Anthrax were identified in New York (Day, 2003). The targets of the attacks in Florida and New York were both media outlets (television and newspaper) (Day, 2003). On 15 October, the attacks moved to Washington DC when a US Senate worker opened a letter containing a different form of anthrax. The anthrax in this letter and a second letter targeting a Senator contained a "weaponised form of anthrax [that] was squeezed out of the letters as it passed through the high-speed automated [mail] processing equipment" (Day, 2003, p. 111). Whilst there was no contamination of US postal service (USPS) employees in Florida, wide-spread contamination was identified at the mail processing centers in Washington DC and New Jersey, resulting in the deaths of two USPS employees in Washington DC on 20 and 21 October (Day, 2003). In response to their deaths, the USPS in Washington DC was immediately closed and employees were provided with antibiotics (Day, 2003). The last two deaths caused by letters containing anthrax were in New York and Connecticut (Day, 2003). As no anthrax spores were found in their residences, it was assumed that it was due to the "cross contamination" of their mail that they had been infected (Day, 2003, p.112). An eight year investigation by the Justice Department provided significant support for the FBI's argument that the attacks were carried out by one individual, biologist Bruce E. Ivins (Warrick, 2010). However, subsequent scientific research has questioned whether Irvins was able to carry out the attacks alone or if he was involved at all (New York Times, 2011).

The attacks provided lessons on communicating with different stakeholders during a terrorist attack, which can be considered by organisations planning and preparing for terrorism. The lessons learnt from the USPS perspective, include (Day, 2003):

- The importance of communication being open and honest. Provide information on what is known (i.e., provide the facts without over speculating), which help to establish credibility
- Reach out and communicate with all stakeholders (e.g., employees, customers, unions, etc.)
- Use multiple communication channels

The Madrid bombings, 2004

Both the attacks in Madrid on the 11 March, 2004 and the attacks in London on the 7th July, 2005, examined in the next section, were attacks on the transportation network using bombs. Land based transportation networks are a preferred target for terrorists due to their vulnerability (Johnstone, 2005). Reasons for their vulnerability include that; they are easily accessible; their infrastructure is fixed and unguarded and only a small amount of force is required to cause damage and serious injuries (ibid.). Jenkins (2007) also outlines how they provide easy escape, anonymity in a group of strangers, a vulnerable crowd in a contained area and the attacks create alarm and disruption. The importance of considering preparedness for and the response to terrorist attacks on land based transportation systems is highlighted by the fact that approximately one-third of all attacks world-wide have been on land based transportation systems, with bombings being the most frequent type of attack (Johnstone, 2005).

The Madrid bombings involved bomb attacks on public transport during the morning rush hour (Raab and Jones, 2014). Ten bombs exploded on four commuter trains resulting in the deaths of 191 people and more than 1,800 people injured (ibid.). The explosions were co-ordinated, occurring within a ten minute period (Sciolino, 2004). The attacks were not a complete surprise as in October 2003, Spain had been threatened in a recording allegedly made by Osama bin Laden (ibid.). In the lead up to the 11 March, there had also been fears of an attack due to the Spanish elections and twelve days before the attacks a van containing explosives was intercepted by police (BBC, 2004).

Antoni Bruel i Carreras, head of international and domestic emergencies at the Spanish Red Cross, was involved in the immediate response to the bombings and outlined how psychologically the population was not prepared for the attack;

> “There’s something different about a situation where the intention has quite simply been to kill as many people as possible…Nobody was prepared for this…We were not ready to face this kind of situation in our country, we don’t have big natural catastrophes and were not psychologically prepared to see this many people dying on our streets” (The Guardian, 2004).

Immediate responses to the attack included cancelling all trains in and out of Madrid, setting up an “emergency field hospital” outside a major railway station, requesting the public to give blood, establishing a morgue in an exhibition hall to enable relatives to identify remains and making requests for the public to send text messages instead of making calls to reduce the pressure on the phone network (BBC, 2004). The 112 “emergency communication centers” that were established to take calls from concerned members of the public received over 20,000 calls on the morning of the attacks (ibid., 139).

