SEVENTH FRAMEWORK PROGRAMME

Collaborative project
Small- or medium-scale focused research project
FP7-SEC-2011-1
Grant Agreement no. 285533

TACTICS

Tactical Approach to Counter Terrorists in Cities

Deliverable details	
Deliverable number	D8.2
Title	Policy and strategic impacts, implications and recommendations
Author(s)	RAND Europe PRIO ISCA
Due date	31 August 2015
Delivered date	31 August 2015
Dissemination level	PU
Contact person EC	PO

Cooperative Partners	
1.	ITTI Sp. z o.o.
2.	Nederlandse Organisatie voor toegepast natuur-wetenschappelijk onderzoek (TNO)
3.	Peace Research Institute Oslo (PRIO)
4.	RAND Europe
5	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
6	Universitat Politècnica de València (UPVLC)
7	Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V.
8	Koninklijke Marechaussee
9	International Security and Counterterrorism Academy (ISCA)
10	Morpho
11	LERO

Table of Contents

List of abbreviations

ACPO (TAM)	Association of Chief Police Officers (Terrorism and Allied Matters)
AFSJ	Area of Freedom, Security and Justice
AIT	Advanced Imaging Technology
ANPR	Automatic Number Plate Recognition
API	Advanced Passenger Information
ATC	Authority to Carry
BIA	Border and Immigration Agency
CAA	Civil Aviation Authority
CCTV	Closed-Circuit Television
CEPOL	[European police college]
CM	Capability Manager
CMT	Capability Management Tool
DHS	Department of Homeland Security
DPD	Data Protection Directive
ECHR	European Convention on Human Rights
ETF	Electronic Test Facility
EU	European Union
Eurojust	[the European Union's judicial cooperation unit]
Europol	[the European Union's law enforcement agency]
EXCON	Exercise Control
FAA	Federal Aviation Authority
FEX	Field Exercise
GPS	Global Positioning System
GTD	Global Terrorism Database
HMRC	Her Majesty’s Revenue and Customs
IED	Improvised Explosive Device
JBOC	Joint Borders Operations Centre
LIBE	Committee on Civil Liberties, Justice and Home Affairs

NBTC	National Border Targeting Centre
OECD	Organisation for Economic Co-operation and Development
PDCS	Pre-departure Checks Scheme
PIRA	Provisional Irish Republican Army
PIU	Passenger information Unit
PNR	Passenger Name Record
RIPA	Regulation of Investigatory Powers Act 2000
TACTICS	Tactical Approach to Counter Terrorists in Cities
TDM	Threat Decomposition Manager
TDT	Threat Decomposition Tool
TFEU	Treaty on the Functioning of the European Union
TM	Threat Manager
TMT	Threat Management Tool
TRL	Technology Readiness Level
TSA	Transportation Security Administration
UAV	Unmanned Aerial Vehicle
UK	United Kingdom
UKAB	United Kingdom Airport Board
US	United States

Acknowledgements

We are enormously grateful to the experts who took part in interviews, without which this report would not have been possible. Their affiliations and, in most cases, their names are listed in Appendix 1; some interviewees' identities have been anonymised at their request. We would also like to thank the participants in our validation workshop for their valuable insights and feedback on emerging findings.

We owe a particular debt of gratitude to Dr Chris Giacomantonio and Dr James Fox, our peer reviewers who are part of RAND's quality assurance process and whose comments improved the content of the report. We are also grateful to our colleagues Alexandros Kokkoris and Dylan Marshall for their support in transcribing interviews, and to Laurine Freylone for her assistance in the case study research.

Executive summary

In recent years the threat of terrorism in urban environments has become an important issue, emphasised by several successfully carried out terrorist attacks (New York, Madrid, London, Copenhagen and Paris are just some examples). When security forces are alerted to a specific terrorist threat, their main goal is to prevent an actual attack. On the other hand, if prevention fails and the attack is carried out, independent of the degree of success, security forces become responsible for stopping it and mitigating its consequences. In both cases, the efficiency and effectiveness of the response relies on three key pillars:

1. Ability to **respond quickly**, without bias in decisionmaking, enabled by specific and precise requests for information and clearly issued orders.
2. Ability to **decompose threats** into observable terrorist behaviours specific for urban environments to enable an increased level of preparedness by security forces.
3. Ability to efficiently and effectively **manage capabilities**.

TACTICS is an FP7 project commissioned by the European Commission in 2012 to develop mid technology readiness level (TRL5, Proof of Concept) decision support technology to assist security forces in countering terrorist threats in urban environments. The system that was developed as part of this project brings an innovative approach built around the three core capabilities described above. The acronym stands for **T**actical **A**pproach to **C**ounter **T**errorists **i**n **C**ities. Conceptually, it can be defined as a counterterrorism decision support technology designed to facilitate a clearer understanding of both the threat and the capabilities available to counteract it, enabling a faster, more efficient and effective security force response.

Technology has played, and will continue to play, a central role in counterterrorism policy, strategy and operations. Recent years have seen rapid innovation and the development of new technological applications, such as facial recognition and biometrics, counter-IED, communications interception, airport security, explosive and weapon detection, and so on. This report analyses eight case studies of counterterrorist technology implementation in order to extract lessons that can be applied in the context of deploying a TACTICS-like system in Europe. Furthermore, it presents a series of lessons extracted from relevant case law.

There are a number of challenges that policymakers face today in the ever-increasing reliance on technology for countering terrorism in Europe. These include:

- The level of engagement with the communities affected by the technology implementation;
- The effectiveness of counterterrorism measures;
- The resources dedicated to counterterrorism;
- Achieving an appropriate balance between privacy and security;
- Data sharing challenges; and
- Respect for criteria of legitimacy, necessity and proportionality.

Based on the research, the report proposes the following recommendations:

Recommendation 1: Deploy appropriate counterterrorism technologies that enhance decisionmaking, but be prepared for ongoing changes in the technology landscape

As is evident from the TACTICS project, technologies clearly have the potential to enhance the effectiveness of CT activities, provided they are appropriate for the use to which they are put and they are deployed and operated correctly. The technologies can, as demonstrated by the TACTICS system, introduce access to a wealth of additional information to improve the decisionmaking of end users during a time-critical situation. Furthermore, the technology itself can be used to prompt the user to consider whether cognitive biases have been introduced into the process, and whether the human operator needs to consider alternatives, thus reducing the risk of error and unwanted consequences. The human operator will, however, continue to be the most important element of the CT operations, because critical decisions must remain human decisions. Once more, technology can support the decisionmakers and ensure there is a full record of their use of it, the decisions they have made and the rationale behind them.

- **Future considerations are necessary.** The threat from terrorist attacks is becoming increasingly sophisticated as terrorists develop new ways to carry out attacks and use new technology itself to do so. As the case of body scanners highlights, it is necessary to continue to enhance developed technologies to overcome their potential technical limitations against new threats or the terrorists' exploitation of any limitations associated with existing technologies.
- **Over-dependence on technology can be problematic.** Unmitigated dependence is a good definition of vulnerability. In CT it might seem contrary to common sense that reliance on technologies as listed above could in itself represent a vulnerability, but this is precisely the case. If a security system relies, for example, on a very high level of communications intercept technology, then the terrorist adversary might respond by using 'low-tech' means. If highly developed systems fail for innocent infrastructural reasons, will there always be sufficient and effective 'reversionary modes' to hand? Over-reliance on technology in CT could be a double-edged sword simply because it might be based upon a complacent and simplistic understanding of the relationship between technology and security policy – for example, that the benefits of the former belong exclusively to those who believe they dominate the latter.

Recommendation 2: Apply a structured approach to deployment of counterterrorism technology

We propose the need to apply a structured deployment process with particular emphasis on the respect for national and European legislation and on the definition and respect for appropriate safeguards (as described in full detail in TACTICS deliverable D8.1 – TACTICS Deployment Strategy). The recommended deployment strategy has two key elements: first, a step-by-step deployment process that guides relevant decisionmakers in member states through a series of critical decision points, and, second, a deployment checklist covering the full range of factors (contextual and environmental, organisational and regulatory, technical and infrastructural, human, legal and ethical) that decisionmakers should consider in their decisionmaking process. The combination of these two elements ensures that the scope and purpose of the system are clear from the start and that requirements for the technology are well understood and compatible with existing structures, infrastructures, laws and regulations. In addition, the proposed structured approach prompts decisionmakers to consider not only the operational effectiveness of the technology, but also its ethical use, including its impact on local communities and its compliance with the principle of proportionality.

Recommendation 3: Carefully consider data collection and data sharing

Trusted partnerships, national and international, are by definition a prior necessity for effective data sharing. Where it is not possible to harmonise and/or share the data sources, it is recommended to work first towards standardising the data assumptions and taxonomies to facilitate potential future sharing of data structures and content. As demonstrated in the case of ANPR, it is vital to ensure that the need for mass collection of data is proportionate, necessary and justified. Similarly, the case of body scanners illustrates how to encourage the institution of an oversight mechanism – in this case one that monitors how body scanners collects and uses its data. This is particularly pertinent when there are issues of data sharing without guaranteeing protection of citizens' rights, or where there is a disproportionate data retention period (e.g. as evidenced in the PNR case study).

- Previous deliverables in TACTICS highlighted the need for the technology to be able to deal with specific urban environments, which may lend itself to different data requirements and outputs and which, in turn, may cause difficulties with regards to data sharing initiatives, not only between national agencies but also across international borders.

Recommendation 4: Deal early with considerations around privacy

It is recommended that when policy-makers consider the introduction of new technologies in the context of CT, they **identify** and **address** potential privacy issues as early as possible. As we have seen from the technologies in the case studies and in the TACTICS systems itself, the balance between privacy and security is pertinent. The case studies also demonstrate that there are civil liberties implications for whole communities, e.g., Project Champion or Ring of Steel. It is therefore recommended that impact assessments be undertaken on any community into which they are introduced or where they are used as early as possible, to determine what the potential impact of the intervention may be on the community and how it can be mitigated or removed. It should be noted that in early product development, it is possible to build in **privacy by design** in the development process (see D6.2 for further elaboration about the use of privacy by design) and this, too, should be incorporated from the very beginning. It is much easier to implement this upfront than to retrospectively fit in privacy measures.

- Despite the rhetoric of win–win in the context of protecting privacy and enhancing counterterrorism measures, the discrepancy between privacy and security can be wide and present a tricky balance for policy-makers to manage. Building in these considerations to the wider deployment strategy (see D8.1) and holding relevant parties to account for addressing them may be an appropriate approach to begin to tackle the issue.
- Policy-makers may also need to consider the impact on the local urban environment. Surveillance and overly controlling security measures potentially prevent people from enjoying the benefits that the urban environment has to offer. As D4.3 emphasised: 'While TACTICS as a system is promising in terms of improving the citizens' security in urban areas, it is necessary to accompany the development of the system with a level of critical awareness of the weaknesses and potential unintended consequences of such systems.'

Recommendation 5: Establish relevant partnerships and networks

Countering terrorism requires partnerships within all levels of national government, law enforcement agencies, private sector and the communities, as well as an integrated approach in collaboration with international partners and key allies. Partnership with citizens is equally important, as we have seen in the range of acceptance of the CT technologies in the case studies. Citizens need to be informed of the threat in an honest, straightforward manner to foster a deeper understanding of why particular actions are needed in response to the threat. Where possible, the involvement of relevant citizens in other forms of pre-deployment assessments could prevent potential issues later on in the deployment process. Multilateral fora can be established and nurtured in order to initiate and sustain dialogue and understanding, leading to an integrated approach to counterterrorism.

- While the idea of partnership of end users around design and development of new technologies in the context of CT may also be beneficial for reasons of cost and harmonisation of technology, there may be difficulties around this, particularly because the technology specification requirements differ between different end users.
- The first and most obvious challenge to European member states is that of establishing **trusted relationships** between governments and security agencies such that intelligence, early warning and analysis of terrorist threats can all be shared in a timely fashion. These trusted relationships must also be routinized, rather than require reinvention on a case-by-case basis. Unless it can be shown that it will add to the strength and security of participating member states, collaboration in this most delicate and closely-guarded area of national security policy will remain difficult and will yield little tangible benefit. But if trusted relationships can be formed then the path is open to address the next set of challenges to collaboration. These are of a more material nature, but no less taxing: can member states **cooperate** in their response to a terrorist threat? Can procedures, equipment and finances be shared? Could member states agree a set of **common standards**? And might it even be possible to agree a level of **role specialisation** among EU member states with, for example, some governments concentrating on the financial aspects of CT while others specialise in 'kinetic' operations?

Recommendation 6: Carry out regular audits and evaluations on the system use

The research indicates the need to introduce evaluation of the use of the technology on a regular basis. This is particularly important after each use of the TACTICS system, both to ensure that the system is effective, proportionate and thus necessary in relation to its purpose, and to further tune it to future use. In order to ensure that the technology is operationally effective in the context of counterterrorism, it is necessary to establish an approach to evaluating the use of the approach with regards to its effectiveness to meet its purpose. Another main benefit of undertaking evaluations is the potential to flag up capability needs as a result, in terms of either systems performance or operator/manager training needs. As identified in previous TACTICS deliverables, there is scope for using a TACTICS-like system for training purposes, and this would aid in the evaluation of the system.

Furthermore, if the system allows for access to personal data or introduces privacy issues in its use, the conduct of internal and/or external audits of the system use is recommended. As identified in the PNR case study, there is a need to establish appropriate mechanisms for independent review, potentially through the appointment of data protection officers. The presentation of reports also permits ensuring a transparent use of the system and, in turn, maintains a high level of trust from the community.

Evaluation is often seen as retrospective analysis of a project, programme or policy to assess how successful or otherwise it has been, and what lessons can be learnt for the future – in other words, it is

something that should happen after a programme has been implemented. In this report we argue that although post-implementation assessment is the ultimate goal of evaluation, for an evaluation to be most robust, the evaluation design element should be part of the policy programme from the outset of any new initiative and should be carefully designed alongside the monitoring system.

1 Introduction

1.1 What is TACTICS?

1.1.1 TACTICS as a new concept[1]

In recent years the threat of terrorism in urban environments has become an important issue, emphasised by several successfully carried out terrorist attacks (New York, Madrid, London, Copenhagen and Paris are just some examples). When security forces are alerted to a specific terrorist threat, their main goal is to prevent an actual attack. On the other hand, if prevention fails and the attack is carried out, independent of the degree of success, security forces become responsible for stopping it and mitigating its consequences. In both cases, the efficiency and effectiveness of the response relies on three key pillars:

4. Ability to **respond quickly**, without bias in decisionmaking, enabled by specific and precise requests for information and clearly issued orders.
5. Ability to **decompose threats** into observable terrorist behaviours specific for urban environments to enable an increased level of preparedness by security forces.
6. Ability to efficiently and effectively **manage capabilities**.

TACTICS is an FP7 project commissioned by the European Commission in 2012 to develop low technology readiness level (TRL) decision support technology to assist security forces in countering terrorist threats in urban environments. The system that was developed as part of this project brings an innovative approach built around the three core capabilities described above. The acronym stands for **T**actical **A**pproach to **C**ounter **T**errorists **i**n **C**ities. Conceptually, it can be defined as a counterterrorism decision support technology designed to facilitate a clearer understanding of both the threat and the capabilities available to counteract it, enabling a faster, more efficient and effective security force response.

1.1.2 TACTICS as a 'system of systems'

From a more practical point of view, TACTICS consists of three main elements:

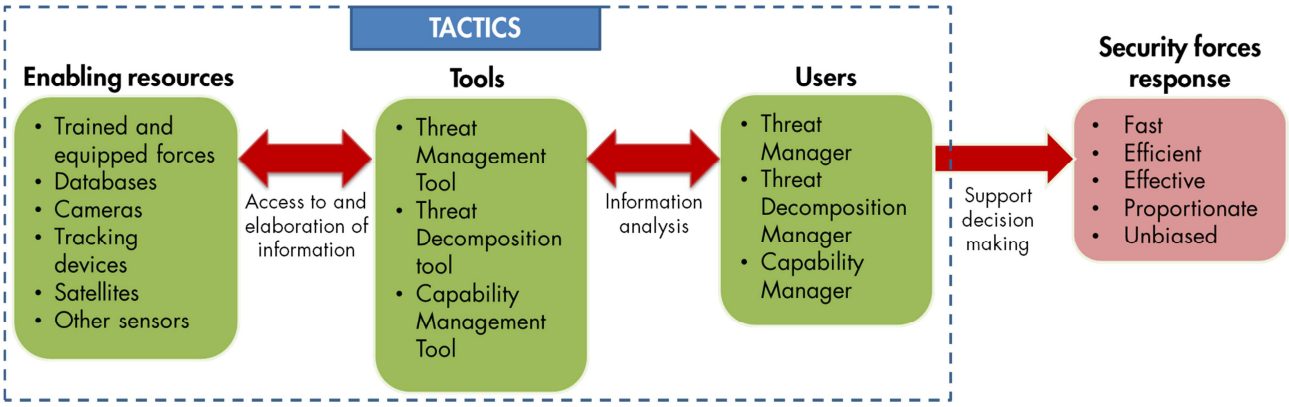
1. A team of trained users with specific roles and responsibilities;
2. A software-based set of tools to be installed either on existing systems or on dedicated terminals/workstations;
3. A set of pre-existing enabling resources (e.g. databases, cameras, unit tracking devices and other sensors) that the tools can access to obtain the required information.

In TACTICS, the system tools (a) allow the users to easily access and elaborate information from different sources/resources and (b) support the analytical process that underpins decisionmaking.

This basic operating concept is illustrated in figure 1. More information on TACTICS' architecture is provided in the following section.

[1] For more information on TACTICS conceptual framework, please refer to project deliverable D3.1, *White paper with the conceptual framework including interoperability with the systems context*, available on the project's website, http://www.fp7-tactics.eu/index.html

Figure 1. TACTICS basic operating principle



Source: RAND Europe analysis

1.1.3 TACTICS system architecture[2]

TACTICS includes three main software-based tools and three associated managers:

- Threat Management Tool (TMT) and the associated Threat Manager (TM)
- Threat Decomposition Tool (TDT) and the associated Threat Decomposition Manager (TDM)
- Capability Management Tool (CMT) and the associated Capability Manager (CM)

The three managers are responsible for managing the use of the tools by specialised operators in order to generate a clear operational picture to support decisionmaking. In particular:

- The purpose of the **Threat Decomposition** process is to improve preparedness of security forces by decomposing threats into observable terrorist behaviours specific to urban environments. As the main actor in this process, the **Threat Decomposition Manager** is responsible for providing, for example, information on terrorist groups and their *modus operandi*.[3]
- The purpose of **Capability Management** is to improve (a) awareness about the general availability of capabilities most appropriate in a given situation, (b) access to capabilities, and (c) management of capabilities. This is done by automatically matching indicators of a potential threat to available capabilities (e.g. security staff, surveillance cameras). The **Capability Manager** will then be able to activate the Threat Manager upon request.[4]
- Based on the information provided by the TDM and CM (as well as by other external security agencies), the **Threat Manager** will be in a position to respond to the situation at hand in the most timely, effective, efficient, proportionate and unbiased way.

Figure 2 provides a quick overview of the system architecture.

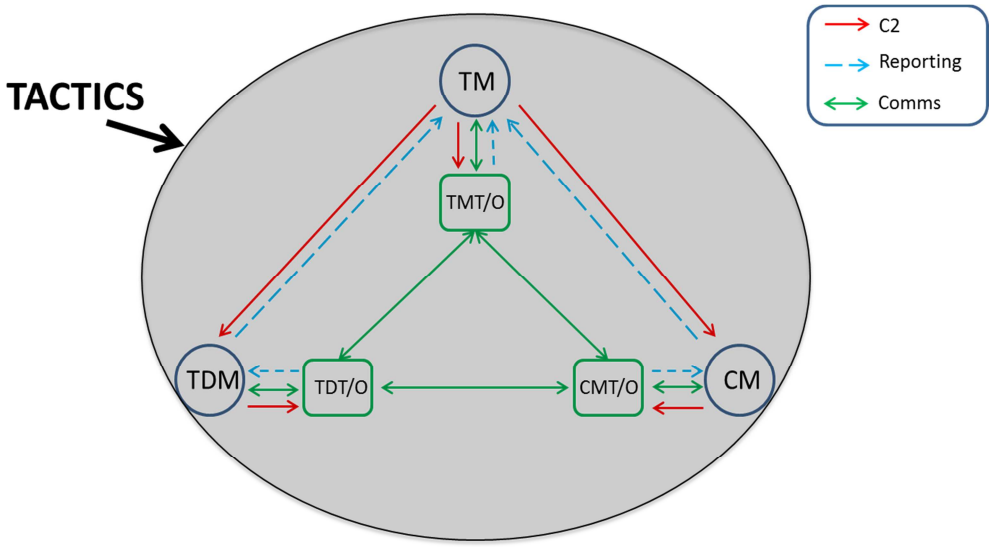
---

[2] For more information on TACTICS' system architecture, see D3.2, *System architecture: Design patterns and interfaces*, available on the project's website, http://www.fp7-tactics.eu/index.html

[3] TACTICS D3.1, p. 4

[4] Ibid.

Figure 2. Overview of TACTICS architecture: Three managers and three tool operators



1.2 Overview of TACTICS research approach

TACTICS development followed a structured approach comprising of nine work packages (WP).[5] The substantive WP of the projects can be summarised as follows:

- **WP 2 User Requirements & Scenario Definition**: the goal of this work package was to define urban environments and threat scenarios based on up-to-date end user needs and requirements.
- **WP 3 System Design**: this WP aimed at creating the conceptual framework for TACTICS, including the relations with the context of the system and methods. It also specified the design patterns to be used in WPs 4–6 and as well as the architecture.
- **WP 4 Threat Decomposition**: this WP aimed at (1) generating terrorist behaviour models in order to feed into the development of the Threat Decomposition Tool. The models were based on a compendium of previous attack profiles; (2) developing the Threat Decomposition Tool; (3) exploring privacy, ethics and human rights issues related to counterterrorism (CT) in urban environments.
- **WP 5 Capability Management**: the goal of WP 5 was to develop the Capability Management Tool capable of (1) generating a list of currently deployed capabilities in a specific area; and (2) automatically matching needs (based on the threat) and available capabilities.
- **WP 6 Threat Management**: the outcome of this work package was the Threat Management Tool, which will integrate and fuse the information flows from different sources, such as sensors (e.g. cameras, first responders' global positioning system [GPS] positions), the Threat Decomposition Tool (WP 4) and the Capability Management Tool (WP 5).
- **WP 7 Validation**: the goal of this work package was to design and conduct a series of validation events using scenario-based exercises to simulate the response to a known specific threat or an actual terrorist attack with the use of TACTICS. The data gathered during these events was then used to generate a TACTICS implementation manual and inform the preparation of the cross-European deployment strategy and policy recommendations in WP 8.
- **WP 8 Deployment Strategy and Policy Recommendations**: this WP aimed at (1) determining the strategy required to deploy the project into a live environment (deployment strategy) and (2) producing a series of policy recommendations (with their impacts and implications) in order to enable policy-makers to formulate directions concerning the development, deployment and operation of TACTICS in the context of the European Union (EU).

[5] Descriptions of WP 1 and WP 9, respectively covering project management and dissemination aspects, are not relevant for the purpose of this report and are therefore not included in this section.

The present report is the culmination of the three-year project, which has included a number of deliverables to date. A full list of project deliverables can be found in Appendix D. Those that are in the public domain can be found on the project website, http://www.fp7-tactics.eu/

1.3 Aims and objectives of D8.2

> The goal of this report is to present a series of policy recommendations to assist policymakers in the development, deployment and operation of TACTICS in the EU context

The questions this deliverable seeks to address are:

(1) What is the European Union policy **landscape** in which a TACTICS-like system may come to be deployed?

(2) What can be **learnt** from 'best practices' and lessons with regards to introduction of comparable systems?

(3) Given the policy landscape and lessons, what are the main **policy issues** and **implications** of the operational deployment of TACTICS in a cross-European context?

The ultimate goal is to support decisionmakers and operators in being able to deal with potential terrorist incidents such that the urban environment is resilient to a terrorist attack. The aim of the research for this deliverable is thus to present the European landscape in which TACTICS might be deployed, with particular emphasis on human rights and the rule of law. Furthermore, the aim of the research was to identify lessons associated with introducing a system such as TACTICS in the context of counterterrorism. Finally, drawing on implementation case studies, this research extract out a number of policy recommendations.

The intended audience for this report is therefore predominately policy-makers engaged with counterterrorism and with procurement of technologies to support end users.

1.4 Structure of the deliverable

In this report, we first present the European policy landscape (chapter 2). We then present the methodology that was applied in order to identify the lessons for policy-makers with regards to the introduction of a 'system of systems' in the context of counterterrorism in Europe (chapter 3). Chapter 4 summarises findings from previous deliverables from the TACTICS project with implications for WP 8. In the subsequent chapter (chapter 5), we present the findings from a number of case studies on technology implementations. Finally, chapter 6 presents the policy implications for European policy-makers considering the deployment of a system such as TACTICS.

2 EU policy landscape in the field of counterterrorism

Counterterrorism efforts have traditionally been at the core of states' activities, as an expression of sovereign powers and a crucial element of national security. Yet, counterterrorism has become one of the areas where European cooperation has been the most pressing, and a field that has shaped European politics and governance in recent years.