The measures introduced in response to the Madrid bombings included targeting the public with "sensitization campaigns" encouraging the public to report any abnormalities (ibid., p.96). Carreras, from the Spanish Red Cross, highlights how civil society can also support the response to large-scale emergencies in the future, outlining how; "[w]e don't want to create communities of victims, we need to be creating communities of people who are prepared to deal with a disaster on home soil, whether it be a terrorist bomb, flooding or a train accident" (The Guardian, 2004). Similar to other terrorist attacks, the public assisted in the response and were seen on television helping paramedics (Corrigan, 2004).

The London Bombings, 2005

The London attacks began at 8.50am on 7th July (7/7) 2005 and involved three bombs exploding within minutes of each other on the London Underground (on the Circle and Piccadilly Lines) and a further explosion approximately one hour later on a double decker bus at Tavistock Square (London Assembly, 2006). The attacks killed 52 people and injured 770 (ibid.). However, "many more hundreds of people were directly affected by the attacks, including passengers who were uninjured but potentially traumatised by the experience" (ibid, p.12). The attacks also resulted in "chaos" to the transport network, with the London Underground and buses in central London being suspended and mainline trains, airport services and roads also being affected (The Guardian, 2005a). Wider impacts included the disruption to healthcare and the closure of schools in London boroughs (The Guardian, 2005b; Ford, 2005). As British citizens, the terrorists that carried out the attacks were "home-grown" (Campbell and Laville, 2005).

Whilst public preparedness for 7/7 is unknown as individual preparedness in the UK was not evaluated prior to 7/7 (Page et al., 2008), organisations had undertaken activities to prepare for a terrorist attack. "London had planned, prepared and practised its response. Emergency planners had worked for years to put in place effective plans to respond to a terrorist attack or other major or catastrophic incidents in the capital" (London Assembly, 2006, p.6). The activities that had been undertaken to plan and prepare include;

- Establishing London Resilience partnership following 9/11 to "assess London's capacity to respond to a similar incident, and to drive London's preparation for emergencies" (London Regional Resilience Forum, 2006, p.1). The partnership is led by London Resilience Forum
- The development of Operation Sassoon, a confidential plan drawn up by government for the mass evacuation of London in response to a terrorist attack (Sky News, 2003). Additional plans that had been developed for London through the years include; "the London Emergency Services Liaison Panel (LESLP) Major Incident Plan, Operation Benbow (joint operation by London's police forces), and the London Command and Control Protocol, Local Authority Gold Protocol, First Alert Protocol, Public Information Plan, Mass Fatality Plan and Disaster Fund Plan" (London Regional Resilience Forum, 2006, p.3)
- Implementing measures to protect infrastructure (e.g., by placing concrete blocks around parliament) (Griffiths, 2006)
- Multiple exercises including a counter-terrorism exercise on the London Underground in 2003 (Sky News, 2003) and a practice exercise of Gold Command (responsible for the strategic response) on 12 June, 2005, close to the Aldgate explosion (Seegal, 2006)

Thus, as highlighted by a participant during workshop 1, whilst communities may have low levels of preparedness for terrorism, organisations are undertaking various activities to plan and prepare.

Despite this planning and preparedness, a number of issues were identified related to the effectiveness of the response. The initial response was confusion based on London Underground Network Control Centre initially responding to the attacks as if they were power surges due to the loss of power and reports of loud bangs (London Assembly, 2006). Whilst at 9.15am, it was known that the incident involved explosions, there was still a lack of knowledge on "the cause, severity, and precise locations" resulting in the emergency services being deployed to incorrect locations (ibid., p.13).

The attacks occurring underground heightened the confusion and made communication difficult, if not impossible, for both the public and the emergency services. As mobile phones are unusable underground, the public were unable to contact the emergency services or friends or relatives to provide information on the incident. In addition to mobile phones being unusable, network congestion was an additional issue for the public and particularly the emergency services. For the public, the congestion meant that "survivors leaving the scenes were unable to contact their friends and family. People worried for their loved ones could not get through to them. Businesses could not communicate with their employees" (ibid., p.90). A study of Londoners in the weeks following 7/7 found that people who had difficulty in using their mobile to contact others during the attacks were significantly more likely to report experiencing substantial stress (Rubin et al., 2005). The communication issues and confusion also resulted in misinformation being provided to the media and ultimately the public who were initially informed that six attacks had occurred (London Assembly, 2006).