Nowadays, counterterrorism policymaking stands at a crossroad. On the one hand counterterrorism remains primarily in the competence of EU member states, while at the same time being actively shaped by the European Union (e.g. through the development of new tools and the continuous intervention by different institutions). On the other hand, counterterrorism efforts in different ways touch on areas of cross-border police cooperation, external border control, crime and policing, and immigration and asylum, areas where states remain the most eager to retain their sovereign prerogatives.[6] Moreover, European efforts in counterterrorism have had to face the challenge of widely differing understandings of what terrorism means and of different historical experiences across the EU member states.

The European dimension of counterterrorism highlights a series of tensions that have always underlain these activities, notably the relations among different institutions (national and supranational) and the relations between security practices and human rights. For example, the European Commission has been proactive in fostering more EU integration in the field, and so has the European Parliament, both to defend its position in EU policy-making and to influence the substance, notably by stressing the importance of civil liberties, data protection and ensuring proportionality in the security responses. While often being sidelined prior to the Lisbon Treaty, the European Parliament has rather softened its stances on data protection and civil liberties after Lisbon, allegedly out of concerns to not lose credibility in decisionmaking processes.[7]

In the following pages, we present the main cornerstones which defined and still shape the current policy landscape in the so-called EU area of freedom, security and justice. This overview is crucial to understand the landscape in which TACTICS tools are to be further developed and eventually deployed. In this analysis of the EU policy landscape in the field of counterterrorism, we also include a brief introduction to the fundamental rights dimension. In particular, we present the main elements and developments of data protection, which has become a key issue in the field, both at the national and the European level. Emphasis on data protection and other fundamental rights is also crucial to ensure a legally, politically and socially sound and acceptable deployment of TACTICS tools in the future.

2.1 Counterterrorism and the construction of the European Area of Freedom, Security and Justice concept

A TACTICS-like system is designed to operate at the local (urban) level, maximizing local capabilities and competences, and it does not necessarily imply the setting up of a pan-European structure. In other words, it is reasonable to assume that a TACTICS-like system may be thought of as a tool designed and deployed by national authorities. However, even if the policy decision concerning a TACTICS-like system had to be taken only at national level, the current development of the EU area of freedom, security and justice (AFSJ) would oblige national policy-makers to take into account the European panorama. For this reason, this sub-chapter presents the main features of this landscape, in terms of guiding policies, strategies and available instruments.

The AFSJ concept was first introduced in the **Amsterdam Treaty**, signed in May 1999.[8] It stated that the EU must 'maintain and develop the Union as an area of freedom, security and justice, in which the free movement of persons is assured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime' (Amsterdam Treaty, Article 1(5)). In 2009, the entry into force of the **Lisbon Treaty** triggered a series of institutional changes. Policy-making

[6] MacKenzie et al. (2015)

[7] See Ripoll Servent and MacKenzie (2012)

[8] It was the Maastricht Treaty in 1993 that marked the beginning of the EU's formal involvement in security matters, internally and externally. The role of the EU in external security was through the common foreign and security policy, referred to as the EU's 'second pillar', while internal security, known as justice and home affairs, was the 'third pillar' of the new European Union. Cf. Murphy and Arcarazo (2014)

and implementation have, over the years, become progressively more integrated, with more competences given to the EU's supranational institutions, together with increased parliamentary and judicial oversight. The Lisbon treaty introduced the 'community method', referring to processes where supranational institutions such as the European Commission, the European Parliament and the Court of Justice of the European Union have a central role, and these were then extended. With regard to the institutional and policy landscape of the AFSJ, it should be noted that all relevant provisions concerning the AFSJ have been included in the new Treaty on the Functioning of the European Union (TFEU), under Title V. This implies a generalization of the 'ordinary legislative procedure', which brings the European Parliament on equal footing in terms of policy-making. Furthermore, the European Union Court of Justice becomes entitled to carry out judicial control of legislation passed under this framework (with relevant exceptions concerning Denmark and the United Kingdom). As discussed below, the entry into force of the Lisbon Treaty also has major implications in terms of fundamental rights, in particular data protection.

It is important to highlight that the constitution of the AFSJ does not substitute national approaches and policies concerning internal security: as stated by Article 72 TFEU: '[t]his Title shall not affect the exercise of the responsibilities incumbent upon member states with regard to the maintenance of law and order and the safeguarding of internal security'. Given the relevance in terms of internal security, *counterterrorism remains a competence of member states, and the EU policies should be considered in terms of added value and subsidiarity*. Moreover, counterterrorism is often a security practice deeply rooted in the history of each member state and of its law-enforcement authorities. Nevertheless, the European dimension seems particularly important, not only because intergovernmental cooperation has been an important asset since at least the establishment of the so-called TREVI group in 1975,[9] but also because EU institutions have increasingly and deeply invested in this field in the past 15 years.

The terrorist attacks on 11 September 2001 in New York deeply impacted EU law and policy, an effect that has been only reinforced by subsequent attacks in Europe. Notably, in the aftermath of the 2004 Madrid attacks, the European Council decided to create a **Counterterrorism Coordinator** who has the task to 'co-ordinate the work of the Council in combating terrorism and, with due regard to the responsibilities of the Commission, maintain an overview of all the instruments at the Union's disposal with a view to regular reporting to the Council and effective follow-up of Council decisions'.[10] Then, following the 2005 London attacks, the EU adopted an important piece of counterterrorism legislation (discussed in more detail below): the **Data Retention Directive** (DND) (Directive 2006/24 EC), aiming at the ensuring the retention of location and traffic data concerning communications. More recently, after the attacks in France and Denmark, the inter-institutional negotiations concerning the setting up of a pan-European system for passenger surveillance – known as the Passenger Name Record (PNR) system – have been resumed, with a strong impulse from the EU Counterterrorism Coordinator.

Besides punctual responses to major events, EU counterterrorism policy is also shaped through a series of multiannual programs. It has adopted three programmes to develop its '**area of freedom, security and justice**' over the past 16 years, signed in Tampere (1999), The Hague (2004), and Stockholm (2009). With its Action Plan on Combating Terrorism, the European Council sought, through the **Hague Programme,** to urgently take stronger action on a series of cross-border challenges, including terrorism and organized crime. The Hague Programme largely addresses the same priorities as the **Tampere Programme**, which was the first multiannual program focusing on the development of policy in the field of justice and home affairs. They both focus on migration and free movement of EU citizens, the strengthening of criminal justice and security cooperation and the development of a coherent external dimension to EU policy. As described by Murphy and Arcarazo, the Hague Programme is in line with government action across the world in the 'war on terror', and 'the field of EU counterterrorism law is just as problematic as US policy'.[11] A lot has been written about the balancing act between 'freedom' and 'security', seen as an impossible one in the eyes of many,[12] while others argue that the 'illiberalism' has been part of EU security law and policy since long before 9/11.[13]

In 2005, the Council adopted the **European Union Counterterrorism Strategy**.[14] The overall 'strategic commitment' is 'to combat terrorism globally while respecting human rights, and make Europe safer, allowing

[9] Casale (2008)

[10] Council of the European Union (2004) p. 14.

[11] Ibid, p. 6.

[12] Among others, De Hert (2005); Neocleous (2007); Waldron (2003)

[13] A similar critique about the latent illiberal posture of liberal democracies in 'fighting' terrorism is developed in Bigo et al. (2008)

[14] Council of the European Union (2005)

its citizens to live in an area of freedom, security and justice'.[15] Such a goal is pursued through four kinds of action (so-called 'pillars'): 'prevent', 'protect', 'pursue' and 'respond'.[16] The first, 'prevent', essentially includes strategies to avoid recruitment to terrorism, through various anti-radicalization measures, and to develop better media communication strategies to make EU policies better understood, and in turn further develop inter-cultural dialogue within and outside the EU. The second, 'protect', is focused on border control measures and efforts to protect critical infrastructure through a common EU approach. The third, 'pursue', revolves around various policing measures, through an improved police and judicial collaboration through Europol and Eurojust. Finally, the fourth pillar, 'respond', consists of various civil protection and crisis-response measures and assessments of the needs to strengthen these capabilities. It should be noted that this strategy acknowledges explicitly the 'primary responsibility' of member states in counterterrorism, but attempts to clarify the possible *added value* of the European dimension and EU contributions. The main idea is that the EU can play a pivotal role both between member states, for example by facilitating the sharing of 'best practices' or creating 'collective capabilities' between them and international partners. All in all, this reinforces a vision of terrorism as a border-less phenomenon, which cannot be tackled at 'mere' national level. The Counterterrorism Strategy is also important because it further reinforces the rationale of 'prevention', even if, in practice, it is mostly a set of policies to counter-radicalisation, recruitment and propaganda, rather than preventing attacks. Finally, and probably most importantly, the Counterterrorism Strategy foresees a mechanism of continuous review of the progress made – 'once every six months'.[17] While we provide below a brief overview of the latest review completed so far, it should be noted that this kind of systematic reporting, a sort of benchmarking mechanism, has become a quite typical instrument in the AFSJ to both control and foster implementation.

The **Stockholm Programme**, released in 2010, is a product of some of these reflections and a 'post-"war on terror" world', giving prevalence to fundamental rights and the role of the EU citizen. The programme states that the principal challenge for the coming years 'will be to ensure respect for fundamental freedoms and integrity while guaranteeing security in Europe'. Hence, it is important to ensure that 'law enforcement measures and measures to safeguard individual rights, the rule of law, [and] international protection rules go hand in hand in the same direction and are mutually reinforced'.[18] Next to defining a somewhat new approach to the intersection between security and fundamental rights, the Stockholm Programme also emphasizes the need to further consolidate the 'tools' at disposal, ranging from 'mutual trust' to 'legislation', from 'implementation' to 'evaluation' and 'training'.[19] While other instruments are presented, e.g. technological and organizational measures to ameliorate law enforcement cooperation and the management of information, the Stockholm Programme seems to stress the need to facilitate the implementation of what has been already developed, rather than promising a new overall strategy.

In fact, a strategic vision is introduced again with the **European Internal Security Strategy**, adopted by the European Council in February 2010. This document is a sort of companion to the European Security Strategy (adopted in 2003 and reviewed in 2008), and it complements it by sketching a vision and some overall guidelines on how to address threats to the 'internal', rather than 'external' security of Europe. However, the very notion of 'European internal security' remains ambiguous. On the one hand, the two European security strategies tend to overlap when it comes to the identification of specific threats, and in particular terrorism, where the internal/external divide is difficult to assess once and for all. On the other hand, the exact relation between the 'European' and the 'national' dimensions of internal security are not very clear. Moreover, the definition provided by the European Internal Security Strategy itself risks furthering complexity: '[t]he concept of internal security must be understood as a wide and comprehensive concept which straddles multiple sectors in order to address these major threats and others which have a direct impact on the lives, safety, and well-being of citizens, including natural and man-made disasters such as forest fires, earthquakes, floods and storms'.[20]

Probably the best way to understand the scope of the strategy is to focus on the kinds of institutional actors that may be considered at the core of the European internal security: 'law enforcement and border authorities, judicial authorities, and other services in, for example, the health, social and civil protection

[15] Ibid. p. 2
[16] Ibid. p. 3
[17] Ibid. p. 17
[18] Official Journal of the European Union, European Council, The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens (2010/C 115/01), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010XG0504%2801%29&from=EN
[19] Ibid. pp. 5-7

[20] Council of the European Union (2010) p. 3

sectors'.[21] The military is not mentioned, so that the kind of internal security foreseen in the European Internal Security Strategy seems one that can, and should, be ensured through civilian means, even when it comes to terrorism. Overall, the European Internal Security Strategy aims at defining a European Security Model, which should integrate and foster already developed approaches and tools, from judicial supervision to intelligence-led policing and information management, and which should embody principles at the roots of the European project, such as respect of fundamental rights, the rule of law, solidarity and mutual trust.[22]

While the Stockholm Programme and the European Internal Security Strategy are still to be considered the two main guiding documents when it comes to counterterrorism, it should be noted that European institutions are currently updating these guidelines. In December 2014, the European Council decided to launch the process for the 'development of a renewed European Union Internal Security Strategy', able to take stock of the implementation assessments carried out by the European Commission.[23]

A new **European Agenda on Security** was released on 28 April 2015.[24] The agenda proposes five guiding principles: 'full compliance with fundamental rights'; 'transparency, accountability and democratic control'; 'better application and implementation of existing EU legal instruments'; 'joined-up inter-agency and […] cross-sectorial approach'; and connection between 'all internal and external dimensions of security'.[25] These key principles are largely in line with the approach of the Stockholm Programme, in particular the emphasis on the role of fundamental rights and the need of further implementation. All in all, the document seems to adopt an approach that can fortify what has already been done or finalize 'pending' issues, rather than introducing completely new initiatives. This further shift towards the operationalization of EU policies, and the realization of the potential of the EU added value, is also evident in the attention devoted to the generalization of policy practices already tested at the European level (e.g. risk assessment capabilities, inter-agencies cooperation) and to the use of training, funding and research programs. Notably, the commission mentions the work underway in the development of a ''privacy by design' standard aimed to promote the embedding of high standards of security and fundamental rights at the earliest stage in technological design'.[26] Also relevant for TACTICS is the attention dedicated to the strengthening of existing cooperation networks, not only among EU agencies (such as Europol, Eurojust or CEPOL), but also between member states authorities (for example, the cooperation between special intervention units, or the Police and Customs Cooperation Centres).

An underlying concern in the new Agenda, and in similar security strategy documents, is about creating a secure *internal* European space, through the protection of the European *external borders* and exclusion of unwanted elements from the outside. For instance, terrorism is listed as the first of the three key priorities of the agenda, followed by 'serious and organized cross-border crime' and 'cybercrime'.[27] It should be noted that terrorism is most often mentioned, as in the previous treaties and programmes, in the context of 'cross-border crime and terrorism'. However, terrorism-related threats in Europe today have both domestic and cross-border elements, and when it comes to crossing borders, it will just as often be European citizens returning to Europe after a stay abroad. There has been a growing awareness of this in recent years, pushed forward with the challenges related to the so-called 'foreign fighters' going to Syria, Iraq and Afghanistan, for example. The latest report on the implementation of the EU Counterterrorism Strategy, from November 2014, shows the central place that the issue of foreign fighters has taken up in the past period (December 2012 to mid-October 2014).[28]

---

[21] Ibid.

[22] Ibid. pp. 9-ff

[23] Council of the European Union (2014)

[24] European Commission, The European Agenda on Security, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee And the Committee of the Regions, Strasbourg 28.4.2015, COM(2015) 185final, http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

[25] Ibid. pp. 3-4

[26] Ibid. pp. 11-12

[27] Ibid. pp. 12-ff

[28] Council of the European Union (2014)

Compared with the previous documents, the European Agenda on Security narrows its scope, implicitly clarifying what should be understood as European internal security. Yet, internal security is still often described as a matter of protecting the internal against the external. In this respect, counterterrorism strategies in cities are often conceived of as an increase of regular police activities and an extension of border policing activities internally, including in some instances the potential militarization of these policing activities.

The 2015 February **Council Conclusions on Counterterrorism** call for 'comprehensive action against terrorism in line with the 2005 EU Counterterrorism Strategy and in full compliance with international law, fundamental values and international human rights standards. While member states have the primary responsibility for addressing terrorism, the EU as such can add value in many ways.'[29] As an echo to the 2014 EU Counterterrorism Coordinator's Report on the implementation of the EU Counterterrorism Strategy, the awareness of the increasingly border-less and cross-border character of terrorism, and the challenge of new recruitment to terrorism and the issue of 'foreign fighters', in the 2015 conclusions the council further decide to step up, 'as a matter of urgency, its external action on countering terrorism in particular in the Mediterranean, the Middle East, including Yemen, and North Africa, in particular also Libya, and the Sahel.'[30,31] Further, more emphasis will be placed on preventing terrorism, notably through efforts to counter radicalization and recruitment to and financing of terrorism, while also addressing 'underlying factors such as conflict, poverty, proliferation of arms and state fragility that provide opportunities for terrorist groups to flourish.'[32] The council conclusions also call for a reinforcement of 'the role of EU INTCEN [Intelligence Analysis Centre] as the hub for strategic intelligence assessment at EU level, including on counterterrorism.'[33]

The European counterterrorism cooperation is also characterized by the use of reporting mechanisms to assess and foster implementation, and the active participation of European agencies, such as Europol and Eurojust.

As foreseen in the European Counterterrorism Strategy of 2005, a '**report on the implementation of the EU Counterterrorism Strategy**' is completed at (more or less) regular intervals by the EU counterterrorism Coordinator. The latest report has been released in late November 2014 and provides an overview of both the state of play of counterterrorism efforts and priorities, and of the underlying vision behind it.[34] The report is mainly structured along the pillars of the EU Counterterrorism Strategy – prevent, protect, pursue, respond – but it also concerns recent compelling issues, such as 'foreign fighters', and the 'external dimension'. Overall, it shows a panorama characterized by an impressive amount of initiatives, but fails to offer a clear picture of the effective implementation of the different measures, or of the tools that prove their added value.

In the past 10 years, **Europol** has increasingly become an important hub for the construction of the AFSJ, and for European counterterrorism efforts. While terrorism was not included as a specific aim of Europol at the outset, it has, since 2003, been defined as the agency's main priority. Europol mainly collects, analyses and exchanges information with national agencies, notably through a 24-hour service provided by the Europol Operational Centre and a counterterrorism task force (both established in the aftermath of 9/11), and supports operational investigations by EU police and joint investigation teams. It also produces an Annual Terrorism Situation and Trend Report (TE-SAT). It is, however, difficult to estimate the impact of Europol, mainly due to the lack of information provided by the organization itself on its own activities.[35] What is known, however, is that there is a challenge in making member states share relevant information with Europol, which is a prerequisite for it to be able to fulfil its tasks successfully.[36] An important reason behind member states'

[29] Council of the European Union, 'Council Conclusions on Counterterrorism', 9 February 2015, http://www.consilium.europa.eu/en/press/press-releases/2015/02/150209-council-conclusions-counterterrorism/

[30] Semi-arid region of western and north-central Africa extending from Senegal eastward to the Sudan, Encyclopædia Britannica.

[31] Ibid.

[32] Ibid.

[33] Ibid.

[34] EU Counterterrorism Coordinator (2014)

[35] Casale (2008) op. cit.

[36] Wolff (2009)

reluctance to share is a mistrust that the sources of sensitive data will be sufficiently protected, a condition for the continued future access to information.[37]

Eurojust is a network of national judicial authorities of the EU member states, established in 2002 by the Council of the European Union. Its objectives include facilitating cooperation between national authorities in the investigation and prosecution of serious crime involving two or more member states, co-ordinating investigations and prosecutions in member states, and providing expertise to member states and the Council (e.g. recommendations for law amendments to improve the legal framework for the fight against cross-border crime). Eurojust's tasks were redefined at the end of 2002 to strengthen its contribution to the fight against terrorism, notably by asking each member state to designate a National Correspondent for terrorism, who should have access to all relevant information resulting from criminal proceedings relating to cases of terrorism.[38] Moreover, the tasks of Eurojust in terms of counterterrorism include: organization of National Correspondents the national level, transmission and processing of information, and assistance and feedback. Eurojust has faced some of the same challenges as Europol in terms of access to information and the fact that different member states have different legislations as to what can (or should) be shared.

All in all, the EU policy landscape in the field of counterterrorism remains pretty scattered: an increasing number of institutions, policy priorities and tools have to be taken into account. From a TACTICS perspective, it should be noted that some of the features of the system seem to resonate with the most recent developments: an ambition to manage multiple kinds and sources of information, an increasing attention towards the fundamental rights implications of counterterrorism, and the effort to specify what is the added value of new forms of cooperation or technical measures.

2.2 Fundamental rights and the European policy landscape

A key element of the EU AFSJ policy landscape is data protection. Nowadays, the protection of personal data is enshrined as a fundamental right, distinct from privacy, in the EU Charter of 2000. Discussions about counterterrorism and state surveillance are framed, mostly, in relation to data protection. While this is far from being the only fundamental right relevant for counterterrorism, it has probably become the main prism through which law security measures are discussed at the European level, as also noted above in the analysis of the EU policies. For example, as early as December 2001, the Article 29 Working Party, which is a derivative European body representing member states' data protection authorities, noted that '[a]ll these measures [the counterterrorism measures proposed in the aftermath of the attacks] have a direct or indirect impact on the protection of personal data'.[39] In other words, data protection is often the site where counterterrorism policies first encounter fundamental rights. It is also one of the EU factors that has the most direct impact in the policy-making concerning TACTICS-like systems, even when this happens at the national level. Indeed, European principles and rules percolate to the national level through the transposition or direct application of European instruments. For all these reasons, we present the main features and the current evolution of data protection, as they have a major effect on the possible shaping and use of a TACTICS-like system.

The very term 'data protection' is a European construct,[40] introduced with the adoption of Convention 108 of the Council of Europe and, more importantly, with the adoption of the Data Protection Directive in 1995. Currently, the EU legal framework on data protection is a complicated patchwork, where several legal instruments stand next to the Data Protection Directive: from the so-called Council Framework Decision that focuses on police and judicial cooperation, to the ePrivacy Directive on electronic communications, as well as a series of specific provisions concerning EU agencies or EU policies.

---

[37] Casale (2008) op. cit.

[38] Council Decision of 19 December 2002 *on the implementation of specific measures for police and judicial co-operation to combat terrorism in accordance with article 4 of the Common Position 2001/931/CSFP,* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003D0048&from=EN

[39] Article 29 WP. 2001. Opinion 10/2001 on the need for a balanced approach in the fight against terrorism. Brussels: Article 29 Data Protection Working Party.

[40] González Fuster (2014)

Moreover, a fundamental right to the protection of personal data is now enshrined in the **Charter of Fundamental Rights of the European Union**, and it has gained legal force since the entry into force of the Treaty of Lisbon. Its structure resembles that of Article 8 of the **European Convention on Human Rights** (ECHR), with the first paragraph establishing the right and the following paragraphs defining its limits. However, the 'default position' is different: there is no prohibition of processing, but, rather, rules to ensure legitimate processing. The main principles of data protection that emerge from the Charter are the following: 'fair processing'; 'specified purpose'; 'consent' or 'legitimate basis'; legality ('laid down by law'); 'access' and 'rectification'; and supervision by an 'independent authority'. These principles are similar to those underlying the Data Protection Directive, and they can be considered as the core of data protection as a fundamental right.

From a data protection point of view, the second effect of the **Lisbon Treaty** has been the introduction of a specific data protection article in the Treaty on the Functioning of the European Union: Article 16 TFEU. The consequences of this article are far-reaching. First of all, it does reaffirm the renewal of an autonomous right of 'protection of personal data' for 'everyone' – thus a right delinked from the notion of citizenship. Second, it implies a positive obligation to 'Union institutions, bodies, offices and agencies' and even to 'Member States when carrying out activities which fall within the scope of Union law' to enact data protection regulations. At the same time, it also reinforces the role of 'control' of 'independent authorities', which remain a cornerstone of the data protection dispositive. Finally, Article 16 TFEU also establishes the type of legislative procedure to be followed in the decisionmaking processes touching upon data protection.

The main implication of these developments for TACTICS is that data protection principles, case law and legislation will play a major role in both policy-making and deployment. Most probably, data protection will be the main interface for several actors, including individuals, to relate with the deployment of this kind of counterterrorism system and to question, if necessary, its use.

The most important legislation concerning data protection at EU level is the **Data Protection Directive**. The EU Directive on Data Protection was proposed in order to correct the divergence of national data protection laws, and it is applicable for data that are being processed by member states or private parties.[41] The 1995 directive excluded from its scope the processing of data by justice and home affairs authorities, entailing, notably, police and judicial cooperation. However, as the pillar system is no longer valid, and as the directive is increasingly used to regulate traditional 'third pillar' domains, it should be mentioned here. The basic presumption of the directive is that personal data can be processed but that certain conditions should be met. These conditions are centred around three principles:

(1) Transparency: relates to the processing of data, which should only be carried out in specific circumstances, such as where there is consent on behalf of the data subject, when processing is necessary for the compliance with a legal obligation or for the performance of a task in the public interest. They should always be in respect of the fundamental rights and freedoms of the data subject.

(2) Legitimate purpose: indicates that data may only be processed for explicit and specified purposes and may not be processed further in a way incompatible with those purposes.

(3) Proportionality: underlines that personal data should only be processed when it is adequate, relevant and not excessive in relation to the purposes stated for the data collection. Data should not be kept in a form enabling identification of individuals for longer than necessary and for purposes other than for which they were collected or further processed.

Furthermore, extra restrictions apply for the processing of sensitive personal data (Article 8). Lastly, a decision which produces legal effects or significantly affects the data subject may not be based solely on automated processing of data (Article 15), and a form of appeal should be provided when automatic decisionmaking processes are used.

Data protection is also a key element of the EU AFSJ policy landscape because of the increasing relevance of its related institutions: both national data protection authorities (mandated by both the Data Protection Directive and Article 8 of the EU Charter) and the EU bodies. At the EU level, the previously mentioned **Article 29 Working Party**[42] and the **European Data Protection Supervisor** (EDPS) have come to play an

[41] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031–0050

[42] Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data is an independent advisory body on data protection and privacy, set up under Article 29 of the Data Protection Directive

increasingly guiding role in the debates concerning counterterrorism legislation, through opinions and working documents. The EDPS has been particularly vocal in advocating an approach to counterterrorism that can escape the deadlocks of the opposition of security and liberty: instead of conceiving the two as mutually exclusive if not 'conflicting' goals, the EDPS argues that the two ends should be pursued at the same time.[43]

Particularly important for policy-making about TACTICS-like systems is the fact that data protection is also increasingly translated into a series of **technical and organizational solutions**. Among the most relevant 'smart initiatives' for counterterrorism is the (sometimes still attempted) introduction, by the European Commission, of a 'fundamental rights' check list,[44] which would facilitate the identification of possible tensions between proposed measures and fundamental rights – the specific provisions on data protection by design and by default in the framework of the data protection reform.