A final key issue related to the effectiveness of the response to 7/7 was concerned with supporting the needs of the public that had minor injuries or were uninjured in the attacks. The emergency services focus on the individuals "who are trapped and/or severely injured. That is why it is important that there are systems in place to meet the needs of those who are less seriously injured, or uninjured" (ibid., p.69). The London Assembly (2006) recommends that to meet these needs, a "survivor reception area" should be established close to the incident site, however, on 7/7 there was a failure to systematically establish survivor reception areas (ibid., p.69). This resulted in survivors leaving the areas of the explosions without having first provided their personal details or having received any support or advice (ibid.).

In terms of the public's immediate response to 7/7, research highlights how "rather than personal selfishness and competition prevailing, mutual helping and concern was predominant amongst survivors, despite the fact that most people were amongst strangers rather than affiliates" (Drury et al., 2009, p.84). This is an important finding as the public are typically the first to respond to an incident (Alexander, 2014). Whilst the public's immediate response was concerned with helping and concern, research undertaken with 1010 Londoners approximately two weeks after 7/7 found that 31% indicated having substantial levels of stress and 32% indicated that they would travel less by tube, train or bus into central London (Rubin et al., 2005). The attacks had a wider impact on public behaviour as "[r]etail sales fell 8.9% in the capital…shoppers and day-trippers kept their distance from the capital…and tube travel dropped substantially, by 10-15%" (Bux and Coyne, 2009, p.2939-2940). Thus, there is the need for governments and emergency management organisations to not only prepare communities for the short-term impacts of a terrorist attack but also for the "return to normal" and long-term recovery.

The Mumbai terrorist attacks, 2008

The Mumbai terrorist attacks began on 26th November 2008 and lasted approximately four days. The attacks were designed to cause maximum impact through the co-ordinated shooting and bomb attacks at multiple locations including hotels, a train station, restaurant, hospital, college, cinema and a religious building (Rodrigues, 2014). One hundred and sixty six people died as a result of the attacks and over 300 people were wounded (ibid.). Due to the wide variety of different targets, the attacks impacted upon different sectors and groups of society (ibid.).

A report examining the systematic failures of the Mumbai police's response found that both the administration and police officers were not prepared for the attack (Rodrigues, 2014). However, in comparison, Rodrigues (2014) highlights how the Taj hotel that was attacked had preventative measures in place prior to the attacks, including CCTV, security scanners and sniffer dogs, and was considered to have responded effectively. During the incident, the Taj "set up a war room, kept the community informed through a microsite and used senior managers to minimise collateral damage" (ibid., p.123). Following the attacks, the Taj focused on proactive communication and employee welfare by providing psychological support (ibid.).

The Anders Brevik attacks, 2011

The terrorist attacks by Anders Brevik in Norway during 2011 also involved bombings and shootings. On July 22 at 2.36pm, a bomb exploded in the centre of Oslo, "damaging the offices of the Norwegian Prime Minister…and the country's largest newspaper" (Buchanan, 2012). At 4.57pm, Brevik arrived at Utøya Island where a youth camp was being held by the Labour party (ibid.). Disguised as a police officer, Brevik began shooting at teenagers, which continued until 6.00pm when Brevik was apprehended (ibid.). The bombing and shootings resulted in the deaths of 77 people (BBC, 2012).

The attacks in Norway (2011) and Boston (2013) are examples of "lone-wolf" terrorism, whereby attacks are committed by individuals without a clear affiliation to terrorist groups. As outlined below, lone-wolf terrorism can have an impact on a similar scale to attacks carried out by larger terrorist groups. Due to advances in technology (e.g., weapons) and information (e.g., the availability of information over the internet) that will assist individuals, this type of terrorism is predicted to rise in the future (Simon, 2013a). Lone wolves are considered particularly dangerous as they work alone and have the freedom to do what they want without any restrictions (e.g., on the degree of violence) being imposed by others (Simon, 2013b). Working alone also means that these individuals are difficult to identify and capture as there are typically little or no communication with others (Simon, 2013b). The public's responsibility to help prevent lone-wolf terrorism is acknowledged. This responsibility is concerned with the public reporting "unattended packages" at potential target locations (e.g., airports, bus stations, shopping centres) (ibid.). Whilst Simon (2013b) recommends these measures specifically for reducing lone-wolf terrorism, they would also prevent other types of terrorist attacks from occurring.