As already mentioned, the EU data protection legal framework is currently undergoing a major reform. Following up on a series of institutional discussions, the European Commission presented two legislative proposals in January 2012: the **General Data Protection Regulation (GDPR)**[45] and the **Data Protection Directive Proposal (DPDP)**.[46] The processing of personal data in the course of law enforcement and judicial activities is covered by the DPDP, which can be considered a more sectorial instrument. Hence, it is safe to assume that the DPDP will become the most important legal instrument when it comes to data protection in the field of counterterrorism and to policy-making in relation to TACTICS-like systems. Yet, the increasing reliance by public authorities, including security forces, on data generated in commercial or administrative environments, will probably create situations where the DPDP will not be the only relevant legal framework.

Particularly relevant for TACTICS is the fact that both instruments introduce a specific provision on **data protection by design and by default**. Based on these texts, it is possible to propose the following working definition of data protection by design and by default: First, data protection by design implies both 'technical and organizational measures', as well as 'procedures': not only ad hoc fixes but also iterative solutions. Second, the aim of these measures and procedures is both general and specific: 'meet the requirements' set by the legal instrument, and 'protect the rights of the data subject'. Finally, *data protection by design* is also *data protection by default*: the functioning of processing technologies should be based on the principle of data minimization – 'only those personal data which are necessary for the purposes of the processing are processed'.

Finally, it is important to mention in this overview of the policy landscape the **2014 judgment of the European Court of Justice on the so-called Data Retention Directive**.[47] The judgment came after a

---

95/46/EC: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm. For example, the Article 29 Working Party has released the following key documents on counterterrorism in the past decade:

- Working Document on surveillance of electronic communications for intelligence and national security purposes, 14/EN, WP228
- Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, 536/14/EN, WP211
- Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing, 01008/2011/EN WP186
- Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime
- Opinion 1/2007 on the Green Paper on Detection Technologies in the Work of Law Enforcement, Customs, and other Security Authorities, 0039/07/EN WP129
- Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism, 11885/04/EN WP99

[43] Cf. Buttarelli (2011)

[44] European Commission (2010)

[45] European Commission (2012)

[46] European Commission (2012)

[47] European Court of Justice (2014)

request for a preliminary ruling on the issue of the validity of the Data Retention Directive (DRD). Requests came from two high courts – Ireland and the constitutional court of Austria. The issue was of two case challenges of the validity of the DRD from Case C-293/12 (DRI case) and Case C-594/12. Both questioned the compatibility of the directive with the 'rights of privacy laid down in Article 7 of the Charter and Article 8 of the ECHR' (Case C-293/12, para 2). Additionally, both cases challenge whether the directive really is able to achieve, and to do so in a proportional way, the objectives it pursues without unjustifiable interference with fundamental rights.

As further discussed in Chapter 5, the judgment of the European Court of Justice is particularly important for policy-makers focusing on TACTICS-like systems. The court held that the Data Retention Directive does in fact constitute a violation of the Charter rights as the EU legislature had exceeded the limits of the principle of proportionality (Articles 7, 8, 52). The court also highlighted that the directive failed to meet the proportionality requirement laid down by Article 52 of the Charter, arguing that there is a 'general absence of limits in the directive' and that it 'fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities' (para 60). Yet, the ECJ judgment is particularly relevant in the EU AFSJ landscape, and for policymakers in particular, because the Court provides a series of more or less explicit policy guidelines. By commenting on the main shortcomings of the existing legislation, while not contesting the necessity of these kinds of counterterrorism measures, the court seems to provide a checklist of what should be taken into consideration by the legislator. As noted by Horsley, 'the Grand Chamber's decision is principally concerned with the fixing of parameters for future constitutionally legitimate policy-making by the EU legislature in the relevant policy area'.[48]

2.3 Issues and challenges facing European policy-makers in the context of counterterrorism

In addition to the issues surrounding privacy and data protection, combating terrorism poses several sets of challenges to policy-makers and security agencies, at all levels. These sets of challenges – attack methods, scale, source, vulnerability and reassurance – might all be familiar, but they are not trivial; they require the commitment of intellect, imagination and resources, possibly over decades. They also require constant, tangible demonstration of success in terms of policy and operations. This is difficult in that 'success' in CT is almost by definition a 'non-event', thus evoking the problem of negative proof. And at the largest and most complex levels of policy, proof of success becomes more difficult still. A political organization such as the European Union, for example, could not meaningfully be said to face an 'existential threat' from any terrorist group or collection of them. Yet in a paradoxical way, even as the terrorist threat to the EU is (in relative terms) diminished, the expectations placed upon the EU by European governments, businesses and electorates seem only to increase. In other words, although the organizational scale and complexity of the EU mean that it is essentially immune from any conceivable terrorist threat, the EU is nevertheless not permitted to be a 'safe haven' for policy-makers, aloof from the challenges of CT policy. On the contrary, the EU is expected to do *more* to confront a problem in which it is *less* engaged.

On a practical level, the first set of challenges to be confronted concerns the very wide range of plausible **attack methods**, not just in the physical domain but also in the cyber domain. All of the following have, at one point or another, been discussed in mainstream CT analysis: hoaxes; random sniper shootings; cyber attacks on networks or facilities; military explosives (such as C-4 and Semtex); industrially available chemical explosives (such as ammonium nitrate/fuel oil (ANFO)); chemical weapons (such as Sarin); biological weapons (such as anthrax); radiological weapons and dispersal devices (or 'dirty bombs'); and even atomic/nuclear weapons. This very wide range of possibilities presents obvious policy/operational and investment challenges in terms of the control of know-how, technology and materials; detection and identification; and counter-measures (including decontamination).

The next set of challenges concerns the **scale** of a terrorist attack. An attack could be undertaken by a so-called 'lone wolf' or, at the other end of the scale, it could be more extensive and orchestrated, perhaps against several targets simultaneously, perhaps involving chemical, biological, radiological and nuclear (CBRN), perhaps with international organization. An attack could be generalized (i.e. against a city as a whole) or it could be functional (e.g. focused on infrastructure key points and nodes). Of particular concern for the EU, terrorist attacks could take place against one or more EU member states, but not against others, in an attempt to create political divisions. In policy/operational terms, a level of cohesion and solidarity must be demonstrated in the face of attacks; there must be sufficient intelligence capacity to provide early warning

[48] Horsley (2015) p. 8

of terrorist attacks, whatever the point on the scale, and there must be sufficient flexibility to ensure that any response is proportionate to the scale of the attack and therefore credible and legitimate.

The third set of challenges concerns the **source** of a terrorist attack. It will be essential – politically, strategically and in terms of public confidence – to establish the source of a terrorist attack as swiftly and as accurately as possible. **Vulnerability** prompts yet another set of policy and operational considerations. The member states and institutions of the EU are best described as a 'target-rich environment' for a terrorist attack, whatever the method, scale and source. EU member states are open societies, and the EU has itself sought to make a virtue out of openness, not least in the principle of free movement of goods, services, capital and people. Open societies and organizations are by definition structurally vulnerable to exploitation and attack: airports, docks, communications and energy infrastructure, power stations, official buildings, shopping malls, pharmaceutical factories, sports stadiums, civic events and parades, apartment blocks, etc. can all be *protected*, but they cannot be made *invulnerable* to attack. In such circumstances, where vulnerability cannot be eliminated, what is required of policy-makers and security agencies is prioritisation and risk management (or 'risk balancing'[49]). Making trade-offs between different targets, interests and vulnerabilities is a complex enough task at the national level. At the level of the EU, the task must be more difficult still when the respective interests of member states might be drawn into contention.

On the basis that vulnerability can be both physical and psychological, the final set of policy challenges are those related to **reassurance**. Terrorism is the subject of constant definition and redefinition, prompting one analyst to remark that 'the search for a definition of terrorism has been long and painful and is now living a separate life of its own.'[50] Yet if there could be said to be a single characteristic common to all terrorist actions, at whatever level and for whatever motive, it would be that terrorism is an attack on public perceptions, confidence and trust in government. Policy-makers and security agencies must anticipate and respond appropriately, by reassuring public opinion and key stakeholders that order and control have not been lost and by ensuring that unwarranted perceptions of vulnerability are not allowed to proliferate.

Overall, the challenge presented to European Union CT policy-makers and agencies is therefore clear enough. For the EU to be credible in this difficult and often controversial field of security policy, it must demonstrate capacity, competence and 'value-for-money' in all the components of traditional counterterrorism: recognition (establishing the method, source and intention of a terrorist threat); response (pre-empting or reacting in a timely and proportionate manner); and, finally, reassurance (demonstrating to stakeholders and public opinion generally that the right measures are being taken by a competent government and without generating a wave of uncertainty and even panic). In other words, the EU must show that it is more than the sum of its parts (i.e. its member states and institutions); that it can contribute to meeting all types of terrorist threat, at all levels of severity and whatever the scope; and that it can mitigate elements of the EU's structural vulnerability. Providing support to practitioners dealing with the handling of terrorist incidents will help demonstrate the commitment to mitigating the vulnerabilities described above.

2.4 Challenges (and opportunities) for collaboration among European member states in the field of counterterrorism

If the practical obstacles to collaboration can be surmounted, a still more complex set of problems then comes into view; **political and constitutional differences** among European member states. In terms of the initial analysis of terrorist threats, for example, there could be grave differences of opinion as to the suitability of labelling this or that group as 'terrorist' as opposed to 'legitimate movement of national liberation', or some similar choice of words. There could, equally, be different levels of sensitivity among European Union governments as to the trade-offs that might be made in favour of security. Any democracy – and indeed any collection of democracies – must be expected to be highly sensitive to the costs (political, constitutional, social, financial) of proposed security measures. Even if such measures could be shown to promote security, there will always be the argument that the cost of security might be excessive if a 'surveillance society' entails the loss of certain freedoms (i.e. of movement) and even human rights (i.e. of privacy) and if it might require disinvestment in other, unrelated areas of public spending.

Collaboration among member states could allow for the participants, together with the hub organization (i.e. the EU) to contribute to the **mitigation of vulnerability**. If vulnerability cannot be negated altogether by some means or another, then it must be mitigated. At the national level, mitigation can be achieved by addressing the adverse consequences of vulnerability, that is, building sufficient redundancy and resilience

[49] See Van Brunschot and Kennedy (2008) p.12

[50] Malik (2000) p. xvii

into the system such that it can absorb terrorist attacks and recover. Alternatively, in a larger political system such as the EU, mitigation can be achieved by a system-wide off-setting arrangement, such that weaknesses in some parts of the system are buttressed by strengths in others. The ability to transfer strength and resilience within the system is the most important benefit to be gained from collaboration. The opportunity this presents to the EU is nothing less than becoming an acknowledged 'high-reliability organisation' where counterterrorism policy and operations are concerned: 'High reliability organisations are organisations that work in situations that have the potential for large-scale risk and harm, but which manage to balance effectiveness, efficiency and safety. They also minimise errors through teamwork, awareness of potential risk and constant improvement.'[51]

[51] The Health Foundation (2011) p. 3; see also Lekka (2011) pp. v, 18

3 Methodology

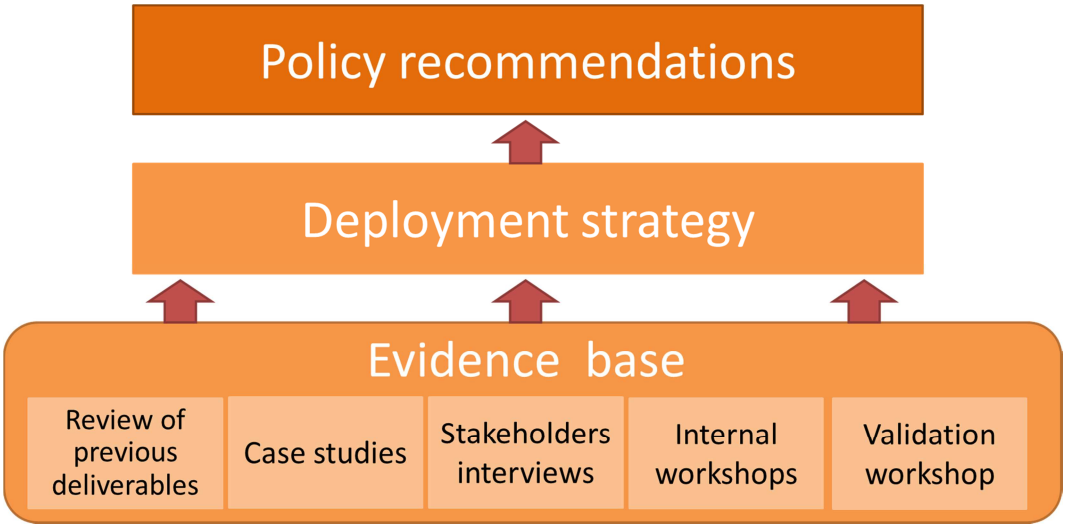
This chapter presents the methodology that the study team applied to generate the policy recommendations that emerge from the TACTICS project. We employed a structured methodology in order to develop a rigorous evidence base and to identify lessons from technology implementations that have policy implications in a European context.

The methodology used consisted of five elements:

- **Review of previous deliverables**: Undertake a review of all previous project deliverables in order to extract relevant deployment and policy implications for TACTICS.
- **Case study analysis:** Conduct eight case studies focusing on different technology applications in the field of counterterrorism or, more broadly, public security, including the identification and analysis of relevant case law.
- **Qualitative interviews:** Conduct semi-structured interviews with academics, policy-makers, law enforcement practitioners and human rights experts.
- **Workshops:** Conduct a series of internal workshops to develop and refine the deployment strategy and policy recommendations.
- **Validation:** Conduct a workshop with external stakeholders to validate both the deployment strategy and the policy recommendations.

Figure 1 summarises the methodological approach, while the following sections provide more detailed information about each component of the methodology.

Figure 2. Summary of the research approach and methodology



3.1 Review of previous deliverables

The TACTICS system is more than just a new technology developed to support law enforcement agencies in the management of counterterrorism operations. TACTICS brings in a new concept of operation that is captured in its architecture and primary features and characteristics (e.g. decomposing the threats based on historical data, managing capabilities rather than resources/assets, using automated behavioural analysis combined with facial recognition) and that responds to the necessity of ensuring an ethical use of technology by following a privacy-by-design approach. Therefore, the study team first undertook a review of all relevant previous project deliverables to extract implications that could inform policy recommendations. For each of the previously delivered reports, the study team extracted relevant findings and implications for the present work package.

3.2 Case studies

While security technology has been evolving quickly in recent years, the application of technology in the context of public safety and security is not a recent trend. Therefore, several lessons can be learned from previous, more or less successful, attempts to use technology in support of security agencies. This study therefore applied a case study approach to understanding issues associated with deploying a technology system in support of counterterrorism.

Case studies as a methodology are often used to focus on retrospective analysis, such as examining the evidence base supporting key decisions and identifying effective practice. By collecting information about the introduction of analogous systems, analysis can be conducted to identify cross-case lessons.

For the purpose of this project, we reviewed eight case studies:

- Ring of Steel
- Project Champion
- Passenger Name Record (PNR)
- e-Borders
- Body scanners
- ShotSpotter
- Police surveillance drones
- Data Retention Directive (DRD)

In preparation for the case study analysis, the team held an internal workshop to discuss which case studies would be most relevant to the study's objectives. During the workshop, case studies were selected on the basis of five criteria, namely, that the case study must: (1) have relevance for counterterrorism; (2) be deployable in urban environments; (3) use technology to support decisionmaking; (4) have an impact on civil liberties; and (5) be deployed in a European context. Table 1 assesses the eight case studies against the five criteria in order to explain their inclusion in the team's analysis.

Table 1. Criteria for the selection of case studies

	Criterion 1: **Relevant to counterterrorism** [52]	***Criterion 2:*** **Deployable in urban environments**	***Criterion 3:*** **Uses technology**	***Criterion 4:*** **Has impacts on civil liberties**	***Criterion 5:*** **EU deployment**
Ring of steel	✓	✓	✓	✓	✓
Project Champion	✓	✓	✓	✓	✓
Passenger Name Record (PNR)	✓	✓	✓	✓	✓
e-Borders	✓	✓	✓	✓	✓
Body scanners	✓	✓	✓	✓	✓
ShotSpotter		✓	✓	✓	
Data Retention Directive	✓			✓	✓

As Table 1 indicates, most of the case studies match all of the selection criteria. However, given the limited evidence base on technology-driven counterterrorism initiatives in the EU, the scope of the team's analysis was widened to include security and crime prevention tools in the EU and the US.[53] While ShotSpotter is

[52] While the study team found that most of the case studies have counterterrorism objectives, many were also considered to have a wider set of security purposes, including, *inter alia*, preventing and responding to crime, protecting public safety and countering illegal immigration.

[53] The scope was expanded to include the US because of the wider availability of source material for the ShotSpotter and police surveilance drones case studies.

primarily a US-based crime prevention and response tool, for example, it was included because it offers relevant law enforcement lessons for EU counterterrorism practitioners. The use of small arms in recent terrorist attacks in European cities, such as the January 2015 Paris attacks, has highlighted the relevance of systems such as ShotSpotter in the European counterterrorism context.

The eight case studies were also selected because they illustrate a range of capabilities that may be used by, or in parallel to, a tool such as TACTICS. While the ring of steel and Project Champion are both examples of surveillance initiatives that rely on CCTV and Automatic Number Plate Recognition (ANPR) technologies, the other initiatives – PNR, e-Borders, the Data Retention Directive and police drones – all involve the collection and retention of citizens' personal data. Body scanners exemplify a different capability: the physical detection of objects that pose a security threat. ShotSpotter is a gunshot detection system that operates using a network of sensors. Surveillance, data collection, physical security, and gunshot detection are all capabilities that could be used by a counterterrorism system such as TACTICS. The case study on the Data Retention Directive, while not related to the use of a particular technology, was considered relevant for the purpose of this deliverable as it provided a useful insight into the legal and regulatory dimensions of personal data retention, thus highlighting the importance of considering the impact on civil liberties. Because TACTICS may draw on enabling resources that collect and retain personal data, the challenges presented in the DRD case study are particularly relevant.

A data capture spreadsheet was developed in Excel to ensure consistency of data collection for each of the cases. Data for each case was captured around the description of the technology, the context for its introduction, how the implication was conducted and by whom, and any information about the outcomes or evaluations conducted on the impact of the technology in meeting its aim. Finally, we also included considerations with regard to the relevance to the TACTICS project.

3.3 Methodology for case law selection and analysis

The case law analysed in chapter 5 below has been selected on the basis of three criteria: (i) relevance of the case law for the European jurisprudence on the relation between counterterrorism practices and human rights; (ii) relevance of the specific counterterrorism practices at stake for a TACTICS-like system; (iii) relevance of the human rights at stake in relation to the specific challenges raised by a TACTICS-like system.

The project team, based on its own expertise in the field, has drawn a final list of five cases of the European Court of Human Rights (ECHR) in Strasbourg. Each case law contributes from an original angle to understand what are the main principles and constraints, in terms of human rights, that should be taken into account in counterterrorism policy-making. The decision to focus on the ECHR case law has the purpose to complement the overview of the EU AFSJ landscape proposed in chapter 2 above. This choice permits to cast a light on crucial elements of European jurisprudence and, increasingly, of everyday policy-making at the national and European levels.

The same grid of analysis applies to each case: (i) what are the main facts brought to the ECHR?; (ii) what are the main issues at stake in terms of protection of human rights and counterterrorism practices on the basis of the conclusions of the Court?; (iii) what is the specific relevance of the case law for TACTICS?; and (iv) what are the main lessons applicable to the design and deployment of a TACTICS-like system?

3.4 Expert interviews

As part of the research, the study team undertook 27 semi-structured interviews between May and August 2015 to obtain qualitative description of perceptions or experiences. To ensure consistency of data collected through the interviews, a structured interview protocol was developed and applied in the interviews. The interview protocol that was developed for this study is available in Appendix B.

The interviews had two main purposes: gather evidence for the case studies and capture different perspectives on the general issue of the use of technology in counterterrorism or public security. For this reason, the pool of interviewees was very diverse both in terms of background and in terms of geographic origins. In particular, the interviewees included:

- Eight law enforcement practitioners;

- Seven academics;
- Four human rights experts;
- Three policy professionals.

To capture the wider European picture, we interviewed people based in the United Kingdom, France, the Netherlands, Germany, Belgium and Australia. We also interviewed people in the US. We have included experts from outside of Europe where they had particular expertise of a technology or implementation (e.g. ShotSpotter).

The interviewees were also selected to ensure that all case studies had at least one expert who could validate the findings of the literature review. Table 2 illustrates the distribution of expertise among the case studies. Some of the interviewees were able to comment on more than one case study.

Figure 3. Areas of interviewees' expertise by case study

Areas of expertise	Number of experts
Ring of Steel	2
Project Champion	5
Passenger Name Record	6
E-borders	3
Body scanners	1
ShotSpotter	2
Police surveillance drones	2
Others*	6

*Includes expertise in either national policing approaches (the Netherlands, France and the UK) or relevant technologies (e.g. CCTV)

3.5 Internal workshops

Throughout the preparation of the deployment strategy and the cross-European policy recommendation, the project team organised internal workshops to extract from the collected evidence all relevant implications from both a deployment and a policy perspective. This allowed the project team to continuously refine the content of the two deliverables as additional evidence became available.

3.6 Validation workshop

The final element of the methodology included the organisation of a validation workshop involving external stakeholders from the policy-makers community. The purpose of the workshop was to present the findings to date and ensure that the areas covered had relevance and application for the policy-makers. The agenda, the list of participants and a short write-up of the event are available in Appendix C.

3.7 Potential methodological limitations

There are a number of limitations with the methodologies chosen.

The data used for this study are largely qualitative and relate to the CT field, which, as we noted in the literature review, faces issues in developing a good empirical evidence base and conducting systematic analyses of effects or effectiveness of different interventions. In turn, lessons and conclusions from this study are based on the available evidence, but recognise that in many cases the evidence is equivocal or limited. The research was also limited to the inclusion of eight cases due to size and scope of the study. This means that the cases are not necessarily globally representative or cover the full range of technologies introduced in the context of counterterrorism. Because each of the cases took place at different times and in different

contexts, the comparison of the cases is difficult. However, by ensure we extracted similar types of information across all cases, we sought to minimise the risk of non-comparability.

A substantial amount of the data and participant input comes from American or Western European sources, given that this is where much of the established expertise lies. While many of these lessons have clear cross-European relevance, there may be considerations specific to southern and eastern Europe that are not included here. Finally, the validation workshop took place in Brussels, in July 2015, which potentially limited the attendance of participants from outside Brussels, and indeed outside Europe. Furthermore, the timing of the workshop was in the month of July, which often conflicts with the summer holiday season. We did, however, receive sufficient interest and participants to allow for a solid discussion around the key findings and issues of the project.

4 Review of previous TACTICS deliverables

This chapter presents a review of previous relevant deliverables from the TACTICS project, in order to identify any implications relevant to the present deliverable 8.2.

Below, we have included an overview of the work package conclusions most relevant to this present report and highlighted the implications for the cross-European policy recommendations.

4.1 WP 2: User requirements & scenario definition

The purpose of this WP was to identify the user requirements for the TACTICS system and define the scenario that the system should potentially be deployed in.

First, it should be noted that not every city or urbanized location is equally 'attractive' for terrorists. Consequently, there are locations that are more threatened with terrorist acts than others. [D2.1; section 4.4.1]. Awareness of the indicators characterizing the city and representing its physical attributes may contribute to the better perception of terrorism risk and to more suitable allocation of resources supporting counterterrorism. [D2.1; section 7]. Terrorist target planning is a rational decisionmaking process. [D2.1; section 5.4.3]. End users distinguished gaps/limitations in existing ICT decision support tools – including a point at which tools should be tested and applied. [D2.1; section 3.1/III/5]. Finally, CT end users noted international cooperation/sharing data and/or knowledge as a currently under-fulfilled need. [D2.2; section 3.1/II/1].

The findings from WP 2 highlight the need for any technology addressing CT to maximise its use with regard to enhanced decision support and the need to know and understand the city's characteristics. This will in turn enhance the situational awareness of the end users operating there. Furthermore, if TACTICS were to be deployed simultaneously in environments with the potential for cooperation (border cities, cities in same country, etc.), the possibility for TACTICS to enhance information/knowledge sharing could be tested. Finally, validations/tests/pilots should be part of any continued development of TACTICS.

4.2 WP 4: Threat Decomposition

In WP 4, the focus was on improving the threat decomposition process by defining deviant terrorist behaviour. This was done by deconstructing past, and postulating future possibilities for, terrorist modus operandi. The deviant behaviours were connected to urban characteristics in order to select relevant deviant behaviours for specific urban environments possible. Furthermore, the Threat Decomposition Tool was developed based on functional requirements.

In D4.3 the main challenges of counterterrorism in cities were provided, in particular the issues of privacy, ethics and the human rights perspective. The very purpose and scope of TACTICS-like systems necessitates an adoption at the national level and verification of its design to specific national legal requirements and administrative constraints. While the European Union and the international legal frameworks provide essential references and guidance, the legitimacy of counter-terrorist systems and the ground rules governing their operation are highly dependent on national legislations and regulations. Therefore, the decisions taken in each specific implementation of TACTICS would be crucial for the ethical and legal validation of the system, and each time it is used, a tailored and thorough assessment will be needed.

The report identified three main concerns associated with the implementation of a TACTICS-like system. These were:

(1) The system makes use of unreliable data (i.e. the quality of external data cannot be controlled).

(2) The TACTICS system may adversely affect public trust if it is over-used or used for unnecessarily extended durations.

(3) TACTICS may reveal methods, techniques and information that organizations may wish to keep secret.

The report recommends the use of a surveillance impact assessment (SIA) in further development of a TACTICS-like system. While such an assessment is not the ultimate tool to ensure that a project or a system

does respect fundamental rights, it is an occasion to consider the implications of the on-going work for fundamental rights. [D4.3].

4.3 WP 5: Capability management

WP 5 focused on supporting the capability management process in two ways. First, the project analysed which deviant behaviours can be detected best by which kind of sources. Second, the Capability Management Tool was developed based on the same principles as the tool in WP 4.

This WP reported that end users envisioned potential further uses for and/or extensions to the CMT beyond TACTICS, for instance the potential of being able to use the CMT to manage capabilities for intervening, as opposed to only capabilities to observe and detect. Furthermore, it was indicated that social networks could be used as information sources and/or to steer behaviour [D5.2; section 6] for further development.

The implications are that the TACTICS system could integrate additional capabilities and that more uses could be applied, therefore possibly expanding the possible impacts and/or implications. This, equally, leads to further considerations with regard to the transparency of the purpose of the system and the potential extension of use of the system beyond a situation of immediate threat.

4.4 WP 6: Threat Management

In **WP 6,** the threat management process was supported in two ways. First, the project designed a communication and cooperation framework taking into account psychological risks in communication and decisionmaking, such as confirmation bias and stereotyping. Second, the TMT was developed based on the same principles as the tools in WP 4 and WP 5, i.e. ensuring that commanding officers and their teams remain in charge of decisionmaking and thus in control of the situation.

D6.1. describes three groups of biases that can hamper decisionmaking when using TACTICS. They are:

- *Attention:* related to the limited capacity of humans to give equal attention to all signals presented to them, and the irrational ways in which people collect information
- *Categorization:* related to the way humans see other people, and the way they organize information
- *Interaction:* relates to obstacles in communication between humans or between humans and machines (e.g. a computer system)

The TACTICS system therefore integrates systems that help mitigate bias. However, it was also recommended to supplement this technological solution with bias-awareness training for the end users and system operators.

WP 6 reminds us that cognitive biases remain, and the introduction of a ‘system of systems’ should include aspects of training and wider consideration of the capability of the users of the technology. However, openly admitting and acknowledging these biases (and using a system that acknowledges and takes measures to counteract bias) could affect policy of governmental organizations using TACTICS and could improve efficiency and accuracy by way of fewer false positives and false negatives, therefore lessening tension between law enforcement officials/agencies and public citizens. Taking up these recommendations would enhance the significance and potential effects of the TACTICS counter-bias measures.

4.5 WP 7: Validation

The TACTICS system was tested in **WP 7**, where a validation of knowledge and tools was performed by using a scenario-based exercise of a terrorist threat taking place in the mythical city of Hamsterdam. It used the two urban environments chosen in WP 2, i.e., a sports stadium and a conference centre. The work included developing an appropriate experimental design, conducting the validation and evaluating the result.

D7.1 highlighted that speed was the added value indicated by end users as being what TACTICS could best bring to existing decisionmaking procedures. This is central to positively impacting upon the state of the art because it leads to subsequent added values, including increased performance, effectiveness and efficiency by making better informed decisions earlier. In the day-to-day practice of TACTICS end users, this could mean preventing a terrorist attack, saving lives, mitigating damage, and other impacts crucial to the safety and well-being of European citizens and cities. [D7.1; section 3]. However, the validation also indicated that

the implementation of a TACTICS system requires the presence of a pre-existing infrastructure to fully employ its potential. [D7.2; section 5].

The clear definition of communication and reporting lines, roles and responsibilities are critical for the successful use of TACTICS. [D7.2; section 5]. In order for TACTICS to be used to its full potential, it is fundamental that not only the tool operators, but also the managers are trained and aware of how to maximise the benefits of the system. [D7.2; section 5]. TACTICS is currently not designed to be a command and control system, but its architecture could be further developed to undertake this role. [D7.2; section 5]. Finally, it was indicated that there is potential use for applying TACTICS as a training tool for practitioners to develop their skills in a 'safe', non-critical but operational environment. [D7.2; section 5].

4.6 Summary

There are clearly lessons from previous deliverables that should be brought into the present deliverable. Previous deliverables have indicated the potential for a technological solution to enhance the decisionmaking process in the event of terrorist incidents, particularly through the increased speed of access to information, but also through the technology's potential to aid in bias mitigation. The introduction of a technology, particularly one that draws on behaviour and imagery analysis and personal data, must, however, always address the issues surrounding privacy and legality. These are issues that should be considered as part of the design or use assessment, e.g. surveillance impact assessment, as well as considered by national policy makers in light of their national legislation.

5 Analysis of case studies and relevant case law

In the methodology section, the rationale and approach for our case study selection and analysis was included. The case studies provided the project team with several important aspects that may have an impact on both the development of the deployment strategy and the generation of cross-European policy recommendations. Table 2 includes a quick summary of each case study, providing a brief contextualisation and the main considerations regarding community reception and counterterrorism effectiveness.

This chapter discuss the main findings from these case studies.[54]

Table 2. Overview of case studies and key findings on community reception and CT effectiveness

Case study	Context	Community reception	Counterterrorism effectiveness
Ring of Steel	• Surrounds City of London[55] • Checkpoints, CCTV, Automatic Number Plate Recognition (ANPR) • Installed in 1990s against the IRA threat	• Supported by businesses • Civil libertarians concerned about 'function creep' • Lack of meaningful public consultation	• Widely seen as successful • Used as template for initiatives elsewhere – could be seen as a marker of success • However, technology outdated
Project Champion	• Surrounded 2 Muslim areas in Birmingham • 200 CCTV/ANPR cameras • Installed in 2010 using £3m counterterrorism funding	• Public objections raised over lack of community consultation, 'scope creep', invasion of privacy and blanket targeting of Muslims	• Project scrapped in <1 year • Cameras never activated, so no measure of effectiveness available • Ongoing debates about utility of CCTV/ANPR
Passenger Name Record (PNR)	• Collection, retention and exchange of passenger data • €50m made available by European Commission for Passenger Name Record (PNR) programs in 14 member states in 2013	• Supported by most member states • Civil society concerns over proportionality, data retention, scope creep • Largely unnoticed by the public	• Mixed views on effectiveness • Weak evidence base on PNR and on mass surveillance tools more widely
e-Borders	• Advanced Passenger Information (API) programme • Implemented at UK airports • Commissioned in 2003 but never achieved full potential; name changed in 2010	• Human rights and data protection concerns raised by some civil liberties groups – but no wider public outcry	• e-Borders system provided security benefits to law enforcement agencies • However, effectiveness was limited by unwillingness of carriers to share API data
Body scanners	• Airport people-screening systems • Installed from 2007 in response to plane bombing attempts in 2000s	• Polls indicate 80% of US citizens support body scanners; 48% have privacy concerns • Body scanners generally preferred to hand-searches	• Experts divided on effectiveness of Advanced Imaging Technology (AIT) systems • Concealment tactics remain a security concern
ShotSpotter	• Gunshot detection system introduced in US in 1990s • Primarily used to target gun crime but provides transferrable lessons for counterterrorism	• Positive impact on community–police relations • Concerns over microphones recording conversations	• Insufficient evidence base on overall effectiveness • Benefits include enhancing officers' situational awareness • Problems include false positives
Police surveillance drones	• Unmanned Aircraft Systems capable of advanced surveillance for law enforcement purposes	• Privacy concerns raised by US public • Levels of permissiveness vary across different	• Limited available evidence on utility

[54] The full case studies are presented in Appendix E, including case law relevant to the research on counterterrorism.

[55] Covering the financial district.

	• Early phase of development	countries (e.g. India vs UK)	
Data Retention Directive (DRD)	• EU Directive adopted in 2006, which established the obligation to retain traffic and location data • Declared incompatible with fundamental rights by the Court of Justice of the European Union in 2014	• Heavily criticised, especially by civil liberties campaigners who held it causes harm to privacy and data protection rights	• Impact on counterterrorism difficult to estimate

There are a number of themes emerging from the analysis of the case studies. These are presented below thematically.

5.1 The level of engagement with the community impacted by the counterterrorism technology impact the implementation of the technology

The case studies show the importance of active and concerted communications efforts related to new security measures, as well as the consequences of poor communications strategies. The analysis of the case studies showed differences in the extent the technology was received by the community. The spectrum of case studies covered the case of an implementation going largely unnoticed by the public, as in the case with the transfer of PNR data, to one being heavily criticised by the public, as in the case of Project Champion. Clear communication appears to be key to successfully implementing new technologies in the field of CT and public security in general. For instance in the case of Project Champion, there was no public consultation initially when the surveillance initiative in Birmingham, UK, was installed targeting two Muslim wards. This blanket targeting provoked a community backlash, and cameras were hooded or relocated without ever being switched on. The impact was that this approach was highly damaging to relations between the Muslim community and West Midlands Police. Community engagement was vastly different in the case of the introduction of the e-Borders programme, an advanced passenger information programme, that was rolled out by the Home Office at UK airports between 2003 and 2014. Here e-Borders security personnel engaged with the Information Commissioner's office to ensure data was being used appropriately and in a way that took into account human rights concerns. The implementation team involved personnel from across multiple Law Engagement Agencies (police, immigration and customs staff) to promote information-sharing and more effective targeting. Representatives from EU MS (law enforcement professionals, oversight, academics) were invited to the UK police 'targeting centre' to provide feedback on the programme. The engagement applies to both internal communication and coordination among relevant stakeholders and agencies, as well as to public engagement, especially where a particular community may be affected by a CT surveillance initiative. Policy-makers at the WP 8 validation workshop, however, indicated, that although this is preferable, sometime timelines make it difficult to engage the community fully into the implementation process. It was also pointed out that, even within the communities, there are often different views about whether a technology is justified and appropriate to introduce to counter terrorism.

5.2 Effectiveness of CT measures

The findings indicate the necessity of ensuring that the introduced technologies are justified through their effectiveness in countering terrorism. For instance, in the case of body scanners, according to the Transportation Security Administration (TSA) of the United States, advanced imaging technology provides 'the best opportunity to detect metallic and non-metallic anomalies concealed under clothing without the need to touch the passenger.'[56] In contrast, the evidence base on the counterterrorism effectiveness of Passenger Name Record is extremely thin.[57] According to the European Parliamentary Research Service,

[56] Mowery et al. (2014); see also Mitchener-Nissen et al. (2012): '[with AIT] the TSA expects to be able to quickly, and without physical contact, screen passengers during primary and secondary inspection for prohibited items including weapons, explosives, and other metallic and non-metallic threat objects hidden under layers of clothing.'

[57] Research interview with Abraham Newman, Associate Professor, Georgetown University, 09 June 15; Research interview with an anonymous MEP, European Parliament, 09 July 15; Research interview with Diego Naranjo, Advocacy Manager, European Digital Rights, 30 June 15

'there seems to be no agreement as to whether PNR systems – and mass surveillance tools in general – are efficient'.[58] However, it was recognised that generally the effectiveness of CT interventions is difficult to assess. Mostly this is because the comparison between the handling of an incident supported by a technology and the handling of an incident not supported by a technology is pragmatically impossible. A suggestion may be to assess technologies and their use in a training environment, where these scenarios can be run. Also, there is the potential to review events and technology use post-incident, in order to identify areas where the technology operated effectively and where there are potential opportunities for further development. Two issues, however, make the measurement of effectiveness difficult: the lack of commonly used metrics to assess the effectiveness of CT measures and the problem of establishing a causal link between the technology and the effectiveness of a CT measure.

5.3 Resources dedicated to CT

The issue of resources lies at the heart of any effective counter-terrorist response. The most obvious of these focuses on the acquisition, training and deployment of the skilled personnel required and the cost of carrying out all the measures that are deemed necessary to combat the threat. However, at least as great a challenge is that the ownership and control of much of the technology that the counterterrorism effort draws on does not lie in the hands of counterterrorism practitioners. For example, CCTV camera systems may be owned by the municipal authority if they are in the street, or by local shops and businesses. Shopping malls, railway stations and airports are all likely to have extensive CCTV systems, each one owned and operated by different entities with their own priorities and aims. To utilise resources of this type on behalf of societies and communities to counter threats from terrorism is not only a challenge today in Europe; it will continue to be so for the foreseeable future.

5.4 Delicate balance between privacy and security

One of the benefits of technology is its empowerment of individuals to access the data and information made available to them by others from across the globe. Technologies are becoming increasingly complex and computer processing capabilities even better at dealing with large amounts of data. More and more data is being captured by organisations in the private domain about their users, which they can then exploit not only for marketing purposes but also for the personalisation of services. The public domain is also active here, and perhaps unsurprisingly, organisations find it harder and harder to keep secret their capabilities and operations. Information technology users today are therefore more aware of the issues of privacy and security and the tensions between the two.

If counterterrorism is not to be made unnecessarily difficult, an acceptable balance must be found between the need for security measures carried out on behalf of communities, on the one hand, and the individuals' general expectation of privacy and non-interference, on the other. As we saw in a number of our case studies (e.g. body scanners), the engagement with the community is critical for the acceptance of a particular CT measure. Where it does not occur, it can be damaging to the counterterrorism effort (e.g. Project Champion). This demonstrates that any opportunity to increase collaboration must be taken.

5.5 Potential for, and interest in, but difficulty with data sharing

The final area of challenge that has emerged involves the sharing of data and information for counterterrorism purposes. Its impact is felt across a wide spectrum. Within member states, it can occur between their own relevant organisations (or, indeed, even between different parts of the same organisation) and also between counterterrorism practitioners and those whose help and cooperation they seek e.g. technology providers, local communities and community-based organisations. Internationally, there are bilateral issues with it from member state to member state. Regionally, sharing information from member states to EU-wide bodies such as Europol, and even to those operating globally, such as Interpol, raises both fundamental and practical dilemmas.

[58] European Parliamentary Research Service (2015)

5.6 Respect for criteria of legitimacy, necessity and proportionality

The five law cases emphasise the crucial importance for counterterrorism policies and technologies to respect the criteria of legitimacy, necessity and proportionality set forth in the European Convention on Human Rights, and nowadays a cornerstone of the EU approach to fundamental rights too. It should also be noted that the technicalities of the counter-systems to be developed are highly relevant for assessing the overall proportionality of a measure. While counterterrorism is considered a legitimate aim and the court has recognized the importance of national activities in the field, this does not mean that national authorities have a blank cheque or can operate in a sort of state of exception. What matters is not what is technically possible, but how specific instruments and powers permit authorities to achieve clearly set purposes while ensuring appropriate safeguards.

6 Policy recommendations

Technology has played, and will continue to play, a central role in counterterrorism policy, strategy and operations. Recent years have seen rapid innovation and the development of new technological applications, such as facial recognition and biometrics, counter-IED, communications interception, airport security, explosive and weapon detection, and so on.

As described earlier in the report, there are a number of challenges for policy-makers in the context of the ever-increasing reliance on technology for countering terrorism in Europe today. Based on the research undertaken, particularly the case studies, we propose a number of policy recommendations drawn from these. These recommendations are also outlined below. The chapter concludes with reflections on the use of technologies by terrorists.

6.1 Policy recommendations

6.1.1 Recommendation 1: Deploy appropriate counterterrorism technologies that enhance decisionmaking, but be prepared for ongoing changes in the technology landscape

As is evident from the TACTICS project, technologies clearly have the potential to enhance the effectiveness of CT activities, provided they are appropriate for the use to which they are put and they are deployed and operated correctly. The technologies can, as demonstrated by the TACTICS system, introduce access to a wealth of additional information to improve the decisionmaking of end users during a time-critical situation. Furthermore, the technology itself can be used to prompt the user to consider whether cognitive biases have been introduced into the process, and whether the human operator needs to consider alternatives, thus reducing the risk of error and unwanted consequences. The human operator will, however, continue to be the most important element of the CT operations, because critical decisions must remain human decisions. Once more, technology can support the decisionmakers and ensure there is a full record of their use of it, the decisions they have made and the rationale behind them.

- **Future considerations are necessary.** The threat from terrorist attacks is becoming increasingly sophisticated as terrorists develop new ways to carry out attacks and use new technology itself to do so. As the case of body scanners highlights, it is necessary to continue to enhance developed technologies to overcome their potential technical limitations against new threats or the terrorists' exploitation of any limitations associated with existing technologies.
- **Over-dependence on technology can be problematic.** Unmitigated dependence is a good definition of vulnerability. In CT it might seem contrary to common sense that reliance on technologies as listed above could in itself represent a vulnerability, but this is precisely the case. If a security system relies, for example, on a very high level of communications intercept technology, then the terrorist adversary might respond by using 'low-tech' means. If highly developed systems fail for innocent infrastructural reasons, will there always be sufficient and effective 'reversionary modes' to hand? Over-reliance on technology in CT could be a double-edged sword simply because it might be based upon a complacent and simplistic understanding of the relationship between technology and security policy – for example, that the benefits of the former belong exclusively to those who believe they dominate the latter.

6.1.2 Recommendation 2: Apply a structured approach to deployment of counterterrorism technology

We propose the need to apply a structured deployment process with particular emphasis on the respect for national and European legislation and on the definition and respect for appropriate safeguards (as described in full detail in TACTICS deliverable D8.1 – TACTICS Deployment Strategy). The recommended deployment strategy has two key elements: first, a step-by-step deployment process that guides relevant decisionmakers in member states through a series of critical decision points, and, second, a deployment checklist covering the full range of factors (contextual and environmental, organisational and regulatory, technical and infrastructural, human, legal and ethical) that decisionmakers should consider. The combination of these two elements ensures that the scope and purpose of the system are clear from the start and that requirements for the technology are well understood and compatible with existing structures, infrastructures, laws and regulations. In addition, the proposed structured approach prompts decisionmakers to consider not only the

operational effectiveness of the technology, but also its ethical use, including its impact on local communities and its compliance with the principle of proportionality.

6.1.3 Recommendation 3: Carefully consider data collection and data sharing

Trusted partnerships, national and international, are by definition a prior necessity for effective data sharing. Where it is not possible to harmonise and/or share the data sources, it is recommended to work first towards standardising the data assumptions and taxonomies to facilitate potential future sharing of data structures and content. As demonstrated in the case of ANPR, it is vital to ensure that the need for mass collection of data is proportionate, necessary and justified. Similarly, the case of body scanners illustrates how to encourage the institution of an oversight mechanism – in this case one that monitors how body scanners collects and uses its data. This is particularly pertinent when there are issues of data sharing without guaranteeing protection of citizens' rights, or where there is a disproportionate data retention period (e.g. as evidenced in the PNR case study).

- Previous deliverables in TACTICS highlighted the need for the technology to be able to deal with specific urban environments, which may lend itself to different data requirements and outputs and which, in turn, may cause difficulties with regards to data sharing initiatives, not only between national agencies but also across international borders.

6.1.4 Recommendation 4: Deal early with considerations around privacy

It is recommended that when policy-makers consider the introduction of new technologies in the context of CT, they **identify** and **address** potential privacy issues as early as possible. As we have seen from the technologies in the case studies and in the TACTICS systems itself, the balance between privacy and security is pertinent. The case studies also demonstrate that there are civil liberties implications for whole communities, e.g., Project Champion or Ring of Steel. It is therefore recommended that impact assessments be undertaken on any community into which they are introduced or where they are used as early as possible, to determine what the potential impact of the intervention may be on the community and how it can be mitigated or removed. It should be noted that in early product development, it is possible to build in **privacy by design** in the development process (see D6.2 for further elaboration about the use of privacy by design) and this, too, should be incorporated from the very beginning. It is much easier to implement this upfront than to retrospectively fit in privacy measures.

- Despite the rhetoric of win–win in the context of protecting privacy and enhancing counterterrorism measures, the discrepancy between privacy and security can be wide and present a tricky balance for policy-makers to manage. Building in these considerations to the wider deployment strategy (see D8.1) and holding relevant parties to account for addressing them may be an appropriate approach to begin to tackle the issue.
- Policy-makers may also need to consider the impact on the local urban environment. Surveillance and overly controlling security measures potentially prevent people from enjoying the benefits that the urban environment has to offer. As D4.3 emphasised: 'While TACTICS as a system is promising in terms of improving the citizens' security in urban areas, it is necessary to accompany the development of the system with a level of critical awareness of the weaknesses and potential unintended consequences of such systems.'

6.1.5 Recommendation 5: Establish relevant partnerships and networks

Countering terrorism requires partnerships within all levels of national government, law enforcement agencies, private sector and the communities, as well as an integrated approach in collaboration with international partners and key allies. Partnership with citizens is equally important, as we have seen in the range of acceptance of the CT technologies in the case studies. Citizens need to be informed of the threat in an honest, straightforward manner to foster a deeper understanding of why particular actions are needed in response to the threat. Where possible, the involvement of relevant citizens in other forms of pre-deployment assessments could prevent potential issues later on in the deployment process. Multilateral fora can be established and nurtured in order to initiate and sustain dialogue and understanding, leading to an integrated approach to counterterrorism.

- While the idea of partnership of end users around design and development of new technologies in the context of CT may also be beneficial for reasons of cost and harmonisation of technology, there may be difficulties around this, particularly because the technology specification requirements differ between different end users.

- The first and most obvious challenge to European member states is that of establishing **trusted relationships** between governments and security agencies such that intelligence, early warning and analysis of terrorist threats can all be shared in a timely fashion. These trusted relationships must also be routinized, rather than require reinvention on a case-by-case basis. Unless it can be shown that it will add to the strength and security of participating member states, collaboration in this most delicate and closely-guarded area of national security policy will remain difficult and will yield little tangible benefit. But if trusted relationships can be formed then the path is open to address the next set of challenges to collaboration. These are of a more material nature, but no less taxing: can member states **cooperate** in their response to a terrorist threat? Can procedures, equipment and finances be shared? Could member states agree a set of **common standards**? And might it even be possible to agree a level of **role specialisation** among EU member states with, for example, some governments concentrating on the financial aspects of CT while others specialise in 'kinetic' operations?

6.1.6 Recommendation 6: Carry out regular audits and evaluations on the system use

The research indicates the need to introduce evaluation of the use of the technology on a regular basis. This is particularly important after each use of the TACTICS system, both to ensure that the system is effective, proportionate and thus necessary in relation to its purpose, and to further tune it to future use. In order to ensure that the technology is operationally effective in the context of counterterrorism, it is necessary to establish an approach to evaluating the use of the approach with regards to its effectiveness to meet its purpose. Another main benefit of undertaking evaluations is the potential to flag up capability needs as a result, in terms of either systems performance or operator/manager training needs. As identified in previous TACTICS deliverables, there is scope for using a TACTICS-like system for training purposes, and this would aid in the evaluation of the system.

Furthermore, if the system allows for access to personal data or introduces privacy issues in its use, the conduct of internal and/or external audits of the system use is recommended. As identified in the PNR case study, there is a need to establish appropriate mechanisms for independent review, potentially through the appointment of data protection officers. The presentation of reports also permits ensuring a transparent use of the system and, in turn, maintains a high level of trust from the community.

Evaluation is often seen as retrospective analysis of a project, programme or policy to assess how successful or otherwise it has been, and what lessons can be learnt for the future – in other words, it is something that should happen after a programme has been implemented. In this report we argue that although post-implementation assessment is the ultimate goal of evaluation, for an evaluation to be most robust, the evaluation design element should be part of the policy programme from the outset of any new initiative and should be carefully designed alongside the monitoring system.

6.2 Terrorists can also exploit the benefits of new technologies for their own ends

As a final consideration, linked to the first recommendation above, we note that the technology landscape is changing – and not only for governments and the counterterrorism practitioners. For terrorists, battle-winning, tactical weaponry and equipment might be little different in their effect from war-winning, strategic technology. Relatively commonplace technology can offer the strategic effect that the terrorist needs: as Amitav Malik notes, 'even moderate levels of technological capability in the wrong hands will have serious security implications'.[59] An example is the now-commonplace terrorist use of a mobile phone to initiate the detonation of improvised explosive devices, e.g. in the Madrid train bombings of 11 March 2003.

Technology of this sort might not only give terrorists a tactical success, it might also prevent their strategic defeat and allow their attacks to continue, which terrorists can then propagandise as 'victory'. Perhaps at this level, terrorists can be said to be taking a more pragmatic approach to technology than do the governments they confront. Terrorists can be capable of innovation and ingenuity, as Bruce Hoffman's account of the evolution of IRA bomb-making makes clear.[60] Furthermore, when terrorists do innovate they can present a low–high span of inventiveness which governments might find hard to match – particularly governments

[59] Mallik (2004) p. 122
[60] Hoffman (2006) pp. 252–4

which assume the technology–strategy relationship to be a matter of constant striving for ever more sophisticated and decisive innovation, as well as something only within the scope of their own control.