Boston Marathon bombings, 2013

With 23,000 people participating in the Boston marathon on 15 April, 2013 (Eligon and Cooper, 2013), the Tsarnaev brothers clearly wanted to create a large impact. At 2.50pm the first bomb exploded, followed by a second explosion approximately thirteen seconds later (ibid.). The two bomb blasts resulted in the deaths of three people and injured 264 (Kreissl, 2014). The immediate impacts also included the closure of the surrounding neighbourhood and bus and train stops, the grounding of planes and the cancellation of events (Eligon and Cooper, 2013). These impacts were likely to be felt the next day as streets were closed to allow the crime scene investigation, random checks were to be made of the backpacks and bags of "transit riders" and planned events had been cancelled not just on the day of the attacks but for some time after (ibid.). Security was tightened at important locations in New York and Washington (ibid.), highlighting the far-reaching impacts of the attacks. Three days after carrying out the Boston Marathon bombings, Tamerlan and Dzhokar Tsarnaev were on their way to Times Square, New York to detonate a further six bombs in a suicide bombing, when they were caught by police (Gunaratna and Haynal, 2013).

The institutional response to the Boston Marathon bombings (2008) highlights how organisations were prepared for a terrorist attack of this nature. Kreissl (2014), outlines how "[w]ith regard to the immediate reaction of the emergency services we find a high level of competence and preparedness. First responders were on the spot and law enforcement personnel acted highly professionally" (p.127). This preparedness was a result of the planning that had been undertaken months in advance of the marathon. The Undersecretary for Homeland Security and Homeland Security Advisor, Kurt Schwartz (2013), outlines how;

> "On April 15, the public safety community was prepared. As we have done for many years, a multi-agency, multi-discipline team spent months developing the operational plans for this year's marathon. We did worst-case scenario planning, preparing for a wide array of incident and events that might impact the marathon or their communities" (p.7).

Related to planning, Schwartz (2013) attributes the effectiveness of the response to several factors, including:

- Investments in training, exercises, incident command systems and developing specialized capabilities
- The use of emergency operations centres
- The development of regional response capabilities
- Established mutual aid agreements
- Interoperability to ensure effective communication
- Cooperation and collaboration between agencies and jurisdictions
- The strong relationships with and support from Federal Government
- The involvement of the public in the response.

The Police Commissioner for Boston Police Department, Edward Davis (2013) also highlights the value of fully integrating international learning and training on terrorism as part of organisational preparedness. Thus, the organisational preparedness and response to the Boston Marathon bombings provides support for the findings of workshop 1, indicating that for terrorism, organisational rather than community preparedness is key.

In terms of the public's response, there was a brief period of panic and shock, followed by the public providing help and support to the rescue workers (Kreissl, 2014). Additionally, following requests by authorities on social media, the public provided information that had been collected on the suspects (ibid.; Papadimitriou et al., 2013). Davis (2013) outlines how "[t]he community plays one of the most important roles in our Nation's fight against terrorism. They contributed to the success, efficiency and safe resolution of the investigation by providing videos, photographs, information and sheltering in place". Preparing the public could contribute to them assisting the organisational response.

Cyber-terrorism

As outlined in D1.1, in April 2014 the UK Ministry of Defence published a report outlining how future terrorism could include cyber attacks. The potential for misuse of the internet and computer systems by terrorists is growing as society becomes increasingly dependent on them for carrying out everyday activities (e.g., communication, banking, etc.) (Archer, 2014). Additionally, as "more and more systems are interconnected and dependent on computer networks, new vulnerabilities appear that can be exploited by ill-intentioned individuals and groups" (Heickerö, 2014, p.555). In the 1990s, the term "electronic Pearl Harbor" was created to refer to potential cyber terrorism attacks (Weimann, 2004, p.2). Similar to terrorism, there is no widely agreed upon definition of cyber terrorism (Archer, 2014). However, this report uses the definition provided by Denning (2001) on how "cyberterrorism, refers to the convergence of cyberspace and terrorism. It covers politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage. An example would be penetrating an air traffic control system and causing two planes to collide" (p.241). Distinctions are made between 'pure' cyber terrorists who are planning to carry out attacks such as this and terrorists using the internet to co-ordinate their attacks (Heickerö, 2014).