Technology is central to both terrorism and counterterrorism, yet each side sees technology in a different way. For the governments of advanced liberal democracies, technology has long been expected to confer a decisive advantage in battle and war, and something of this expectation can be discerned in counterterrorism policy and strategy. For terrorists, however, technology is tactical; it is a means to an end.

7 References

Afzal, Saima, Mike Hughes & Paul Fitzgerald. 2012. *West Midlands Police Authority: Post Implementation Review of Project Champion – Recommendations*. As of 27 August 2015: http://www.westmidlands-pcc.gov.uk/media/57254/12_PoliceAuthority_21Jun12_Project_Champion_External_Review_Appendix1.pdf

Archick, Kristin. 2014. *US–EU Cooperation against Terrorism.* Washington, DC: Congressional Research Service.

Associated Press, The. 2012. 'TSA Quietly Removing Some Full Body Scanners.' *CBS News*. October 25. As of 27 August 2015: http://www.cbsnews.com/news/tsa-quietly-removing-some-full-body-scanners/

Awan, Imran. 2011. A Lesson in How Not to Spy on Your Community? *Criminal Justice Matters* 83(1): 10–11.

Bigo, Didier, and Anastasia Tsoukala. 2008. *Terror, Insecurity and Liberty. Illiberal Practices of Liberal Regimes*. London: Routledge.

Birmingham City Council. 2010. *Project Champion: Scrutiny Review into ANPR and CCTV Cameras.* Birmingham, UK: Birmingham City Council.

Boehm, Franziska. 2011. 'EU PNR: European Flight Passengers under General Suspicion – The Envisaged European Model of Analyzing Flight Passenger Data.' In *Computers, Privacy and Data Protection: An Element of Choice*, edited by Serge Gutwirth, Yves Poullet, Paul De Hert, Ronald Leenes. New York: Springer.

Bourg, Allison. 2014. 'New Crime-Fighting Technology Comes to Baltimore.' *ABC2*. March 12. As of 27 August 2015: http://www.abc2news.com/news/region/baltimore-city/new-crime-fighting-technology-comes-to-baltimore

Buttarelli, Giovanni. 2011. Counterterrorism Policy and Data Protection (Hearing of the European Economic and Social Committee). Brussels: European Economic and Social Committee.

Byman, D., & A.K. Cronin. 2013. 'Death from Above: Are Drones Worth It?' Byman vs. Cronin. *Foreign Affairs* July/August 2013.

Casale, David. 2008. EU Institutional and Legal Counterterrorism Framework. *Defence Against Terrorism Review* 1: 49-78.

Chang, Giselle. 2008. 'City Police Tests New Gunshots Detection System' *The Johns Hopkins News-Letter*. November 19. As of 27 August 2015: http://www.jhunewsletter.com/2008/11/19/city-police-tests-new-gunshot-detection-system-96969/

Choi, Kyung-Shick, Mitch Librett & Taylor J. Collins. 2014. 'An Empirical Evaluation: Gunshot Detection System and Its Effectiveness on Police Practices.' *Police Practice and Research* 15(1): 46–61.

City of London Police. 2013. Ring of Steel: Visions and Aspirations – Update. Report of Commissioner of Police. As of 27 August 2015: http://democracy.cityoflondon.gov.uk/documents/s21087/130515%20POL_19-13_Ring_of_Steel_update_final.pdf

Coaffee, Jon. 2004. 'Rings of Steel, Rings of Concrete and Rings of Confidence: Designing out Terrorism in Central London Pre and Post September 11th.' *International Journal of Urban and Regional Research* 28(1): 201–211.

Coaffee, Jon. 2009. *Terrorism, Risk and the Global City: Towards Urban Resilience.* Farnham, UK: Ashgate.

Coaffee, Jon, & Pete Fussey. 2015. 'Constructing Resilience through Security and Surveillance: The Politics, Practices and Tensions of Security-Driven Resilience.' *Security Dialogue* 46(1): 86–105.

Council of the European Union, 1995. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031–0050

Council of the European Union. 2004. Declaration on combating terrorism. Brussels: Council of the European Union.

Council of the European Union, 2002. Council Decision of 19 December 2002 *on the implementation of specific measures for police and judicial co-operation to combat terrorism in accordance with article 4 of*

the Common Position 2001/931/CSFP, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003D0048&from=EN

Council of the European Union. 2010. Draft Internal Security Strategy for the European Union: 'Towards a European Security Model', Brussels: Council of the European Union.

Council of the European Union. 2014. 'Development of a renewed European Union Internal Security Strategy', Brussels: Council of the European Union.

Council of the European Union. 2014. 'Report on the implementation of the EU Counterterrorism Strategy', From the EU Counterterrorism Coordinator, to the Council, Brussels, 24 November 2014, 15799/14.

Council of the European Union. 2015. 'Council Conclusions on counterterrorism', 9 February 2015, http://www.consilium.europa.eu/en/press/press-releases/2015/02/150209-council-conclusions-counterterrorism/

Council of the European Union, 2010. Official Journal of the European Union. The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens (2010/C 115/01), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010XG0504%2801%29&from=EN

Davis, Fergal, Nicola McGarrity & George Williams, eds. 2013. *Surveillance, Counter-Terrorism and Comparative Constitutionalism.* London: Routledge.

Economist, The. 2014. 'Calling the Shots.' September 13. As of 27 August 2015: http://www.economist.com/news/united-states/21617018-how-gunshot-detecting-microphones-help-police-curb-crime-calling-shots

Elias, Bart. 2012. *Airport Body Scanner: The Role of Advanced Imaging Technology in Airline Passenger Screening.* Washington DC: Congressional Research Service.

European Commission. 2010. Communication from the Commission. Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union. Brussels European Commission.

European Commission. 2012. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final. Brussels: European Commission.

European Commission. 2012. Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. COM (2012) 10 final. Brussels: European Commission.

European Commission, 2015. The European Agenda on Security, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee And the Committee of the Regions, Strasbourg 28.4.2015, COM(2015) 185final, http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

European Commission. 2011. Evaluation Report on the Data Retention Directive (Directive 2006/24/EC). Brussels: European Commission.

European Court of Justice. 2014. Joined cases: Digital Rights Ireland v Ireland and Seitlinger and Others (C-293/12 and C-594/12)

European Parliament. 2015. Foreign Fighters': Member States' Responses and EU Action in an International Context. Briefing. As of 27 August 2015: http://www.europarl.europa.eu/EPRS/EPRS-Briefing-548980-Foreign-fighters-FINAL.pdf

European Parliamentary Research Service. 2015. The Proposed EU Passenger Name Records (PNR) Directive: Revived in the New Security Context. Briefing.

Fenton, Justin, & Carrie Wells. 2014. 'Gunfire May Be Four Times as Common as Reported, Contractor Says.' *The Baltimore Sun.* April 20. As of 27 August 2015: http://articles.baltimoresun.com/2014-04-20/news/bs-md-ci-gunshot-detection-report-20140420_1_baltimore-police-gun-discharges-gun-violence

Fussey, Pete. 2013. 'Contested Topologies of UK Counterterrorist Surveillance: The Rise and Fall of Project Champion.' *Critical Studies on Terrorism* 6(3): 351–370.

Fussey, Pete, & Jon Coaffee. 2011. 'Olympic Rings of Steel: Constructing Security for 2012 and Beyond', In *The Security Games: Surveillance and Control at Mega Events,* edited by C. Bennett & K. Haggerty London: Routledge.

González Fuster, Gloria. 2014. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Dordrecht: Springer.

Goode, Erica. 2012. 'Shots Fired, Pinpointed and Argued Over.' *The New York Times.* May 28. As of 27 August 2015: http://www.nytimes.com/2012/05/29/us/shots-heard-pinpointed-and-argued-over.html?pagewanted=all&_r=0

Graham, Stephen, ed. 2004. *Cities, War, and Terrorism: Towards an Urban Geopolitics*. Oxford, UK: Blackwell Publishing.

Graham, Stephen. 2011. *Cities under Siege: The New Military Urbanism*. London: Verso.

Greenberg, Andy. 2014. 'Researchers Easily Slipped Weapons past TSA's X-ray Body Scanners.' *Wired*. August 20. As of 27 August 2015: http://www.wired.com/2014/08/study-shows-how-easily-weapons-can-be-smuggled-past-tsas-x-ray-body-scanners/

Guardian, The. 2015. 'Europe's Great Plane Data Grab.' January 28.

Guardian, The. 2010. 'Surveillance Cameras in Birmingham Track Muslims' Every Move.' June 4.

Hobbing, Peter. 2008. 'Tracing Terrorists: The EU–Canada Agreement in PNR Matters.' Centre for European Policy Studies.

Hoffman, Bruce. (2006). *Inside terrorism*, 2nd rev. edn. New York: Columbia University Press.

Horsley, Thomas. 2015. 'The Court Hereby Rules…' – Legal Developments in EU Fundamental Rights Protection.' *Journal of Common Market Studies* no. Early View: 1-20.

Isakjee, Arshad. 2011. Project Champion and the Securitisation of Muslim Space in Birmingham. Paper presented at the international RC21 conference, Amsterdam, 7–9 July.

Jackson, Brian A; Baker, John C; Cragin, Kim., Parachini, John; Trujillo, Horacio R. (2005) *Aptitude for Destruction.* Vol. 2, *Case Studies of Organizational Learning in Five Terrorist Groups.* Santa Monica, Calif.: RAND Corporation

Johnson, Joel. 2010. 'One Hundred Naked Citizens: One Hundred Leaked Body Scans.' *Gizmodo*. November 16. As of 27 August 2015: http://gizmodo.com/5690749/these-are-the-first-100-leaked-body-scans

Kelly, Owen. n.d. 'The IRA Threat to the City of London: Limiting Access to the City Reduced Terrorist Attacks.' As of 31 August: http://www.rjerrard.co.uk/law/city/irathreat.htm.

Lekka, Chrysanthi. 2011. *High reliability organisations: A review of the literature*. Health and Safety Executive, Research Report RR899, 18: http://www.hse.gov.uk/research/rrpdf/rr899.pdf (accessed 7 August 2015).

MacKenzie, Alex, Kaunert, Christian, and Léonard, Sarah. 2015. 'Counterterrorism: Supranational EU institutions seizing windows of opportunity', in *Policy Change in the Area of Freedom, Security and Justice: How EU institutions matter*, ed. By Florian Trauner and Ariadna Ripoll Servent, London and New York: Routledge.

Malik, Omar. 2000. *Enough of the Definition of Terrorism*. London: Royal Institute of International Affairs, p.xvii.

Mallik, Amitav. 2004. *Technology and Security in the 21st Century: A Demand-Side Perspective*. SIPRI Research Report 20. Oxford: Oxford University Press/Stockholm International Peace Research Institute.

Mowery, Keaton, Eric Wustrow, Tom Wypych, Corey Singleton, Chris Comfort, Eric Rescorla, Stephen Checkoway, J. Alex Halderman & Hovav Shacham. 2014. *Security Analysis of a Full-Body Scanner*.

Mitchener-Nissen, Timothy, Kate Bowers & K. Chetty. 2012. 'Public Attitudes to Airport Security: The Case of Whole Body Scanners.' *Security Journal* 25(3): 229–243.

Mironenko, Olga. 2011. 'Body Scanners versus Privacy and Data Protection.' *Computer Law & Security Review* 27: 232–244.

Murphy Cian C. Arcarazo, Diego Acosta. 2014. 'Rethinking Europe's Freedom, Security and Justice', in Arcarazo, Diego Acosta and Murphy, Cian C (eds.), *EU Security and Justice Law: After Lisbon and Stockholm*, Hart Publishing, UK.

Neocleous, Mark. 2007. 'Security, Liberty and the Myth of Balance: Towards a Critique of Security Politics', *Contemporary Political Theory* no. 6 (2):131-149

Newman, Abraham. 2011. 'Transatlantic Flight Fights: Multi-level Governance, Actor Entrepreneurship and International Anti-terrorism Cooperation.' *Review of International Political Economy* 18(4): 481–505.

New York City Global Partners. 2010. Best Practice: Comprehensive City-wide Security System [London]. As of 27 August 2015: http://www.nyc.gov/html/ia/gprb/downloads/pdf/London_RingofSteel.pdf

New York Times, The. 2015. 'EU Works on Air Passenger Deal to Track Foreign Fighters.' February 24.

New York Times, The. 2005. 'To Fight Terror, New York Tries London's "Ring of Steel".' July 24.

New York Times, The. 2007. 'Manhattan Takes Cue from London's "Ring of Steel".' July 9.

Petho, Andreas, David S. Fallis & Dan Keating. 2013. 'ShotSpotter detection system documents 39 000 shooting incidents in the district.' *The Washington Post*. November 2. As of 27 August 2015: http://www.washingtonpost.com/investigations/shotspotter-detection-system-documents-39000-shooting-incidents-in-the-district/2013/11/02/055f8e9c-2ab1-11e3-8ade-a1f23cda135e_story.html

Ram, Ed. 2014. 'UK Gun Crime: Should Police Retry Gun Sensor Technology?' *BBC News*. July 14. As of 27 August 2015: http://www.bbc.com/news/technology-28004190

Ripoll Servent, A., MacKenzie, A. 2012. 'The European Parliament as a 'Norm Taker'? EU-US Relations after the SWIFT Agreement', *European Foreign Affairs Review*, 17 (Special Issue 2/1), pp. 71-86.

Robinson, Neil, Dimitris Pottoglou, Chong Woo Kim, Peter Burge & Richard Warnes. 2010. *Security, at What Cost? Quantifying People's Trade-offs across Liberty, Privacy and Security.* Santa Monica, Calif.: RAND Corporation.

Rymer, T. (2008) *e-Borders: EU Friend of the Presidency Group Meeting*, Brussels. Unpublished PowerPoint presentation by former Head of Joint Border Operations Centre, 27 March 2008.

Schlossberg, Tatiana. 2015. 'New York Police Begin Using ShotSpotter System to Detect Gunshots. *The New York Times*. March 16. As of 27 August 2015: http://www.nytimes.com/2015/03/17/nyregion/shotspotter-detection-system-pinpoints-gunshot-locations-and-sends-data-to-the-police.html?_r=0

Sedat, John, David Agard, Marc Schuman & Robert Stroud. 2010. Letter of concern to John P. Holdren, Assistant to the US President for Science and Technology. April 6. As of 27 August 2015: http://www.npr.org/assets/news/2010/05/17/concern.pdf

Selby, Nick, David Henderson & Rara Tayyabkhan. 2011. *ShotSpotter Gunshot Location System Efficacy Study*. CSG Analysis.

Statewatch. 2011. 'European Commission's Legal Service Says EU–USA PNR Agreement Is "Not Compatible with Fundamental Rights".' As of 27 August 2015: http://www.statewatch.org/news/2011/jun/03eu-us-pnr-com-ls.htm

The Health Foundation. 2011. *High Reliability Organisations: Evidence Scan*, November 2011, p.3: http://www.health.org.uk/sites/default/files/HighReliabilityOrganisations.pdf (accessed 7 August 2015).

Thomson, Iain. 2014. 'E-Borders Fiasco: Brits Stung for 224 Million Pounds after US IT Giant Sues UK Government.' *The Register.* August 19. As of 27 August 2015: http://www.theregister.co.uk/Print/2014/08/19/raytheon_payout_uk_e_borders/

Thornton, Sara. 2010. *Project Champion Review*. Thames Valley Police. As of 27 August 2015: http://www.statewatch.org/news/2010/oct/uk-project-champion-police-report.pdf

US Department of Homeland Security. 2011. Testimony of David Heyman, Assistant Secretary, Office of Policy, before the House Committee on Homeland Security Subcommittee on Counterterrorism and Intelligence: "Intelligence Sharing and Terrorist Travel: How DHS Addresses the Mission of Providing Security, Facilitating Commerce and Protecting Privacy for Passengers Engaged in International Travel". Washington DC: Department of Homeland Security.

Van Brunschot, Erin Gibbs and Leslie W. Kennedy. 2008. *Risk Balance & Security*, London: Sage.

Vine, J. 2013. *Exporting the Border? An Inspection of e-Borders October 2012–March 2013*. Independent Chief Inspector of Borders & Immigration.

Waddell, Kaveh. 2015. 'Few Privacy Limitations Exist on How Police Use Drones.' *National Journal.* February 5. As of 27 August 2015: http://www.nationaljournal.com/tech/few-privacy-limitations-exist-on-how-police-use-drones-20150205

Waldron, Jeremy. 2003. 'Security and Liberty: The Image of Balance', *The Journal of Political Philosophy*, no. 11 (2):191-210

West Midlands Police Authority. 2012. *Equalities, Diversity and Human Rights (EDHR) Annual Report*. Birmingham: West Midlands Police Authority.

Wolff, Sarah. 2009. 'From the Hague to Stockholm: the Future of EU's Internal Security Architecture and Police Cooperation', Overview Paper, Clingendael European Studies Programme (CESP) Round Table seminar,. http://www.clingendael.nl/sites/default/files/20090930_cesp_paper_swolff_police_cooperation.pdf

Appendix A List of interviewees

Name	Affiliation	Expertise
Marcus Beale	Assistant Chief Constable, West Midlands Police, UK	Project Champion
Alex Deane	Former Director, Big Brother Watch, UK	Project Champion
Diego Naranjo	Advocacy Manager, European Digital Rights, Belgium	e-Borders and Passenger Name Record (PNR)
Lorraine Mazerolle	Professor, University of Queensland, Australia	ShotSpotter
Tony Porter	Surveillance Camera Commissioner, Home Office, UK	Ring of steel, Project Champion, and police surveillance drones
Kimo Quaintance	Lecturer, George C. Marshall European Center for Security Studies, Germany	Police surveillance drones and ShotSpotter
Glenn Schoen	CEO, Boardroom@Crisis, US	Counterterrorism measures and civil liberties
Steve Swain	Former Head of the Police International Counter Terrorism Unit (PICTU), UK	Ring of steel
Anonymous[61]	Former e-Borders Project Executive, Home Office, UK	e-Borders and PNR
Anonymous	Junior Officer, Royal Netherlands Marechaussee, Netherlands	Dutch policing
Anonymous	Anonymous Police Officer, France	Facial recognition technology
Anonymous	Former Senior Executive, anonymous human rights organisation, UK	Ring of steel
Anonymous	Analyst, anonymous research institute, US	PNR
Anonymous	Public Servant, anonymous national policing body, UK	UK policing
Anonymous	Senior Officer, anonymous police force, UK	e-Borders and PNR
Anonymous	Senior Officer, anonymous police force, UK	Project Champion

[61] Owing to the sensitive nature of their professional roles, some of our experts wished to remain anonymous in the report.

Name	Affiliation	Expertise
Anonymous	Associate Professor, anonymous university, US	PNR
Anonymous	Academic, anonymous university, Germany	Body scanners
Anonymous	Analyst, anonymous human rights organisation, UK	CCTV and civil liberties
Anonymous	Professor, anonymous university, US	CCTV and civil liberties
Anonymous	Anonymous MEP, European Parliament, Belgium	PNR
Anonymous	Former Senior Officer, anonymous police force, UK	Project Champion

Appendix B Interview Protocol for Expert Interviews

***Note**: this protocol was tailored to each of the different case studies. For some case studies (e.g. Ring of Steel), the interviewers found it more appropriate to talk about 'this initiative' or 'the technologies used as part of this initiative' rather than 'this technology'.*

RAND Europe study: 'Tactical approach to counter terrorists in cities'

Interview protocol: [Case study]

CORE QUESTIONS

Part A: Interviewee background

1. Please could you tell us about your current position: What is your role in relation to [Case study]? Which positions have you held previously that would be relevant for this study?

Part B: Case study context

2. Please briefly describe the [Case study]. [*Prompts:* How does the technology work? How have its applications changed over time and how is it used today?]
3. What is the purpose of deploying this technology?

Part C: Technology implementation

4. Who was responsible for introducing, implementing and overseeing the technology?
5. How was the technology implemented? [*Prompts (if applicable):* How was a capability gap identified? How were operational, technical and legal requirements determined? Was a feasibility study undertaken? Which commercial procedures did the procurement process involve? Which actions were taken before deployment (e.g. aligning legislation, training)?]
6. How far has the private sector been involved in the design, development and implementation of this technology? Have there been any challenges regarding collaboration between public and private sector actors?
7. What - if any - were the main challenges faced during the implementation of the technology? How were these addressed?

Part D: Evaluation

8. How has this technology been received by the public? By the policy community?
9. How, if at all, has public/policy community reception been measured?
10. How far has the technology achieved its objectives? Explain.
11. Is it possible to measure the operational effectiveness of this technology? If so, how? Have any evaluations been conducted? Is the technology generally considered to be an operationally effective CT tool?
12. This study is examining potential trade-offs between security and human rights considerations. To what extent were these issues discussed during/after the technology's implementation?
13. If you had to make three policy recommendations regarding the use of this technology in counterterrorism, what would they be? [*prompt*] What are the main lessons learnt for law enforcement practitioners?
14. Do you have anything further to add before we close?

ADDITIONAL QUESTIONS: case study-specific questions

Appendix C Validation workshop

Subject	**TACTICS WP8 Workshop**
Location	Résidence Palace, Brussels
Date	Wednesday 15 July 2015

Agenda

15.30 Welcome by RAND Europe

1. What is TACTICS?
2. 5 minutes video clip from the Valencia presentation

15.40 Presentation of findings from TACTICS

1. The EU policy landscape (PRIO)
2. The research (RAND)
3. The deployment strategy (RAND)
4. The cross-European policy recommendations (RAND)

16.30 Facilitated discussion on the policy implications (RAND)

17.00 Reception

10 participants from across NATO, end-user community and European Institutions attended the small facilitated workshop.

Summary of discussion and questions

Participants were interested in the presentation and the topic area. In particular, they proposed additional information on:

1. Evaluation of the effectiveness of CT Technologies: How do you measure the effectiveness of the technologies, what should be the metrics, how use after-lesson reports and reviews?
2. If it is only used for rare events, how ensure that people are trained and confident at using the system for those events
3. Sometimes it is not possible to engage the community although it would be nice to do it. Sometimes there is an urgency to act, e.g. liquids on airlines, etc. Also there will be conflicting views even within the community and interest groups.
4. There are a lot of technologies out there and the specification requirements may different between different law enforcement environments, so it is necessary to work closely with the technology vendors, and also take equipment and adapt it to the specific environment.
5. May need to also look at the European approach to Detection.
6. The participants were in favour of the deployment approach of giving people a structured way of looking at deploying technologies.

Appendix D List of TACTICS deliverables

Work package	Work package title (Work package leader in brackets)	Deliverable(s)
2	User requirements & scenario definition (ITTI)	D2.1 Urban characteristics influencing terrorism and counter-terrorism D2.2 Requirements specification D2.3 Specification of scenarios and KPI D2.4 Recommendations and guidelines to respect privacy
3	System design (TNO)	D3.1 White paper with the conceptual framework including interoperability with the systems context D3.2 System architecture: design patterns and interfaces
4	Threat decomposition (RAND)	D4.1 Compendium of scenario-based attack profiles and compendium of full scenarios D4.2 Terrorist behaviour models for selected scenarios D4.3 Report on issues of privacy and civil rights linked to surveillance of urban areas and on the legal rights–based implications of pre-emptive technologies in urban areas. D4.4 (Non-) Functional Requirements for TDT D4.5 Development of Threat Decomposition Tool
5	Capability management (FHG)	D5.1 Capability description Language D5.2 Algorithm for matching actors' information needs with capabilities D5.3 Capability Management Concept D5.4 Report on privacy, ethics, human rights, legal conditions D5.5 Functional requirements specification D5.6 Capability Management Tool development
6	Threat management (UPV)	D6.1 Overview of possible risks in decision-making and decision support strategies to decrease these risks D6.2 Overview of human rights and ethical principles D6.3 A fusion unit that merges the output of several sensors to create a dynamic live common object model D6.4 Information Management Tool functional requirements D6.5 Information Management Tool development
7	Validation (ISCA)	D7.1 Validation design D7.2 Data analysis report D7.3 Implementation manual
8	Deployment strategy and policy recommendations (RAND)	D8.1 Deployment strategy (EU-wide)
		D8.2 Policy and strategic impacts, implications and recommendations
9	Dissemination and exploitation (MORPHO)	D9.1 Web portal with an overview of the total programme, its progress and the results of the separate work packages, delivered in successive modules
		D9.2 Database with institutions and experts relevant to TACTICS
		D9.3 Four workshop meetings and closing conference

Appendix E: Case studies

7.1 Case study 1: Ring of Steel

7.1.1 Context

London's 'Ring of Steel' is one of the first and best-known examples of wide-area surveillance in Europe.[62] Surrounding the Square Mile (the City of London), the Ring of Steel consists of concrete barriers, roadblocks, CCTV cameras, Automatic Number Plate Recognition (ANPR) cameras and police checkpoints. This form of 'fortress urbanism' was first established in the early 1990s by the City of London Police, the Metropolitan Police Service, and the City of London Corporation, and it is currently undergoing a new phase of technology development.[63]

The Ring of Steel was installed in response to the threat from Irish Republican terrorism. In the 1990s, the Provisional Irish Republican Army (PIRA) successfully attacked a number of key economic targets in the Square Mile, causing trade disruptions and sparking fears that businesses would relocate out of London. The Ring of Steel has been fortified since 9/11 as a result of the City's continued exposure to terrorist risk, as marked by the 7/7 attacks and a reported al-Qaeda plot to bomb the Square Mile. The scheme's purpose is not only to prevent and respond to terrorist attacks; crime prevention and road safety are also key objectives.[64]

7.1.2 Civil liberties implications

The Ring of Steel has largely been accepted by the Square Mile's business community. The Corporation of London has taken steps to engage with City representatives, for example by providing additional policing in areas bordering the City to address their concerns about displacing risk to the 'collar zone'.[65] While the Corporation of London has engaged effectively with the business community, it has failed to consult the wider public to the same extent.[66] Coaffee (2009) goes as far as to claim that the City only paid 'lip-service' to public consultation about ideas that it had effectively already decided to implement.[67]

Civil libertarians have also raised objections over the hidden counter-terrorism purpose of the initiative. The Ring of Steel was initially represented as a traffic control initiative, while its counter-terrorism and crime prevention purposes were downplayed. The use of facial recognition software to identify suspects entering the Square Mile is another aspect of the initiative that has not been communicated to the public.[68] Gareth Crossman, former Policy Director at Liberty (the National Council for Civil Liberties), highlighted this issue of 'function creep', where '*we are told that a system is being set up and used for a certain purpose and then we find out it is being used for another totally different one*'.[69]

The Ring of Steel has also provoked privacy concerns. While the right to privacy is enshrined in the European Convention on Human Rights 1953, the UK Human Rights Act 2000, and the UK Data Protection Act 1998, criticisms have been raised regarding the intrusive nature of CCTV.[70] In some cases, it has been challenging to assure residents that the City of London Police have only been collecting information for appropriate uses, such as identifying a vehicle involved in criminal activity, and not abusing the technology to

---

[62] Davis et al., eds. (2013)

[63] New York City Global Partners (2010); Research interview with Tony Porter, Surveillance Camera Commissioner, UK Home Office, 13 July 15

[64] City of London Police (2013)

[65] City of London Police (2013); Research interview with a former Senior Executive, anonymous UK human rights organisation, 08 May 15; Research interview with Steve Swain, former Head of the UK Police International Counter Terrorism Unit (PICTU), 07 May 15

[66] Research interview with Tony Porter, Surveillance Camera Commissioner, UK Home Office, 13 July 15

[67] Coaffee (2009)

[68] Coaffee (2004)

[69] Crossman in Graham, ed. (2004)

[70] Robinson et al. (2010)

violate privacy.[71] Nonetheless, as the Square Mile is mainly populated by businesses, fewer concerns have been raised by locals in this case than in response to initiatives based in residential areas.