This section and the scenario used in the second workshop, discussed in TACTIC Deliverable 4.2, will focus on 'pure' cyber terrorism. There are two contrasting perspectives on the future threat of cyber terrorism. For governments and security firms, the threat of cyber terrorism is considered "real and considerable, since vulnerabilities multiply when a number of different systems are increasingly integrated, controlled and run via computers" (ibid., p.555). This view is unsurprising considering that "command and control systems in critical infrastructure" are likely to be the target of future cyber attacks (ibid., p.555). Heickerö (2014) further highlights "financial systems, civilian air traffic, health care, and energy systems such as nuclear power plants" as potential targets of cyber terrorism (p.556). For scientists and analysts from universities and research institutes, the threat of cyber terrorism does not exist or is considered minimal (ibid.). This is related to the lack of known cyber attacks and the contradiction between terrorists using the internet to plan attacks and attacking a system that aids their planning (ibid.).

Whilst there are no existing known cases of cyber terrorism to draw lessons from for planning and preparedness, it is important to acknowledge the future threat of cyber terrorism. Hua and Bapna (2012) highlight how "[t]he reason cyber terrorists cannot launch attacks to cause significant damage is that these cyber terrorists have not gained the sufficient expertise, which could be available within the next few years" (Hua and Bapna, 2012, p.102-3). In addition to the threat of cyber terrorism increasing in the future, Weimann (2004) highlights the fear the threat causes.

> "From a psychological perspective, two of the greatest fears of modern time are combined in the term "cyberterrorism." The fear of random, violent victimization blends well with the distrust and outright fear of computer technology. An unknown threat is perceived as more threatening than a known threat. Although cyberterrorism does not entail a direct threat of violence, its psychological impact on anxious societies can be as powerful as the effect of terrorist bombs." (p.3).

Appendix B – London's Emergency Management Actors

The London Emergency Services Liaison Panel (LESLP) and the Metropolitan Police

The creation of the London Emergency Services Liaison Panel (LESLP) in 1973, initially consisting of the emergency services (Police, Fire and Ambulance), was concerned with improving emergency preparedness in London (Lewis, 2012). Today members of LESLP include "the Metropolitan Police Service, City of London Police, British Transport Police, the London Fire Brigade, the London Ambulance Service…local authorities…[t]he Port of London Authority (PLA), Marine Coastguard, RAF, Military and voluntary sector" (LESLP, 2012, p.5). The roles, responsibilities and responses of these organisations in relation to a major incident are outlined in a Major Incident Procedure Manual, now in its eighth edition, and discussed further in Section 2.3.3.

In addition to their roles highlighted in LESLP, the Metropolitan Police have responsibility for protecting London and the UK from the threat of terrorism through their Counter Terrorism command, known internally as SO15 (Mayor's Office for Policing and Crime, 2015a). The command's responsibilities relevant to TACTIC include:

- "Detecting, investigating and preventing terrorist threats and networks…
- Engaging, building and maintaining working relationships with boroughs, local communities, national and international partners to better understand their needs and to use their expertise and experience in jointly combating the terrorist threat.
- Working with communities, partners, institutions, groups and other agencies providing advice and support to tackle the ideologies that drive terrorism and extremism."

Whilst prior to 2014, the Metropolitan Police had responsibility for emergency planning, this responsibility was transferred to a hub with an emergency planning officer for each borough at the beginning of 2014. The data collected highlighted how currently the Metropolitan Police is responsible predominantly for counter-terrorism and in particular the PROTECT strand of CONTEST. In particular areas of London, the Metropolitan Police delivers advice, guidance and briefings to individuals, groups of individuals and large businesses (e.g., the media, councils, football stadiums, banks) on the things that they can do to make themselves more resilient to a terrorist attack. The briefings include a 7 minute DVD, Stay Safe, addressing what the public can do to prepare themselves in the event of a firearms attack.

The Metropolitan Police Service website outlines how "The threat from terrorism to the United Kingdom is real and serious. The Metropolitan Police Service has a key role in protecting London from that threat, but we need the help and support of all our communities" (Mayor's Office for Policing and Crime, 2015a). However, similar to the approaches outlined in Section 1.2.2, the website focuses on how the public can help the police to prevent, rather than prepare for, terrorism by reporting suspicious activity.

London Resilience Team

London Resilience Team (LRT) was established in early 2002 in response to a Government study examining London's preparedness to deal with an incident on a similar scale to the September 11th terrorist attacks (2001) (Greater London Authority (GLA), 2014). Initially part of the Government Office for London, the LRT included representatives from Local Authorities, the Emergency Services, utility companies and transport organisations. Based on the work of LESLP, LRT developed multi-agency plans and procedures for responding to an emergency in London. The 2004 CCA further broadened the responsibilities and work of the LRT. Since 2010, LRT was part of the Greater London Authority, discussed below. However, in February 2015, LRT confirmed that they had been transferred again to the London Fire and Emergency Planning Authority (LFEPA), who run the London Fire Brigade. LRT's role is to support the work of the London Resilience Partnership in order to make London more resilient (GLA, 2014). On a daily basis, LRT have the responsibility to:

- "coordinate the development of multi-agency capabilities, including emergency response and recovery plans
- facilitate meetings of the London Local Resilience Forum and other key partnership groups
- provide a liaison point between the London Resilience Partnership and central government, other Local Resilience Forum areas and internationally promote preparedness for emergencies, and raise awareness of risks
- maintain and update the London Prepared web pages" and Twitter account (GLA, 2014).

The data collected highlighted how LRT do not focus specifically on terrorism as this is the responsibility of the Metropolitan Police. Whilst generic (i.e., multi-hazard) preparedness tips are provided on the London Prepared web pages, information outlines how the public can help the police to defeat terrorism by reporting suspicious activity. Again, this highlights how actors in London focus on communities assisting them to prevent, rather than prepare for, terrorism.

London Resilience Partnership

The London Resilience Partnership was also created in 2002 and is a coalition of organisations who are involved "in preparing, responding and recovering from emergencies in London" (London Resilience Partnership, 2013). As 15 shows, the London Resilience Partnership consists of over 170 organisations and includes both Category 1 and Category 2 responders (London Resilience Partnership, 2013, p.23).

Table 15 Category 1 and 2 Responders forming the London Resilience Partnership

London Resilience Partnership Organisations	
Category 1 Responders	**Category 2 Responders**
Emergency services: British Transport Police City of London Police London Ambulance Service London Fire Brigade Maritime Coastguard Agency Metropolitan Police Service	Utilities: Affinity Water BT Essex & Suffolk Water Level 3 Communications National Grid 02 Scottish and Southern Energy Southern Gas Networks Sutton & East Surrey Water Telehouse Europe Thames Water Utilities Limited UK Power Networks Vodafone and Cable and Wireless Worldwide
Strategic London Government: Greater London Authority	Health Bodies: Clinical Commissioning Groups x32
Local Authorities x33	Transport: Heathrow Highways Agency National Air Traffic Service Network Rail

	Port of London Authority London City Airport Transport for London (incorporating) London Buses London Underground Limited Street Management Docklands light Railway London Overground London Tramlink Crossrail (once operating) London River Services
Heath Bodies Acute Trusts NHS England Public Health England	Government Agencies: Health and Safety Executive
Government Agencies: Environment Agency	
Other Responders: Airwave Department for Communities and Local Government (DCLG) Military Voluntary sector Business sector Faith sector	

The mission of the Partnership is to make London a resilient city, which involves the following tasks:

- "assessing risks to London's resilience
- building resilience through prevention and mitigation
- working together to prepare, respond & recover
- helping Londoners to be prepared" (London Resilience Partnership, 2013, p.4).