7.1.3 Counter-terrorism effectiveness

The Ring of Steel is widely considered to have been successful. The initiative went a significant way to countering the PIRA threat by providing a deterrent and leading to a reduction in recorded attacks.[72] Moreover, UK officials said that images captured by the cameras helped track suspects following the 7/7 London bombings.[73] The benefits of the Ring of Steel have also extended beyond counter-terrorism: recorded crime levels have fallen, traffic accidents have decreased and pollution levels have dropped.[74]

Public–private sector collaboration has increased the Ring of Steel's resilience. After the 1993 Bishopsgate bombing, for example, the City of London introduced a new system called Camera Watch. Under the scheme, the force logged all business-owned CCTV camera systems and encouraged their owners to coordinate in order to reduce overlap and to share monitoring as appropriate. The force encouraged City businesses to install their own CCTV systems outside their premises as an additional deterrent to terrorist attacks and provided advice on how to better protect their buildings, information technology (IT) systems and databases. Camera Watch proved operationally effective because it led to a reduced level of terrorist activity.[75]

Another indicator of the Ring of Steel's success is its use as a template for similar initiatives elsewhere. For example, a security cordon was installed in London's second financial hub, at Canary Wharf (the Docklands), following PIRA attacks in the 1990s. Like the Square Mile's Ring of Steel, this 'Iron Collar' consisted of entry point policing, ANPR cameras and CCTV cameras. The Ring of Steel also provided a template for Olympic Games security planning in 2012. When discussing the Olympic construction programme, the then Metropolitan Police security coordinator for the 2012 Games, Assistant Commissioner Tarique Ghaffur, described the Ring of Steel as an exemplar for the Olympic security regime.[76] The Square Mile–based scheme also influenced the development of a similar scheme in Manhattan in 2007: the Lower Manhattan Security Initiative.[77]

Although the Ring of Steel has widely been hailed as a success, several criticisms have also been raised. One was that the Ring of Steel would simply displace the risk of attacks to the areas bordering the cordon. In Belfast, where a similar ring had been installed in the 1970s, car bombers had targeted areas just outside the ring or had shifted their focus onto alternative, 'softer' targets.[78] However, extra police patrols were deployed at the 'collar zones' of London's Ring of Steel in order to mitigate this risk.[79]

The Ring of Steel has tended to be more successful in identifying perpetrators *after* attacks have taken place than in preventing the incidents in the first place. For all of its comprehensiveness, the Ring of Steel did not prevent the July 2005 subway bombings or the attempted car bombings in June 2007. In the car bomb plots, for example, the cameras proved useful in tracing the suspects, but only after the attacks were attempted.[80] The effectiveness of the Ring of Steel as a preventative tool for counter-terrorism has therefore been limited.

7.1.4 Implementation challenges

Legal constraints impeded the early implementation of the Ring of Steel.[81] According to Commissioner Owen Kelly, the police had a '*lack of legal powers*' for stop and search in the early 1990s and the government had

---

[71] Coaffee (2004); New York City Global Partners (2010)

[72] Research interview with Steve Swain, former Head of the UK Police International Counter Terrorism Unit (PICTU), 07 May 15

[73] The New York Times (2007); Kelly (n.d.)

[74] Kelly (n.d.)

[75] Kelly (n.d.)

[76] Fussey and Coaffee (2011)

[77] Graham (2011); The New York Times (2007)

[78] Coaffee (2000) in Graham, ed. (2004)

[79] Coaffee (2009)

[80] The New York Times (2007; 2005)

[81] Ford (1993) in Coaffee, ed. (2004)

an 'apparent lack of resolve to give [the police] new powers'.[82] Restrictions under PACE (the Police and Criminal Evidence Act 1984) made it impossible to set up permanent checks on vehicles entering the City. PIRA terrorists exploited this legal loophole in 1992: with mobile communications and a scout ahead to alert them if a police check was operating, the terrorists were easily able to drive the lorry carrying the bomb into Bishopsgate.

With a rapidly changing terrorist landscape and continuous technological innovation, it has also been challenging for practitioners to stay one step ahead of the threat.[83] In a 2013 report, the City of London Police acknowledged that the methods used by terrorist groups had developed beyond the capability of the existing Ring of Steel infrastructure. At that time, the system was said to be struggling to meet National Association of Chief Police Officers (ACPO) ANPR standards in terms of functionality, with read rates on ANPR cameras falling below the required standard and the poor picture quality of CCTV footage having a detrimental impact on intelligence gathering. As the initiative's outdated technologies left the City in a state of potential vulnerability, the decision was taken to invest in new infrastructure to ensure that the system was operationally fit for purpose.[84]

7.2 Case study 2: Project Champion

7.2.1 Context

Project Champion was an abortive project to install 290 CCTV and ANPR cameras in Birmingham. Initiated in late 2007 by the West Midlands Police, the scheme introduced surveillance cameras in two largely Muslim areas of the city: Washwood Heath and Sparkbrook.[85] More than half of the cameras were equipped with ANPR capability in order to monitor vehicles entering and exiting the areas and a further 72 covert cameras were concealed in street signs and other features of the urban landscape.[86] Community opposition and an investigation led by *The Guardian* resulted in the suspension of the initiative in June 2010. This 'ring of surveillance' vehicle monitoring approach was not unique to Birmingham, having also been deployed in London's financial districts since the early 1990s, but its implementation in residential areas was a new development.

The initiative was introduced in the context of growing concern about the terrorist threat to the UK and, in particular, to Birmingham. Project Champion was conceived shortly after the failed London nightclub and Glasgow airport bombings of 2007 and two years after the 7/7 London bombings. The scheme was also implemented in response to several terrorist incidents in Birmingham, including the first UK-based al-Qaeda plot in 2000; the arrest of a suspected Taliban leader; and 'Operation Gamble', a plot to kidnap and dismember Muslim soldiers serving in the British Army.

7.2.2 Civil liberties implications

Few surveillance initiatives in the UK have been as controversial as Project Champion with respect to civil liberties.[87] The scheme's purpose was not made clear to the communities affected, and counter-terrorism objectives were downplayed.[88] While the Association of Chief Police Officers (Terrorism and Allied Matters), known as ACPO (TAM), approved £3m of Home Office counter-terrorism funding for the scheme in 2008, Assistant Chief Constable Hyde told local councillors at a briefing session in April 2009 that the cameras were intended to tackle crime and anti-social behaviour.[89] An evaluation found that the project's objectives had been misrepresented to the communities under surveillance, and another report found that 'the secrecy surrounding the purpose was inappropriate'.[90]

---

[82] Kelly (n.d.)

[83] Research interview with Steve Swain, former Head of the UK Police International Counter Terrorism Unit (PICTU), 07 May 15

[84] City of London Police (2013)

[85] West Midlands Police Authority (2012)

[86] Coaffee and Fussey (2015)

[87] Research interview with Alex Deane, former Director, Big Brother Watch, 18 May 15

[88] Research interview with a Senior Officer, anonymous UK police force, 09 June 15

[89] Awan (2011)

[90] Birmingham City Council (2010)

Privacy rights as enshrined in Article 8 of the European Convention on Human Rights 1953 (ECHR) were not adequately taken into account by Project Champion.[91] While court rulings indicate that the overt and legitimate use of security cameras in public spaces does not raise issues under Article 8, Project Champion included hidden cameras, which are necessarily more intrusive than overt CCTV and ANPR. One interviewee observed that Project Champion '*systematically intruded on individuals' privacy*',[92] and another highlighted the importance of protecting privacy rights in public spaces.[93]

Because Project Champion targeted two mainly Muslim areas, concerns were also raised over the discriminatory nature of the scheme. Geographical suspicion was clearly a key driver for Project Champion, and police sources said that the initiative was the first of its kind in the UK seeking to monitor a population seen as 'at risk' of extremism.[94] Project Champion is likely to have breached Article 14 of the UK Regulation of Investigatory Powers Act 2000 (RIPA) and Article 14 of ECHR, both of which prohibit unjustifiable discrimination. While Section 71 of the UK Race Relations Act 1976 requires public bodies to promote equality of opportunity, the West Midlands Police did not conduct a formal Equality Impact Assessment of the initiative.[95]

The initiative was also characterised by a lack of community engagement.[96] Public consultation was limited until the project became headline news in 2010.[97] Section 96 of the UK Police Act 1996 states that arrangements must be made by police to obtain the views of residents concerning policing of their local area, and the Public Space CCTV Strategy 2008 stipulates that 'all proposals for…public space CCTV schemes will be required to consult with the community and fully consider their views in any decisions made'.[98] However, there was no clearly defined consultation strategy for Project Champion and no acknowledgement of the need for proactive community engagement. While public engagement would be inappropriate in some cases due to security concerns, Project Champion's covert surveillance of a single community made consultation necessary.[99]

7.2.3 Counter-terrorism effectiveness

Project Champion was widely perceived to be unsuccessful in achieving its counter-terrorism objectives.[100] The cameras were never activated due to community resistance and were instead hooded and dismantled.[101] Fussey (2013) argues that it is likely that Project Champion would have generated large volumes of data that would have been difficult to manage and that might have concealed threat indicators.[102] The scheme also failed to address factors underpinning radicalisation, such as political grievances, fundamentalist ideology, and socio-economic issues, and instead merely created tensions between the West Midlands Police and the community.[103] One human rights interviewee described the initiative as '*a total failure*' and '*a model of how not to police,*' as it only served to create community resentment towards the West Midlands Police.[104]

---

[91] Fussey (2013)

[92] Research interview with Alex Deane, former Director, Big Brother Watch, 18 May 15

[93] Research interview with an anonymous professor, anonymous US university, 22 June 15

[94] The Guardian (2010)

[95] Birmingham City Council (2010); Research interview with a Senior Officer, anonymous UK police force, 09 June 15

[96] Research interview with Tony Porter, Surveillance Camera Commissioner, UK Home Office, 13 July 15

[97] Thornton (2010); Research interview with a Senior Officer, anonymous UK police force, 09 June 15; Research interview with Alex Deane, former Director, Big Brother Watch, 18 May 15

[98] Birmingham City Council (2010); Birmingham Community Safety Partnership (2008)

[99] Thornton (2010)

[100] Research interview with Tony Porter, Surveillance Camera Commissioner, UK Home Office, 13 July 15; Research interview with a Senior Officer, anonymous UK police force, 09 June 15; Research interview with Alex Deane, former Director, Big Brother Watch, 18 May 15; Thornton (2010)

[101] Afzal et al. (2012); Coaffee and Fussey (2015)

[102] Fussey (2013); Research interview with an anonymous professor, anonymous US university, 22 June 15

[103] Awan (2011)

[104] Research interview with Alex Deane, former Director, Big Brother Watch, 18 May 15

Broader questions have been raised over the effectiveness of CCTV technologies in preventing terrorism.[105] The mixed evidence base is reflected in ongoing debate. On the one hand, the Public Space CCTV Strategy 2008 claims that 'Public Space CCTV systems…have proved exceptionally useful in [an anti-terrorist] role'.[106] However, a Home Office study found that 'the CCTV schemes that have been assessed had little overall effect on crime levels.... In summary, CCTV produced few cost-benefits', while another study indicates that 'CCTV has a modest but significant desirable effect on crime.... CCTV should continue to be used to prevent crime in public space, but that it be more narrowly targeted than its present use would indicate.'[107]

7.2.4 Implementation challenges

The business case for Project Champion anticipated only four implementation challenges associated with the scheme: insufficient funding, insufficient planning consent, disclosure of the locations of the cameras, and cooperation of suppliers of the scheme.[108] However, the most significant stumbling block turned out to be community opposition. Public objections raised over the discriminatory, intrusive and disproportionate nature of the scheme ultimately led to the abandonment of Project Champion.[109]

The divergent aims and remits of the agencies involved in implementing Project Champion constituted another key challenge. For example, the West Midlands Police's aim to 'police from afar' contrasted with the community engagement remit of Birmingham's municipal crime reduction body, the Safer Birmingham Partnership.[110] A West Midlands Police interviewee noted that the force held a very different perspective from that of Birmingham City Council and that there was '*a major disconnect*' between the stakeholders involved.[111]

According to one interviewee, Project Champion faced problems because funding was allocated before the identification of a capability gap and definition of an overall purpose. The £3m of Home Office funding had been allocated to Project Champion as the financial year was approaching its end. The Thames Valley Police interviewee noted that the business case for the initiative was '*weak*' and that the Home Office '*simply sought to use the excess resource*' rather than identifying the problem at hand, tailoring an appropriate solution, and allocating funding accordingly.[112]

7.3 Case study 3: Police surveillance drones

7.3.1 Context

There has been a significant increase in the use of Unmanned Aerial Vehicles (UAVs), colloquially known as drones, as their cost has declined and availability has increased. Despite their title, the vast majority are not truly 'unmanned', but require a human operator. As well as the large numbers being produced commercially for private use and the top-end developments, such as the Predator and Reaper systems being used by military and intelligence agencies, they also provide unique capabilities to police and security forces at a limited cost. In particular they allow police incident commanders to monitor a developing situation remotely and from an aerial view, and they afford the opportunity for remote surveillance and photography of crime or accident scenes and search and rescue capabilities.

Consequently, as drones are becoming cheaper, more and more police departments in the United States and in European and other countries are investing in drones for law enforcement roles. As an academic specialist explained, *'drones are being rolled out in a lot of different countries. The most advanced use of drones are in Israel, and they have been involved in their development for a long time – for obvious reasons like counter-terrorism measures. Today you find drone uses in Russia, China and Gulf States, who are all*

[105] Gill and Spriggs (2005) in Awan (2011)

[106] Birmingham City Council (2008) in Birmingham City Council (2010)

[107] Campbell Collaboration (2008) in Birmingham City Council (2010)

[108] Isakjee (2011)

[109] Isakjee (2011); Research interview with Marcus Beale, Assistant Chief Constable, West Midlands Police, 02 July 15

[110] Coaffee and Fussey (2015)

[111] Research interview with Marcus Beale, Assistant Chief Constable, West Midlands Police, 02 July 15

[112] Research interview with Marcus Beale, Assistant Chief Constable, West Midlands Police, 02 July 15

heavy buyers of drone technology in security applications. Europe is the hold-out, largely because of civil society and privacy issues.'[113]

However, their increased use by police and security organisations has raised concerns among both law-makers and human rights groups concerning their impact on privacy through the potential of intrusive (as opposed to general) surveillance. A further concern in the US is that while the Federal Aviation Authority (FAA) is focused on safety considerations, it does not appear to be considering aspects of privacy, which is being left to the individual US state legislation. These concerns are at their earlier stages because the technology is relatively new and there has not yet been a full roll-out of drone technology in many countries; however, it is likely that such privacy-related concerns will grow as their usage increases.

A further concern is that most countries' regulators have been slow to define and clarify circumstances in which drones can fly in commercial airspace. Fears have been raised of the potential for crashes with passenger jets, particularly over densely populated areas. Consequently, in the UK, there are growing fears that drones pose a threat to passenger aircraft and helicopters when flown without due care, in particular in the vicinity of airports. The United Kingdom Airport Board (UKAB), which examines all 'near misses', warned that the easy availability of drones along with the lack of adherence to regulations 'was highly likely to result in future situations where airspace users would be put in danger by the unthinking or unknowing actions of those who were not concerned with, or were ignorant of, the proper operation of airborne vehicles'.[114] The UK Civil Aviation Authority (CAA) rules require the person flying a drone to have direct, unaided visual contact at all times and state that drones must not be flown in the vicinity of airfields or over congested areas and crowds. Where CAA permission has been granted for aerial work, such as photography, the drone must go no higher than 400 ft and at a distance not beyond the visual range of the operator, or a maximum distance of 1,640 ft.

A recent article has highlighted a number of incidents. In the first a helicopter was coming in to land at Norwich Airport and had to adjust its landing path to avoid a privately owned drone. In the second a para-glider was put at great risk by a drone that appeared to be filming him, with a risk of collapsing his canopy. In the third, a drone came within 10 ft of hitting a two-person gyroplane in Kent, which could have led to catastrophic failure of the aircraft. In perhaps the most serious incident, in December 2014, the pilot of an Airbus 320 passenger jet, making its final approach to landing at Heathrow airport, reported seeing a drone flying towards the passenger jet.[115]

7.3.2 Civil liberties implications

As previously detailed, the main civil liberties implication of the use of drones by police and security organisations is the potential impact on personal privacy. Consequently, in the US, numerous states are proposing various restrictions on the use of drones amid concerns that they could be used to conduct inappropriate and illegal surveillance on the American public. This concern has been exacerbated by the increasing affordability of drones and ease of access.

In the State of Virginia law-makers approved a two-year moratorium on the use of drones by police and government agencies (which was set to expire in July 2015). This moratorium was supported by such diverse groups as the American Civil Liberties Union (ACLU) and the Tea Party Federation, but was opposed by police and government agencies. However, in an attempt to address police concerns, legislators in Virginia made exceptions for the use of drones in certain emergencies: Amber Alerts, when a child goes missing; Senior Alerts, when an old age person goes missing; and Blue Alerts, when a police officer is killed or seriously injured. In Montana, both Democrats and Republicans have backed various proposals to restrict the use of drones, due to their perceived impact on civil liberties. In 2013, the Montana Senate endorsed a measure banning information collected by drones from being used in court. Meanwhile, a Missouri House Committee looked at a bill that would outlaw the use of unmanned drones to conduct surveillance on individuals or property, but that provides an exception for police working with a search warrant. The level of public concern was highlighted in 2012, when the Alameda County Sheriff's Office, in California, faced a backlash after announcing plans to use drones to help find fugitives and assist with search and rescue operations.[116]

---

[113] Interview with Kimo Quaintance, Lecturer, George C. Marshall European Security Studies, Germany, 30 June 2015

[114] Quoted in Gillespie, J. (2015) '*Paraglider's Life Put at Risk by Mini Drone.' The Sunday Times* 19 April 2015.

[115] Based on details contained in Gillespie (2015) op. cit.

[116] Details taken from *'States Step Up Fight against Use of Surveillance Drones by Law Enforcement'* 06 February 2013

At the time of writing (February 2015) only 14 US states have introduced the requirement to obtain a warrant for the use of drones for surveillance. While the FAA enacts legislation in relation to safety at the federal level, unless a law enforcement organisation is within one of the 14 states that have passed privacy legislation, there is little to stop the local police from using drones for surveillance without a warrant.[117]

By comparison, *'Germany doesn't have much use of surveillance drones; there is strong civil society resistance to use of drones by government in military and police applications… There is a civil society backlash in Germany against drone use… In Germany, privacy laws are different. They are more orientated around the principle of individual dignity, meaning there is no need to prove any harm done in collecting the data. If you're a photographer in the US, you can take pictures of the people without their permission. In contrast, you cannot take a picture of a crowd without their permission in Germany. And the logic applies to drones: you cannot fly a drone in public, which would collect information without prior consent of the people that are being surveilled. Drones do not fit with the private laws'.*[118]

The UK perspective on the civil liberties implications of police drone use were provided by the UK Surveillance Camera Commissioner, who stated, *'after all, a police drone is an arm of the state, flying over its citizens, recording, where there is an opportunity for privacy impact. It must be subject to tight rules. The code of practice seeks to minimise any such collateral intrusion. If the police drone surveils an open area, there is minimal intrusion. But if it is in a more intimate area, you can imagine citizens would feel intruded. The police must be clear about how they intend to minimise this intrusion by communicating with the public, and installing systems that pixel out irrelevant figures in the background and eradicate extraneous materials. It has to be a combination of winning the trust of the public and developing suitable technologies to aid the privacy impact'.*[119]

A subject matter expert concluded that *'the privacy concerns come up more when the drones employ an autonomous capacity, that extends beyond what the human operator can do (e.g. mass surveillance over a wide area; long-term collection of data). These new questions arise and they are part of a broader set of questions about how law enforcement is conducted. At the crux of the privacy discussion is whether you want to have police agencies that are purely focused on enforcing the law – which is the traditional role – or use law enforcement to prevent crimes – which is what the US started doing at a large scale after 9/11 with the counter-terrorism aims. Crime response and crime prevention are very different; the prevention model requires highly varied measures with data analysis, because you must identify crimes before they happen'.*[120]

7.3.3 Counter-terrorism effectiveness

While at this point the full potential of the police use of drones in various roles has not been realised, it is clear that they provide a great potential in a counter-terrorist role. In more of an overseas insurgency type of environment, as well as their much publicised use in targeting insurgents in 'drone strikes', drones have proved invaluable in conducting surveillance, both in a pro-active role, identifying locations and targets and in a defensive role, providing an aerial view of road convoys and foot patrols and, in particular, of the potential setting up by insurgents of improvised explosive devices (IEDs) and ambush sites.[121]

In a more domestic counter-terrorist role, drones can provide discreet remote aerial surveillance of suspects and vehicles during a pro-active operation. They also allow an incident commander to remotely view an incident scene or location from a unique vantage point, providing real-time intelligence. In a siege or hostage rescue situation, as well as the incident overview and surveillance for incident commanders previously described, the development of smaller, more covert, drones allows tactical teams to gain real-time intelligence on building lay-outs, terrorist numbers, movements, weaponry and behaviour, being able to operate in locations that a human operator would be unable to gain access to.[122]

A further factor to consider in relation to the effectiveness of drones in counter-terrorism is the reduction of costs. *'In the US, you will find cases now where police departments are comparing the use of drones versus the use of helicopter – this draws interesting parallels, where benefits of moving to a drone platform will be discussed. There is considerable talk about the cost that is involved with human operators and maintenance*

[117] Waddell (2015)

[118] Interview with Kimo Quaintance, Lecturer, George C. Marshall European Security Studies, Germany, 30 June 2015

[119] Interview with Tony Porter, UK Surveillance Camera Commissioner, Home Office, 13 July 2015

[120] Interview with Kimo Quaintance, Lecturer, George C. Marshall European Security Studies, Germany, 30 June 2015

[121] See Byman-and Cronin (2013)

[122] See Marchington (2003)

– helicopters, of course, are very expensive platforms over time. You can replace those capabilities with an inexpensive drone, which is why you are seeing the shift'.[123]

7.3.4 Implementation challenges

In relation to the implementation of drones, an academic specialist explained that *'in the US drones for policing started more in search and rescue application, as an extension of helicopters for finding people in fire disasters. Drones have been adopted by various departments as easier ways of covering land, reaching dangerous locations. Other uses include border patrol – there is a growing use of the observation of Canadian or Mexican borders using drones. It started out very much from the perspective of sending something to look at the field; now they are being more professionalised and there is a trend towards complication of machine vision. This is what you see in Washington DC area, where they use drones in multiple occasions with sophisticated cameras that can track objects in real time. It is used for larger scale data collection and correlation. That seems to be the overall direction that drones are headed – more sophisticated centres, more sophisticated data collection, greater volume and incorporating them into smart city settings where you are integrating different types and sources of data into a common intelligence platform'.*[124]

While much focus has been on US State legislation introduced in an attempt to protect privacy from intrusive drone surveillance, in the majority of cases the laws are more focussed on the technology of the drones themselves, rather than the potential pervasive surveillance they might cause. 'In many cases, this technology-centric approach creates perverse results, allowing the use of extremely sophisticated pervasive surveillance technologies from manned aircraft, while disallowing benign uses of drones for mundane tasks like accident and crime scene documentation, or monitoring of industrial pollution and other environmental harms'.[125] Consequently, because drones are cheaper and have captured the public's imagination, much of the focus from privacy advocate groups has focussed on these. However, this has left identical and more advanced surveillance capabilities in manned aircraft and helicopters. This approach has therefore failed to focus on more sensible legislation that addresses potential harm regardless of the type of technology used.[126]

A few examples from the US also highlight the confusion, lack of clarity and 'patchwork' nature of laws and regulations concerning the introduction and use of drones by the police. In the case of the Mesa Country Sheriff's Office, in Colorado, while there is no state legislation at all regarding the use of drones, the Sheriff's office have introduced their own policy and deployment guidelines on both the use of drones and on data retention. Consequently, their drone is mainly used for search and rescue and crime scene photography, and if it is required for use in an area where someone would usually have a legitimate expectation of privacy, a warrant would be obtained. A different example is provided by the San Jose Police Department, California, which secretly bought a drone in 2014 and faced an uproar when freedom of intervention requests identified its purchase publicly, six months later. The department stated that the drone was to help bomb technicians assess hard-to-reach locations, but they also stated it could be used for active shooters and hostage-taking or other tactical situations where lives might be in immediate danger.[127] It is relevant to note that while these issues are based on the US context, where many laws are state-specific, the risk posed by unharmonised laws, rules and guidelines is real even in the EU context, both at the inter-state level (e.g. for technology deployed in proximity of borders) and the intra-state level (e.g. for technology that may fall under the jurisdiction or responsibility of different governmental bodies and agencies).The concern is that with strong emotive arguments over privacy, a lack of clarity over the precise implementation and specific role of drones, and a patchwork of different rules and regulations, legislation is being introduced which might significantly limit the operational effectiveness of police drones. This is of particular concern when their non-contentious use by police or security organisations might save 'life and limb', for example by providing surveillance during an armed siege, tracking armed criminals or terrorists, helping in cases of missing or abducted children, monitoring a major accident or supporting search and rescue efforts. This was summed up by Tony Porter, the UK Surveillance Camera Commissioner, in an interview, when he stated that *'the issues in relation to drones are again to do with privacy. These have to be balanced against the number of opportunities law enforcement faces, where the value is one of saving a life. This can happen through an*

[123] Interview with Kimo Quaintance, Lecturer, George C. Marshall European Security Studies, Germany, 30 June 2015

[124] Interview with Kimo Quaintance, Lecturer, George C. Marshall European Security Studies, Germany, 30 June 2015

[125] McNeal, G. (2014) p. 2

[126] Ibid.