One of the 'core' functional capabilities underpinning the work of the London Resilience Partnership (2013) is "[c]ommunicating with the public" (p.8). This capability is concerned with ensuring that the people who live, work and visit London have an awareness of the risks in London and how to prepare for these risks. In terms of an actual emergency, people should also be given information that is accurate and timely. The London Resilience Partnership Strategy document (2013) includes a Delivery Plan for 2013 – 2015 for achieving the mission of making London a resilient city. Activities and measures related to TACTIC and community preparedness include:

- publishing a public version of the London Risk Register[13]
- championing resilience and measures that enhance public awareness and preparedness
- encouraging communities to undertake preparedness actions
- increasing social media followers and website visitors
- promoting London resilience partners initiatives designed to increase community resilience
- working with the London business community to ensure they are risk aware and have developed effective business continuity plans

[13] London Resilience Partnership, London Risk Register, February 2015. [Online]. http://www.london.gov.uk/sites/default/files/London%20Risk%20Register%204.0.pdf. (Accessed 23 March 2015).

Thus, whilst actors may not focus specifically on increasing preparedness for terrorism in London, they are required to enhance preparedness for multi-hazards. Additionally, it is not only members of the public that are the focus of preparedness strategies, but also businesses within the community.

Greater London Authority, the Mayor of London and the London Assembly

The Greater London Authority (GLA) was established in 2000 and is a form of government consisting of the Mayor of London, the London Assembly and non-political staff (London Elects, 2012). Chapter 9 of Emergency Preparedness, covering part 1 of the 2004 CCA, focuses on London. The document outlines how the GLA is classified as a Category 1 responder and that "the Mayor of London plays a full part in …improving the preparedness of the capital" (p.3). The emergency management roles of the GLA and the Mayor of London (Cabinet Office, 2012, p.11), include:

- engaging in high-level discussions and decisions concerning managing emergencies in London
- chairing the Local Resilience Forum (or appointing a deputy)
- contributing "as necessary to the pre-informing of Londoners about the content of emergency plans, the correct behaviour in an emergency and good practice in terms of preparedness in the home, as part of initiatives organised both locally and at the UK level"
- preparing to have a key role in terms of warning and informing the public in London during an emergency
- having responsibility for civil protection issues related to managing Parliament and Trafalgar Squares

The London Assembly consists of 25 elected members who act as a "watchdog", holding the Mayor accountable in terms of strategy, decisions and actions (London Elects, 2012). The Assembly have opportunities to quiz the Mayor and officials concerning their responsibilities including those covering emergency planning.

Local Resilience Forums - London Resilience Forum and Borough Resilience Forums

The CCA discussed in Section 2.1, resulted in the establishment of 42 Local Resilience Forums across England and Wales (Cabinet Office, 2011). The Forums are based on police areas and consist of Category 1 and Category 2 responders (GOV.UK, 2013). The duties placed on responders under the CCA may be exercised through the Local Resilience Forums (Cabinet Office, 2011). For instance, Category 1 responders are required to prepare a community risk register, however, this must be delivered collectively through the Local Resilience Forum. The Local Resilience Forums were created "to ensure effective delivery of those duties under the Act that need to be developed in a multi-agency environment" (Cabinet Office, 2011, p.13). The requirement for Local Resilience Forums to meet a minimum of at least once every six months means that the responders have the opportunity "to collaborate and co-operate with each other" (Cabinet Office, 2011, p.23). Local Resilience Forums must also work with neighbouring Local Resilience Forums to develop and exercise generic response plans in order to be prepared to respond to large-scale emergencies. As examined in Section 1.3 and Appendix A, many past terrorist attacks involved multiple attacks and have the potential to be large-scale emergencies that impact upon multiple areas.

The Local Resilience Forums should result in:

- The development of a Community Risk Register

- Category 1 responders addressing policy related to: risk, emergency planning, business continuity management, publishing information on risk assessments and plans, warning and informing the public and other civil protection duties (e.g., promoting business continuity management
- Support for preparing multi-agency plans, protocols and agreement and the co-ordination of multi-agency exercises

Mostly, the frameworks and duties falling under the CCA apply to London as they do to everywhere else (Cabinet Office, 2012). However, there are differences and aspects that are unique to London, including:

- The establishment of a pan-London Local Resilience Forum, previously named London Regional Resilience Forum, that covers all of London and that incorporates the Metropolitan Police and City of London Police areas. However despite the Forum's existence, the data highlighted inconsistences in the preparedness strategies across the 33 London boroughs.
- For each borough of London, a Borough Resilience Forum that meets a minimum of once every six months for more local level planning. The Borough Resilience Forums were introduced to "facilitate co-operation and information sharing at the operational level between local authorities and the emergency services" (Cabinet Office, 2012, p.5).
- Local authorities being supported in undertaking their duties falling under the CCA by the London Fire and Emergency Planning Authority (LFEPA). LFEPA has responsibility for maintaining the arrangements relating to the local authority 'Gold', the control centre, training programmes and annual exercises.

Table 16 outlines in more detail the roles and responsibilities of London's Local Resilience Forum and the Borough Resilience Forums (Cabinet Office, 2012).

Table 16 Roles and responsibilities

Level	Role and Responsibilities
London Local Resilience Forum	• Providing strategic high level direction for multi-agency planning in London • Ensuring that London is prepared to respond to a variety of different incidents including terrorist attacks, the impacts of climate change and pandemics • Agreeing strategic and policy approaches concerning London's preparedness and response • Producing and maintaining the London Risk Register (discussed in Section 2.4) • Enabling information on risk management, threats and hazards to be shared across local, sub-national and national organisations • Ensuring that plans, procedures, training and exercises are in place • Improving co-ordination across London • Reviewing and recommending the key members of the Borough Resilience Forums • Approving the Borough Resilience Forums Risk Registers
Borough Resilience Forums	• Multi-agency emergency planning based on the local risks and needs

In addition to the actors preparing communities for multi-hazards in London, it is important to note that the Home Office lead a CBRN workstream (Cabinet Office, 2011). The "CBRN Resilience Programme seeks to build and improve the UK's ability to respond to and recover from a terrorist CBRN attack, and as part of this programme the Government has equipped 18 sites nationwide with trained officers to improve the multi-agency response to an attack" (Cabinet Office, 2011, p.45). Thus, whilst actors may not be preparing communities for the particular threat of terrorism, they are preparing themselves to respond to a terrorist attack.

Appendix C – Workshop: list of participating organisations

- BBC College of Journalism
- British Red Cross
- European Dynamics
- Helmholtz Centre for Environmental Research – UFZ
- Living Streets King’s Cross local group
- London First
- London Metropolitan University
- Metropolitan Police (Borough level)
- Northumbria University
- Saxon State Office for the Environment, Agriculture and Geology - LfULG
- Trilateral Research and Consulting
- University College London

Appendix D – Workshop agenda

TACTIC

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

Workshop 1 for Case Study 1: Terrorism in Europe

London, 10 February 2015

Timings	Session
9.00-9.30	Registration
9.30-9.35	**Trilateral Research and Consulting** • Welcome
9.35-10.00	**Helmholtz Centre for Environmental Research - UFZ** • Overview and background to the TACTIC project • Briefly introducing the community preparedness audit 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 web-based platform
10.00-10.30	**Trilateral Research & Consulting** • Overview of the case study on terrorism ○ Examining how preparing for terrorism is different to preparing for other types of disaster? ○ The terrorism scenario
10.30-11.30	Group work 1 – Discussing and developing the audit, addressing: • Participants expectations of the audit • What should be included in the audit? • How can participants benefit from the audit? • Strengths and weaknesses of the audit
11.30-11.45	Tea and coffee break
11.45-12.45	Group work 1 continued and feedback to the group (emphasising the strengths and weaknesses of the audit and suggestions on content and structure)
12.45-13.45	Lunch
13.45-14.00	**Helmholtz Centre for Environmental Research - UFZ** • Overview of the catalogue of good practices for education
14.00-15.00	Group work 2 – Discussing and developing the catalogue of good practices for education (What types of material and practices are needed to increase preparedness for terrorist attacks?)
15.00–15.20	Tea and coffee break
15.20–16.30	**European Dynamics** • Linking the audit and good practices to the framework for improving community preparedness and the web-based platform • Discussion for improving the platform
16.30-17.00	**Trilateral Research and Consulting** • Next steps and discussion surrounding the 2nd workshop