[127] Details from Waddell (2015) op. cit.

accurately sourced deployment of search and rescue instruments – only possible through aerial assistance'.[128]

7.4 Body scanners

7.4.1 Context

Traditional aviation security measures were largely reactive until the 9/11 attacks in 2001.[129] The severity of their impact generated sweeping support for more proactive measures in counter-terrorism: the focus shifted from responding to attacks, to preventing them. One such measure was advanced imaging technology (AIT), more colloquially known as full-body imaging. According to the Transportation Security Administration (TSA) of the United States, AIT provides 'the best opportunity to detect metallic and non-metallic anomalies concealed under clothing without the need to touch the passenger.'[130] Various governments have since deployed full-body scanners as the primary method of inspection at airports, starting with the Netherlands and the United States in 2007. The United Kingdom deployed them in 2009.[131]

Subsequent incidents seemed to confirm the need for this arguably intrusive technology. The post-9/11 world saw increases in terrorist attacks (or attempts) where capability gaps were manifest. The list is extensive, including the shoe-bombing incident in 2001, the crash of two Russian airliners in 2004, and the transatlantic aircraft plot in 2006.[132] In particular, the attempted bombing on Christmas Day of 2009 triggered a widespread response.[133] Umar Farouk Abdullmutallab, an al-Qaeda operative from Nigeria, had boarded the Delta-Northwest flight from Amsterdam to Detroit to detonate the plastic explosives sewn onto his underwear. Although the attempt was foiled, the incident heightened the concern that existing security procedures were unable to reliably detect explosives and bomb-making apparatuses. Increasingly adaptive adversaries with intelligent concealment methods required an equally sophisticated scanning technology.[134] Investment in AIT thus accelerated at an exponential rate.

Currently, full-body scanners rely mainly on two technologies: X-ray backscatter and active millimetre wave. X-ray backscatter scanner uses a low-intensity X-ray beam to penetrate visual concealment, flagging up any anomalies.[135] Millimetre wave, on the other hand, uses radio frequency waves to trace contraband. The key difference is that the latter does not expose the passenger to ionised radiation, which has been associated with various health risks.[136] Slight differences in procedure exist as well. Whereas X-ray backscatter scanner requires a security officer to examine each scanned image before deciding to further inspect or discharge the passenger, the millimetre wave scanner utilises automatic threat recognition software: it detects a threat without relying on an officer's discretion, and positions a yellow square around the suspect area of a cartooned body shape. An 'OK' is signalled where no threat is detected.[137]

7.4.2 Civil liberties implications

X-ray backscatter scanners have been subject to steady criticisms. As previously noted, there are potential health issues. While the scanner meets the requirements of the National Institute of Standards and Technology, various experts have objected to their approval, stating that the dose of radiation is dangerously high.[138] Besides, any glitch in hardware could expose a passenger to intense radiation on a single spot.[139]

---

[128] Interview with Tony Porter, UK Surveillance Camera Commissioner, Home Office, 13 July 2015

[129] Mitchener-Nissen et al. (2012)

[130] Mowery et al. (2014); see also Mitchener-Nissen et al. (2012): '[with AIT,] the TSA expects to be able to quickly, and without physical contact, screen passengers during primary and secondary inspection for prohibited items including weapons, explosives, and other metallic and non-metallic threat objects hidden under layers of clothing.'

[131] Mironenko (2011)

[132] Elias (2012)

[133] Elias (2012); Mironenko (2011)

[134] Mowery et al. (2014)

[135] Groeger (2011)

[136] The Associated Press (2012)

[137] Groeger (2011)

[138] Elias (2012)

Ionized radiation is associated with different forms of cancer, in particular, breast cancer, sperm mutagenesis and skin-related diseases.[140] Presently, no independent study affirms the safety of X-ray body scanners.

Another contentious issue is privacy. Civil rights organisations, such as the American Civil Liberties Union (ACLU), have often argued that full-body screening amounts to 'virtual strip searches' that have particularly damaging implications for women, minors and religious groups.[141] Further, privacy concerns are heightened where passengers have special needs, including medical conditions, gender issues and physical disabilities.[142] A number of technical measures have been adopted to address these concerns. The TSA, for instance, employs privacy filters such as facial blurs and issues disability notification cards that allow eligible passengers to bypass the screening.[143] Due to both health and privacy concerns, X-ray backscatter scanners are being increasingly replaced by millimetre-wave scanners.

Other measures are reflected in the ongoing attempts to shape the legal requirements surrounding the use of body scanners. In November 2011, the European Commission adopted an EU legal framework on security scanners, which prohibits any scanner that uses ionising radiation.[144] To safeguard passengers' civil rights, the framework also obliges security agencies to offer alternative pat-down searches and outlines stringent provisions for data protection. These provisions ensure that images cannot be stored, retained, copied, printed or retrieved. In comparison, the US has been much less proactive in adopting new measures. Attempts at supplementing qualifications to the use of body scanners came about only recently, including the Aircraft Passenger Whole-Body Imaging Limitations Act of 2011, which was eventually stymied, and the Checkpoint Images Protection Act of 2011, which addresses data retention of screened images and remains under consideration.[145]

7.4.3 Counter-terrorism effectiveness

Whether the scanners are in fact effective in countering terrorism is disputed. Conventionally, the effectiveness of screening technology is measured by balancing the record of accurately detected threats against the rate of false alarms.[146] The statistics have fluctuated considerably: in Germany, the false positive rate of millimetre-wave scanners was 54%; in Italy, it was estimated at 23%. In the UK, the false positive rate of X-ray scanners was marked at 5%.[147]

One widely cited study on the Rapiscan Secure 1000 scanner reveals that 'while the [X-ray backscatter] scanner performs adequately in a non-adversarial setting, and ensures a fair degree of protection against possible malfunctions or other safety hazards, it performs significantly less well against adaptive adversaries [with sophisticated concealment and cyber tactics].'[148] Notable concealment tactics include positioning, masking, and shaping; these methods enabled the researchers to successfully conceal contrabands, such as a folding knife and 200 grams of plastic explosives.[149] Besides, the scanner is susceptible to software compromise. The attacker could infect the scanner with malware and selectively replace the scanned image.[150] Beyond questioning their effectiveness, the findings demonstrate how poorly scanners were tested prior to being deployed.[151]

7.4.4 Implementation challenges

---

[139] Sedat et al. (2010)

[140] Sedat et al. (2010)

[141] The Associated Press (2012)

[142] Research interview with anonymous university academic, 12 June 15

[143] Elias (2012)

[144] European Parliament (2011) Commission Regulation (EU) No 1141/2011

[145] Elias (2012)

[146] Elias (2012)

[147] Grabell and Salewiski (2011)

[148] Mowery et al. (2014)

[149] Mowery et al. (2014)

[150] Mowery et al. (2014); Greenberg (2014)

[151] Greenberg (2014)

Despite the controversies, public perception of the full-body scanners has been mostly positive. According to a CBS News poll, more than 80% of Americans approve of the use of full-body scanners for aviation security purposes.[152] Another study, in the UK, showed that respondents 'overwhelmingly preferred the use of body scanners in UK airports [as opposed to pat-down searches].'[153] Community reception, at least for the moment, appears not to be a significant challenge (though this is easily subject to change).

Instead, the challenges deal with the technical limitations and procedural inconsistencies surrounding the use of AIT systems. To begin with, the scanners are technically vulnerable to intelligent tricks by adversaries. Without an advanced filtering system, scanning unwilling passengers can lead to severe breaches of privacy and civil rights. Further, the US Department of Homeland Security (DHS) Office of Inspector General notes the inconsistent use of calibration procedures used by operators to retain certain imaging quality (potentially at the expense of increased radiation to passengers).[154]

Whether security officers are sufficiently trained to operate the machines in an 'ethically sensitive manner' remains questionable.[155] In fact, an investigation in 2010 revealed that US marshals operating AITs in a federal courthouse in Florida had illegally retained 35,000 scanned images of private citizens.[156] Despite the TSA's claim that the images are 'automatically deleted from the system after it is cleared by the remotely located security officer', the scanners had retained the images.[157] This incident highlights that regardless of the stated policy, operators can either inappropriately or accidentally misuse the AITs. And yet, accountability mechanisms required to thwart such attempts and mistakes are often too immature or hidden behind the veils.

7.5 Passenger Name Record

7.5.1 Context

Passenger Name Record (PNR) systems involve the exchange of flight passenger data in order to identify potential terrorists and criminals.[158] PNR data is provided by passengers and collected by air carriers, and includes such information as names, travel dates, itineraries, seats, baggage, contact details and means of payment. By detecting behavioural patterns, PNR systems seek to profile risk and target suspects more effectively. The purpose of PNR is not only to combat terrorism, but also to prevent organised crime and illegal migration.[159]

European PNR initiatives have been developed in the context of the growing terrorist threat to the West. Following the Paris and Copenhagen attacks of early 2015, EU policy-makers have dedicated significant time and resources to counter-terrorism and the need to address the foreign fighter threat.[160] Historically, EU counter-terrorism action has followed major crises, including 9/11, the 2004 Madrid attacks and the 2005 London bombings.[161] As the terrorist threat has become more international, European governments have increasingly relied on cross-border security measures, such as PNR.[162]

The use of PNR varies across EU member states, from countries with functioning systems to those where there are no plans to introduce PNR in the foreseeable future. By 2011, only the UK had a fully developed PNR system in place, having set up its Project Semaphore in 2004. In 2013, a total of €50m was made available by the European Commission to 14 member states for the development of national PNR schemes.

---

[152] Lowrey (2010)

[153] Mitchener-Nissen et al. (2012)

[154] Elias (2012); Sedat et al. (2010)

[155] Research interview with anonymous university academic, 12 June 15

[156] Johnson (2010)

[157] Johnson (2010)

[158] Boehm (2011); *The New York Times* (2015)

[159] Boehm (2011); US Department of Homeland Security (2011)

[160] Research interview with an Analyst, anonymous US research institute, 01 June 15

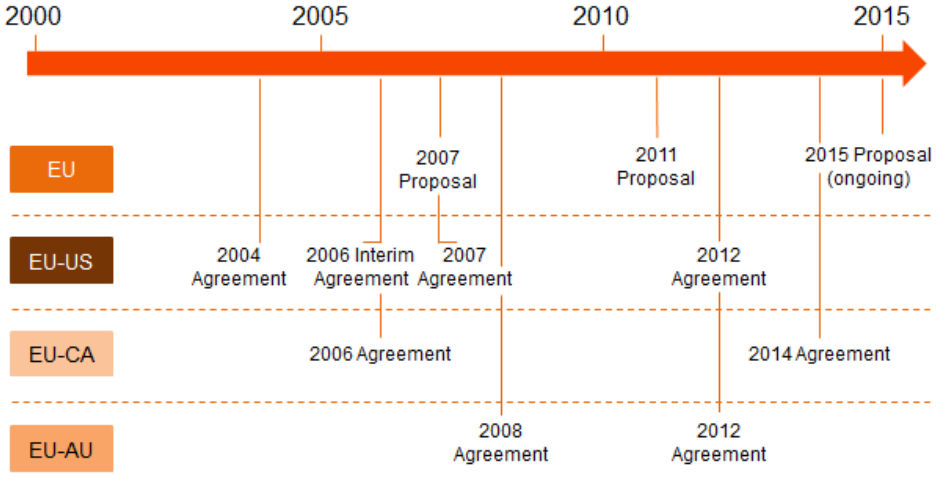
[161] European Parliamentary Research Service (2015); Archick (2014); European Parliament (2015)

[162] Archick (2014)

France introduced its national PNR system in January 2015, and Spain has announced plans to set up a Passenger Information Unit (PIU) in January 2016.[163]

Following calls from member states, the European Commission is developing a proposal to adopt an EU-wide PNR system. Under this proposal, 42 items of personal information relating to air passengers flying in and out of Europe would be collected and stored.[164] This is not the first time the EU has developed such a proposal; plans to institute an EU-wide PNR scheme have been debated since 2007, and the most recent proposal was rejected by the Committee on Civil Liberties, Justice and Home Affairs **(**LIBE)[165] in 2013 due to data protection concerns.[166] Figure A2.1 provides an overview of the EU PNR policy landscape.

Figure A2.1 overview of the EU PNR policy landscape



As figure A2.1 shows, the EU has negotiated bilateral PNR agreements with the US, Canada and Australia. While countries including Mexico and Argentina have requested similar arrangements, the EU has not yet confirmed bilateral agreements with these countries.[167] Figure A3.1 also illustrates that there have been multiple phases of negotiation between the EU and each of its overseas partners. The rejection or modification of international PNR agreements has often been prompted by civil liberties concerns regarding inadequate data protection, disproportionate retention periods and incompatibility with existing legislation, among other concerns that will be explored in the next section.

7.5.2 Civil liberties implications

The 2015 EU PNR proposal has sparked numerous civil liberties concerns. According to its critics, the proposal does not adequately protect the right to privacy that is established in the EU Charter of Fundamental Rights. Questions have also been raised over whether the mass processing of individuals' data meets the data protection requirements laid down in the 2009 Lisbon Treaty and the European Court of Human Rights case law.[168] Further criticisms have been made regarding the lengthy proposed period for data retention, the incomplete nature of data anonymisation, and the transfer of data to third countries without adequate legal safeguards.[169]

Another contentious issue raised by the 2015 proposal relates to passengers' right to freedom of movement. According to the EU Free Movement Directive, member states may restrict the freedom of movement of EU citizens on the grounds of public security. However, such restrictions must also comply with the principle of proportionality. The Article 29 Data Protection Working Party argues that measures affecting the rights of

[163] European Parliamentary Research Service (2015)

[164] See *The Guardian* (2015) for a full list of the items of passengers' personal information.

[165] LIBE Committee: Committee on Civil Liberties, Justice and Home Affairs

[166] European Parliament (2015); Archick (2014)

[167] European Parliamentary Research Service (2015)

[168] Boehm in Gutwirth et al. (2011)

[169] Statewatch (2011); Research interview with Diego Naranjo, Advocacy Manager, European Digital Rights, 30 June 15

travellers are only proportionate when introduced temporarily and in response to a specific threat – which is not the case for the 2015 proposal. Similarly, Statewatch finds that the proposal conflicts with citizens' right to freedom of movement.[170]

Civil liberties objections have mainly been raised by human rights organisations and the European Parliament, but member states have been strong advocates for a European PNR system. The former German Federal Minister of Interior, Wolfgang Schäuble, argued that failure to adopt a PNR system for Europe would be 'inexcusable',[171] and a European Commission-sponsored questionnaire sent to member states found that the majority of members support the initiative. Moreover, one interviewee noted that the transfer of PNR data to security services goes largely unnoticed by the public.[172]

Some EU PNR agreements have been more controversial than others. The EU–Canada agreements have been the least contested cross-border PNR instruments, while EU–US agreements have sparked a greater degree of criticism. The EU–Canada agreements are seen as a 'model' among PNR instruments in relation to purpose limitation, data proportionality and restrictions on the onward transfer of data. Moreover, they are seen as being legally compliant with accepted international standards of privacy protection, such as the Organisation for Economic Co-operation and Development (OECD)[173] guidelines and Article 8 of the European Convention on Human Rights. By contrast, data protection authorities have raised concerns about the US's ability to provide adequate protection of EU citizens' personal data.[174]

7.5.3 Counter-terrorism effectiveness

Many EU and US leaders believe that PNR is a vital tool in the fight against terrorism.[175] While the European Commission has not made detailed statistics publicly available, it claims that the PNR data has led to 'critical progress' in countering terrorism.[176] According to the US Department of Homeland Security, its analysis of PNR data has helped identify 1,750 suspicious cases on average each year and has been essential in many of the US's most well-known terrorism investigations since 9/11.[177]

The retention of PNR data can allow authorities to tackle more complex plots by looking at travel practices over time. Data that do not appear to be relevant at the time of travel can be critically important when linked to a specific case at a later stage. For example, retained travel data assisted the US Department of Justice in securing convictions in several recent counter-terrorism cases. PNR data have aided the high-profile terrorist investigations of David Headley, who pled guilty for his role in the 2008 Mumbai terrorist attacks, and of Najibullah Zazi, who pled guilty to plotting to bomb New York City subways.

However, the evidence base on the counter-terrorism effectiveness of PNR is extremely thin.[178] According to the European Parliamentary Research Service, 'there seems to be no agreement as to whether PNR systems – and mass surveillance tools in general – are efficient'.[179] For example, little evidence of PNR's effectiveness was presented at a hearing on 'the positive value of PNR' held by the EU Committee of the UK House of Lords. While Jonathan Faull of the European Commission alluded to several 'successful' PNR counter-terrorism cases, he was unable to describe them in detail due to the classified status of the cases.[180]

---

[170] European Parliamentary Research Service (2015)

[171] Tomik (2007) in Newman (2011)

[172] Research interview with Diego Naranjo, Advocacy Manager, European Digital Rights, 30 June 15

[173] OECD: Organisation for Economic Co-operation and Development

[174] Hobbing (2008)

[175] Archick (2014); US Department of Homeland Security (2011); Research interview with a Senior Officer, anonymous UK police force, 24 June 15

[176] European Parliamentary Research Service (2015)

[177] US Department of Homeland Security (2011)

[178] Research interview with Abraham Newman, Associate Professor, Georgetown University, 09 June 15; Research interview with an anonymous Member of the European Parliament, 09 July 15; Research interview with Diego Naranjo, Advocacy Manager, European Digital Rights, 30 June 15

[179] European Parliamentary Research Service (2015)

[180] Hobbing (2008)

While government rhetoric often focuses on the urgent need to collect PNR data for national security, it is difficult to assess PNR's actual effectiveness due to the inherent secrecy of the counter-terrorism field.[181]

7.5.4 Implementation challenges

With 14 EU member states setting up their own PNR systems, the integration of different and potentially incompatible systems is likely to be a challenge.[182] Timothy Kirkhope, Conservative member of the European Parliament's Civil Liberties Committee, warned that this approach could lead to 'a patchwork of PNR systems with holes in the net, which criminals will exploit, and lower standards of data protection'.[183] As views on data privacy and intelligence-sharing tend to vary by country, this is also likely to create problems for the harmonisation of national laws and for attempts to establish EU-wide PNR policies. Furthermore, EU member states retain national control over their law enforcement and judicial authorities, and some national police and intelligence services remain reluctant to share information with each other or with Europol.[184]

Collaboration between the EU and its overseas partners can also create challenges. For example, while the US has tended to call for greater security, the EU has often favoured a more measured response that prioritises law enforcement and human rights protection.[185] In the negotiation of several EU–US agreements, EU officials have voiced concerns about US willingness to guarantee a sufficient level of protection for European citizens' personal data.[186] EU concerns have been increased by the Snowden leaks of June 2013 and allegations of US collection activities in Europe.[187] US officials have often been frustrated by the need for time-consuming negotiations with the EU on each individual agreement involving EU–US data sharing, particularly given the time-sensitive nature of the counter-terrorism field.[188] It can therefore be difficult to create interoperable solutions when partners have different priorities and legal regimes.

7.6 E-Borders

7.6.1 Context

The long-term aim of e-Borders was to create a technologically integrated secure border for the 21st century. This came about in response to a growing recognition of the need to facilitate travel while maintaining secure borders – that mass migration and tourism had created an exponential growth in world travel, but that at the same time the United Kingdom's (UK) international position meant it was open to a range of serious threats. Consequently, e-Borders was planned to achieve three main goals. First, it was intended to enhance the security of the UK, by identifying individuals presenting a security risk. Second, it was intended that e-Borders would support a more efficient management of the core resources utilised on UK border control. Third, it was planned to enhance the operational effectiveness of UK border control operations. As well as being a technology solution, e-Border system was intended to benefit integration and cooperation between the Border and Immigration Agency (BIA – later UK Border Agency and now UK Visas and Immigration), Her Majesty's Revenue and Customs and the police, improving the level and effectiveness of UK border management.

Work commenced on the e-Borders programme, originally commissioned in 2003 through the Home Office, with the intention of developing a modern and efficient means of delivering effective immigration control. This was to be achieved through the collection of advanced passenger information (API) and Passenger Name Records (PNR) for all inbound passengers in advance of their travel. As a specialist senior police officer explained, *'the difference between the two sets of data is that API provides an individual identifier; PNR provides a much richer dataset (e.g. credit card, phone number, travel destination etc.). Both were*

[181] Research interview with an Analyst, anonymous US research institute, 01 June 15

[182] The Guardian (2015); Research interview with an anonymous Member of the European Parliament, 09 July 15

[183] The New York Times (2015)

[184] Archick (2014); Research interview with an anonymous Member of the European Parliament, 09 July 15

[185] Monar (2007); Stevenson (2003) in Newman (2011)

[186] Research interview with Abraham Newman, Associate Professor, Georgetown University, 09 June 15

[187] Research interview with an Analyst, anonymous US research institute, 01 June 15

[188] Archick (2014)

considered, but the collection of API was always much easier'.[189] The concept was that this data would effectively allow the authorities to 'export the border' electronically 'across the globe', preventing passengers from travelling (either inbound or outbound) when they were considered a threat to UK security, while also delivering a more efficient type of immigration control. In addition, it was hoped this would better target resources, while also increasing clearance times through immigration control.

In 2004 a pilot was launched to deliver Project Semaphore, a 39-month project costing around £52m,[190] which aimed to test the e-Borders concept in advance of the full procurement and introduction of the main e-Borders solution. Project Semaphore was considered a successful pilot and resulted in the Home Office Group Investment Board releasing the funds to deliver the full e-Borders programme in 2006. In June 2007, a full version of the e-Borders business case was produced, which described a number of anticipated benefits coming from the introduction of the system and the gradual build-up of the amount of API collected until e-Borders reached its full operating capability. The e-Borders programme was intended to be fully functioning by March 2014, and it was anticipated that by this point API and PNR would be collected from all passengers travelling on scheduled transport of all types into and out of the UK.

7.6.2 Civil liberties implications

The primary civil liberties implication associated with the e-Borders programme was the issue of data protection of API and PNR data. In particular, EU data protection legislation has impacted negatively on the effectiveness of the e-Borders programme and wider concept. As a specialist explained, *'there have always been challenges. The greatest challenge in Europe was around the PNR directive, which was used as a political tool by individual parties. The UK and other states showed how we protected the data gathered. Having a directive that would allow having a common platform for data sharing has been obstructed for more than 10 years by single issues serving political games. Europe has been made vulnerable by the actions of these individuals. Our national legislation for data protection and data sharing meant that we were able to conclude bilateral agreements'.*[191]

The primary UK legislation permitting the introduction of e-Borders was enacted in 2006, providing a framework for the powers to be used (Schedule 2 of the Immigration Act 1971, amended in 2006, and Sections 32 to 38 of the Immigration, Asylum and Nationality Act 2006). In particular, these allowed the UK Border Agency and police to obtain API and PNR from carriers prior to their movements into or out of UK airspace and territory. In July 2012, the Security and Travel Bans Authority to Carry (ATC) Scheme came into force. This gave the power to refuse a carrier ATC to the UK for a passenger who had been denied entry and allowed a financial penalty to be imposed on the carrier airline.

Initially, *'there was some concern around intrusion into privacy. There was concern from people working in the field of human rights and data protection areas… It was about balancing the proportionality of the intrusion against the risk we tried to mitigate. The lower down the threat threshold you went, the harder it was to justify why it was necessary to intrude on people's lives'.*[192]

However, as mentioned, the main obstacle to the effectiveness of the e-Borders database and use of API and PNR data was legislative. This took the form of EU data protection legislation, in particular the 1995 Data Protection Directive 96/46/EC, and ensuing data protection regulations and legislation. In turn this meant that while from around April 2012 API was being received in relation to all non-EU flights, there were legal difficulties surrounding the collection and provision of API and PNR data by airline carriers from within the European Union. In addition there are also issues of data retention. As a senior police specialist explained, *'from a national security side, because we require the most data retention, the most intrusive use of the data sets, it's hard to capture data and retain it under the data protection law. There is a fine balance between negotiation and compliance. So even where we may have powers, we may choose not to use them because we try to persuade carriers to change their business processes to deliver effect for us'.*[193]

Nevertheless, *'the debate has matured. Part of the problem was that policy makers didn't quite understand it. For some, any form of data sharing was a dagger in the heart. The initial response was that we shouldn't do it without understanding what it was and how it was used. Now the policy community has a better understanding. They weren't prepared initially to expose how this data was used. That level of lack of*

[189] Interview with senior police specialist, 24 June 2015

[190] Details taken from interview with a former e-Borders Project Executive, 11 June 2015

[191] Interview with a former e-Borders Project Executive, 11 June 2015

[192] Interview with senior police specialist, 24 June 2015

[193] Interview with senior police specialist, 24 June 2015

understanding needed to change and has changed. You have to make people understand why it should be used and how it is going to be used'.[194]

7.6.3 Counter-terrorism effectiveness

Initially the e-Borders programme was found to provide real benefits to law enforcement agencies. In particular it was considered to provide a key component in the overall intelligence picture relating to the fight against terrorism and serious organised crime. It also resulted in numerous arrests in relation to various offences, including murder and rape. In addition, 'the facility to conduct travel history searches using e-Borders was also a valuable tool in the investigation of crime, because it allowed law enforcement agencies to establish the travel history of individuals of interest'.[195] However, ultimately the e-Borders programme 'failed to deliver the planned increases in API and this had a detrimental impact on the delivery of all the anticipated benefits'.[196] These difficulties led to revised data collection targets, and eventually even these had to be dispensed with.

Despite these problems, the National Border Targeting Centre (NBTC) prioritised the processing of e-Borders matches concerning individuals considered potential threats to national security, in the Pre-Departure Checks Scheme (PDCS). This measure to prevent such individuals from boarding an aircraft was introduced in July 2012 and is considered to have enhanced aviation security. In addition, PNR and API data from the Project Semaphore system and planned e-Borders project has proved of value to the UK's security and intelligence agencies in their counter-terrorism roles. While the UK does not profile terrorists using PNR (unlike a number of other countries), the PNR and API data has nevertheless proved extremely useful for counter-terrorism purposes. As a former e-Borders Project Executive explained, *'terrorism is a particularly violent form of criminality and there are some particularly clever people in that area of criminality and they will take actions to disrupt the pattern of their travel. The challenge is concluding the sharing agreement where you are targeting across national borders, the actions of people who can move freely'.*[197]

Consequently, the use of PNR alongside API and other intelligence has helped identify those passengers posing a higher risk. It has also proved supportive to those UK agencies involved in counter-terrorism. However, the problem is that the UK seeks to capture PNR up to 24 hours in advance and where possible up to 48 hours in advance. This has proved essential as many persons of interest travel at short notice. Part of the problem is the scale: there were estimated to be around 300 million passenger movements in or out of the UK in 2014. PNR capture was capped at 100 million records from up to 100 carriers, with a focus on risk and on the understanding that PNR was not available on all journeys. At the same time it was estimated that the UK will get around 20 million increase in PNRs each year.[198] Nevertheless, *'it is an effective counter-terrorism tool and it has become increasingly critical'.*[199]

7.6.4 Implementation challenges

Initially it was planned to implement e-Borders at UK air borders, with the system being introduced at various airports, however, in the longer term the intention was to also introduce the system at rail and maritime points of entry into the UK. However, as a former e-Borders Project Executive explained, *'this project focussed on air-transport…there was effectively a gap in the rail and ferry ports in capturing the data due to their different set-up compared to airlines, in terms of collecting passenger data. The threats posed to general aviation and maritime which will always be a vulnerability for any country'.*[200] Consequently, initially commissioned in relation to air borders in 2003, a year later Project Semaphore was introduced as a pilot scheme before the full e-Borders programme was rolled out and deployed. Initially this appeared to be going well, and as a result, following the release of funds in 2006, in June 2007 a full business case for the introduction of e-Borders was produced.

In November 2007 a contract for the implementation and delivery of the full e-Borders was awarded to the Trusted Borders consortium, led by Raytheon UK (the UK subsidiary of the US-based Raytheon), who in the

---

[194] Interview with a former e-Borders Project Executive, 11 June 2015

[195] Vine (2013) p. 3

[196] Ibid. p. 4

[197] Interview with a former e-Borders Project Executive, 11 June 2015

[198] Data in last paragraph from an unpublished PowerPoint presentation by Rymer (2008)

[199] Interview with senior police specialist, 24 June 2015

[200] Interview with a former e-Borders Project Executive, 11 June 2015

meantime also assumed responsibility for managing the Project Semaphore system. As detailed, it was anticipated that the e-Borders system would be fully deployed and operating by March 2014. In the meantime, from December 2007, the Project Semaphore system was moved from a developmental project to a working mode. As part of the implementation, in March 2010 the NBTC was created to replace the Joint Borders Operations Centre (JBOC).

However, shortly after the Conservative–Liberal Democrat coalition government took over in 2010, the authorities cancelled the £750m contract with the US supplier Raytheon, citing long delays and a non-functioning database of terrorist suspects. Raytheon promptly sued the British administration for unfair termination of contract. Following an extensive legal review, an adjudicating tribunal ruled in favour of the US defence contractor Raytheon. As a result, the UK authorities were ordered to pay £224m in cancellation fees.[201]

An additional issue was that, to be truly effective, the e-Borders system was reliant on aircraft passenger carriers to provide API as a means of establishing an 'electronic border' in advance of the physical border itself. While by 2012 such API data was being supplied by carriers outside the EU, due to EU data protection legislation and regulations, the information provided by EU carriers was more limited. Consequently, while the programme had the technical capability to receive such API data from general aviation carriers, there were limitations to the amount and level of API data being received. In theory, therefore, e-Borders would provide a range of interfaces for carriers to provide API and PNR data, but when such data was supplied, it varied considerably in detail and quality, with no clear format or system. The sheer scale and increasing number of travellers made it increasingly difficult to manage. And this was in addition to the problems of the provision of data from EU carriers.

The lack of a reliable source of data also impacted in other areas, apart from security. As an official inspection commented, 'the e-Borders Programme business case indicated that e-Borders would allow foreign national passengers to be counted in and counted out of the UK, providing more reliable data for the purposes of migration and population statistics and in planning the provision of public services. However, we found that the data set collected by e-Borders was not extensive enough for these purposes. A report from the Office for National Statistics stated that e-Borders data would not be of use for the purposes of migration statistics unless virtually universal data capture could be achieved. The best case scenario was that no migrant count could be produced based on e-Borders data until 2018 at the earliest'.[202] Finally, 'poor quality data on some of the match lists used by the e-Borders system created inefficiencies in NBTC. Out of date and irrelevant entries on the watch lists resulted in a greater volume of work, which NBTC staff were unable to manage'.[203]

The failure of the Raytheon-led consortium to meet key milestones in the contract, which led to its cancellation, meant that e-Borders was taken 'in house' by the UK Border Force and continued to rely on the original Project Semaphore IT platform, which was enhanced and upgraded over time. While it had always been a plan to roll out an e-Borders-type programme to rail and maritime border points, as a result of an inspection in 2013, when it became apparent this was not working, it was proposed to drop specific targets for rail and maritime passenger data. Currently, the e-Borders programme as it stands, which officially came under a new programme titled 'digital services of the border' since 2010 (revised and updated Project Semaphore IT), is officially capable of processing and checking the identities of 80% of arriving visitors and apparently a new computer system is being developed to supersede it.[204] As a UK senior police specialist explained, *'it's a lengthy process, because the legislative landscape and the capability landscape change continuously over time'.*[205]

---

[201] See Thomson (2014)

[202] Vine (2013) p. 4

[203] Ibid.

[204] Details in last paragraph from Thomson (2014) op. cit.

[205] Interview with senior police specialist, 24 June 2015

7.7 ShotSpotter

7.7.1 Context

Gun violence in the United States is staggeringly high: nearly 68% of murders in 2007 involved a firearm.[206] Yet, the rate of gunshot reporting remains problematically low. In Baltimore, the police claims that for every reported gunshot, there are four shots left unheard and/or unreported.[207] Another study conducted by the police in Milwaukee reveals that only 14% of the surveyed residents were likely to call 911 for gunfire.[208] Evidently, community reporting fails to capture the true extent of gun-related crimes. Facing similar predicaments in East Palo Alto in 1990s, an engineer named Robert Showen developed gunshot detection technology for local law enforcement purposes.[209] Today, more than 70 jurisdictions use the technology, starting with Redwood City in the mid-1990s, to Brooklyn in 2015.[210]

The gunshot detection system, called ShotSpotter, is essentially a network of sensors connected to a central computer program and global positioning system. Once the sensors register a loud bang, its acoustic signature is analysed, and the GPS determines the time and location of the noise. The program seeks particular audio qualities of a gun blast, whose sound is distinct from other explosive sounds because it is directional. When an alert is triggered, trained officers verify the sound and visually evaluate the recorded sound wave. Only after this review are dispatch orders are made. On average, the whole process takes about 40 seconds.[211]

7.7.2 Civil liberties implications

Despite the impressive technological achievement, ShotSpotter faces a similar predicament as do CCTVs surrounding the issue of privacy.[212] While the manufacturer argues that 'unlike CCTVs, gunshot detection systems can provide law enforcement with ability to monitor the public without "spying", the microphones are technically capable of picking up conversations.[213] More controversial is when the sensors record incriminating evidence, which can be used in trials.[214] In one case in Washington D.C., ShotSpotter data served in strong defence for the off-duty police officer who killed a 14-year-old boy.[215] Regardless of its efficacy, privacy law professor Eben Moglen argues that ShotSpotter has Fourth Amendment implications: incriminating information generated by ShotSpotter should not be allowed as evidence, as 'it constitutes a warrantless search and seizure by collecting public sounds.'[216]

7.7.3 Counter-terrorism effectiveness

The effectiveness of the ShotSpotter system as a counter-terrorism measure must be studied in light of its effectiveness as a law enforcement tool; the assumption is that if the system is effective as a crime prevention and response tool, it may be useful for counter-terrorism.[217] Despite the various stated benefits, whether ShotSpotter actually improves police effectiveness remains hotly debated, because findings from various studies and expert testimonies often conflict. To date, only a handful of formal assessments have been undertaken on the effectiveness of ShotSpotter.[218]

---

[206] Choi et al. (2014)

[207] Fenton and Wells (2014)

[208] Bourg (2014)

[209] Goode (2012)

[210] Bourg (2014); Schlossberg (2015)

[211] Petho et al. (2013)

[212] Ram (2014)

[213] Choi et al. (2014)

[214] The Economist (2014)

[215] Petho et al. (2013)

[216] Schlossberg (2015)

[217] Research interview with Kimo Quaintance, Lecturer, George C. Marshall European Center for Security Studies, Germany, 30 June 15

[218] Fenton and Wells (2014)

One study highlights the relative benefits of ShotSpotter compared with those of community reporting.[219] The findings illustrate that ShotSpotter significantly improve police effectiveness in two dimensions: response times and time to dispatch. The system, however, did not improve the overall resolution of gun-related crimes. This implies that quicker response and dispatch rates are not sufficient to enhance general police effectiveness: ShotSpotter must be employed in tandem with other sophisticated investigative equipment, such as CCTV.

These findings were supported by a series of interviews with commanders, detectives, patrol officers, dispatchers and analysts.[220] The respondents generally agreed that ShotSpotter is useful for police response, corroborative investigations, and crime pattern detection – that ShotSpotter produces more accurate, real-time and strategic intelligence for police investigations and helps identify hot spots for which resources can be distributed accordingly. These perceptions contradict those presented in an earlier study, but this could be attributed to either the improved technology or wider application since adoption.[221]

7.7.4 Implementation challenges

The system is not without challenges, however. The first is technical: ShotSpotter cannot accurately pick up gunshots fired indoors or at extreme proximity.[222] Besides, certain circumstances can cloak acoustic signatures required to identify gunfire – for instance, the canyon-like structures of an urban landscape.[223] A bigger problem has to do with false positives. In Suffolk County, New York, police claimed that merely 7% of gunshots identified by ShotSpotter system 'could be proved to have happened.'[224] To worsen the situation, criminologist Daniel Webster argues that police forces in many cases do not have adequate resources to respond to gunshot reports.[225] Consequently, sending officers 'chasing phantoms' triggered by copious ShotSpotter alerts can lead to a significant waste of police resources.[226]

The second challenge concerns citizen perception of the effectiveness of or the need for ShotSpotter. While its proponents claim that the system increases police visibility and effectiveness, thereby improving police–community relations, its opponents state that the system is creating a false sense of security at the expense of taxpayer money.[227] Some even refute the need to install the system in their community. When Baltimore police authorities implemented the system without the consent of the Charles Village community, various local groups raised objections, asserting that the community does not have a gun violence problem (which they believed was implied in the installations).[228]

Lastly, police departments are generally facing budgetary issues. The deployment of ShotSpotter requires a considerable upfront investment for police departments, even more so than police surveillance drones, whose costs are replaced by reductions in costs in human operations.[229] Demonstrably, the recently announced two-year pilot program in Brooklyn, New York, is estimated to cost $1.5 million annually.[230] Given the demanding investment required, the crime landscape must decisively warrant this technology. James Beldock from SST echoes this view: 'With gunfire rates as low as they are in the UK [for instance], the cost-benefit equation needs to be carefully thought through.'[231] Nevertheless, as small arms have been the weapons of choice for recent terrorist attacks in urban environments (e.g. Paris), a technology based on the operating principles of ShotSpotter may become relevant also for counter-terrorism purposes.

---

[219] Choi et al. (2014)

[220] Selby et al. (2011)

[221] Mazorelle et al (2000)

[222] The Economist (2014)

[223] Petho et al. (2013)

[224] The Economist (2014)

[225] The Economist (2014)

[226] Bourg (2014)

[227] Mazorelle et al. (2000)

[228] Chang (2008)

[229] Research interview with Kimo Quaintance, Lecturer, George C. Marshall European Center for Security Studies, Germany, 30 June 15

[230] Schlossberg (2015)

[231] Ram (2014)

In order for ShotSpotter to be effective in policing, it must achieve a certain threshold of sensor density. Further, the system has to work in synchronisation with other technologies through a consolidated platform that provides adequate training and guidance for activation procedures.[232] Without the complementary infrastructure, such as high-quality video camera systems or a centralised dispatch centre, ShotSpotter data can be rendered ineffective.[233] This aggravates the cost problem: the police departments under budget constraints have to make difficult choices, especially when they have a shortage of police officers to respond to the alerts in the first place.[234]

7.8 Data Retention Directive

7.8.1 Context

In 2006, the European Parliament and the European Council adopted the so-called Data Retention Directive (DRD) (Directive 2006/24/EC), which established an obligation to retain traffic and location data 'generated or processed by providers of publicly available electronic communications services or of a public communications network' (Article 3(1)). According to the directive, member states were obliged to adopt legislation to ensure that these data were retained for a period between 6 months and 2 years, so as to be available 'for the purpose of the investigation, detection and prosecution of serious crime' (Article 1(1)).

The Data Retention Directive was presented by several institutional actors as a reaction to the attacks in London and Madrid, and its potential for counter-terrorism has often been advocated. However, the DRD triggered an impressive amount of critique across the EU, and it has been challenged in several constitutional courts (e.g. Germany, Romania, Belgium). The Data Retention Directive has also been brought twice before the European Court of Justice (ECJ), which finally declared it incompatible with fundamental rights in 2014. Besides general criticism, the transposition and implementation of the Data Retention Directive proved particularly difficult, and its impact on counter-terrorism proved difficult to estimate.

7.8.2 Civil liberties implications

The DRD has been one of the most controversial pieces of EU legislation concerning counter-terrorism. From the outset, it was heavily criticized, especially by civil liberties campaigners, who held that it would cause harm to the rights to privacy and data protection. The Data Retention Directive is an example of the ongoing trend towards digital surveillance relying on commercially generated data that are subject to blanket retention and stocked 'just in case'. The civil liberties implications of this kind of counter-terrorism practice are well summarized in the European Court of Justice judgment.[235]

The cases brought before the ECJ both challenged the validity of the DRD and questioned the compatibility of the DRD with the 'rights of privacy laid down in Article 7 of the charter and Article 8 of the ECHR' (Case C-293/12, para 2). Additionally, both cases challenged the directive on whether it was really able to achieve, and in a proportional way, the objectives pursued, without unjustifiable interference with fundamental rights. The European Court of Justice held that the DRD did in fact constitute a violation of the charter rights because the EU legislature had exceeded the limits of the principle of proportionality (Articles 7, 8, 52). The ECJ held that the directive failed to meet the proportionality requirement laid down by Article 52 of the charter, arguing that there is a 'general absence of limits in the directive' and that it 'fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities' (para 60). Furthermore, the court found that data retention for the later purpose of access by national authorities does directly 'and specifically affect private life and the rights guaranteed by Article 7 of the Charter' (para 29). The court also points out that any interference with fundamental rights must be, in accordance with Article 52(1) of the charter, 'provided for by law, respect their essence, and subject to the principle of proportionality' (para 38). Regarding proportionality, the court holds that the objective, although provided for by law, and in accordance with fundamental general interest, does not in itself 'justify a retention measure such as that established by the Directive' (para 51).

---

[232] Selby et al. (2011)

[233] Bourg (2014); Choi et al. (2014)

[234] Goode (2012)

[235] ECJ. 2014. Joined Cases: Digital Rights Ireland v Ireland and Seitlinger and Others (C-293/12 and C-594/12)

7.8.3 Counter-terrorism effectiveness

While the text of the DRD foresees an evaluation procedure, the criteria to be evaluated do not include an assessment of its effectiveness in terms of counter-terrorism. This is due to the legal basis on which the DRD had been adopted, which concerns the harmonization of the internal market rather than counter-terrorism and internal security. However, the 2011 evaluation report released by the European Commission noted that 'data retention is a valuable tool for criminal justice systems and for law enforcement in the EU'.[236] While the report did not provide any detail concerning its effectiveness in terms of counter-terrorism, further information was offered by member states in the follow-up exchanges with the European Commission. For example, in a document presenting 'evidence for necessity of data retention in the EU' made publicly

[236] European Commission. 2011 p. 1

Appendix F: Analysis of relevant case law

Below, we briefly analyse the most relevant case law of the European Court of Human Rights concerning counterterrorism and human rights. Each case concerns either counterterrorism practices or issues relevant in case of deployment of a TACTICS-like system: use of biometrics, stop and search powers, electronic surveillance, application of the so-called proportionality test and the tensions with human rights. For each case study we present the facts and the main issues at stake, the conclusions of the Court, the relevance and the lessons for TACTICS.

Case study	**Gillan & Quinton v UK (Application no 4158/05), 2010 – ECHR**
Case issue and facts	The case originated in the UK. The two applicants were stopped on their way to a demonstration and were searched by the police. The applicants upheld that the sections of the Terrorism Act 2000 that allowed the police these powers gave rise to violations of Articles 5, 8 and 11 of the ECHR.
Holding	The court made several conclusions and holdings in response to the case. First, it ruled that the stop and search powers under section 44 were a breach of privacy rights yielded by Article 8 ECHR. The rationale can be found in paragraph 63 of the decision: 'Although the search is undertaken in a public place, this does not mean that Article 8 is inapplicable. Indeed, in the Court's view, the public nature of the search may, in certain cases, compound the seriousness of the interference because of an element of humiliation or embarrassment.' Second, the court considered the powers of confirmation of a stop and search authorization not in accordance with law due to the fact that they are not sufficiently circumscribed and that they lack satisfactory safeguards against abuse. Again, this constitutes an unjust interference with Convention rights that is not allowed as derogation in terms of its objective. Paragraph 80 gives the rationale: '[In sections 44(4) of the Terrorism Act]: There is no requirement at the authorization stage that the stop and search power be considered "necessary" and therefore no requirement of any assessment of the proportionality of the measure'.
Relevance for TACTICS	Examining how the UK stop and search policy was in breach of the Convention therefore can assist in drawing important lessons for what requirements and standards such counter-terrorist laws as the UK Terrorism Act must uphold.
Lessons for TACTICS	Powers of stop and search prescribed by national law must be in accordance with Human Rights. The criticism of Section 44 of the Terrorism Act and the ruling from the ECHR resulted in reform from the Home Office and the Freedom Act 2012 that amended the section. Gillan highlights the necessity for counterterrorism legislation to be in accordance with the Convention, and it emphasizes that such legislation, regardless of the importance of its objectives, must not fail to demonstrate necessity, proportionality, purpose and transparency.

Case study	**Klass & Others v Germany (no. 502971), 1978 – ECHR**
Case issue and facts	The case originated in Germany. The applicants challenged a German law that permitted German authorities to listen in on citizens' phone conversations, open

	their mail, etc. The applicants claimed the law interfered with their rights under Article 8 of the ECHR, 'respect for family and private life, home and correspondence'. The cardinal issue was whether the interference of the German law was justified under paragraph 2, Article 8. Specifically, the legislation was challenged on the fact that it was secret, as there was no requirement upon the authorities to notify the persons after surveillance had been authorized.
Holding	The Court held that the relevant legislation in fact upheld the requirement of having a legitimate aim, which is prescribed by paragraph 2, Article 8. After having considered the proportionality of the German law and whether it was within the bounds of what is necessary in a democratic society, the Court held that under exceptional conditions such as for the prevention of crime, giving special consideration to the growing development of terrorism, the state must be able to undertake the secret surveillance of 'subversive elements operating within its jurisdiction'. The Court however emphasized that any such surveillance methods must guarantee adequately and effectively against abuse. In relation to the secrecy of a specific surveillance activity, the Court also held that not informing the individual that they are under surveillance needs to be tolerable under Article 8 as it is this very fact is essential to ensuring the measure's efficacy.
Relevance for TACTICS	Klass is important because it was one of the defining cases on surveillance of individuals from the European Court of Human Rights. The case of Klass is noted as the first in a long line of Strasbourg decisions on individual rights against surveillance that developed the framework of jurisprudence that, in terms of rhetoric, was restrictive on the power of the states to enact surveillance measures by referring to Article 8 of the ECHR and the protecting of privacy rights.
Lessons for TACTICS	The judgement elaborates upon the issue of secret surveillance and the trade-off between security and civil liberties. Importantly, it decides that, following the Convention, derogations from the principle of non-interference with privacy rights are allowed, but that specific safeguards have to be followed. In particular, the decision explicitly puts into words what is now the general framework of the ECHR on the matter: Paragraph 2 of Article 8 ECHR is to be *narrowly interpreted.* This means legislation that derogates from principles of Article 8 will only be allowed insofar as that derogations are strictly necessary for protecting and safeguarding democratic institutions. Any such derogations must also meet the strict criteria provided by Article 9, including being in 'accordance with law; necessary in a democratic society and in the interest of national security.'

Case study	**Murray v UK (no. 14310/88), 1994 – ECHR**
Case issue and facts	The case concerned a challenge to the British anti-terrorism legislation – the Prevention of Terrorism (Temporary Provisions) Act 1976 as well as section 14 of the Northern Ireland (Emergency Provisions) Act 1978. The facts of the case were that two brothers of the Irish Murray family were arrested and convicted in the United States for being involved in the supply of weapons to the Provisional Republican Irish Army. The mother, Mrs Murray, was then arrested in Belfast under section 14 of the Emergency Provisions Act. The applicants claim was that Mrs Murray's arrest and detention were both illegal, particularly on the ground that there had been no real suspicion that she was

	actually guilty of a crime. The issue in the case is one of alleged breaches of Articles 5 and 8 of the ECHR and, like Gillan, reasonable suspicion.
Holding	On the matter of the alleged violation of Article 5, the Court questioned if the arrest was based on reasonable suspicion and thus in accordance with law, or whether this was not the case. However, after consideration, the judges found that the suspicions laid as grounds for Mrs Murray's arrest were in fact reasonable and that the arrest and detention therefore satisfied the 'lawfulness' requirement. The second challenge from the applicant was that the purpose of her arrest was not in accordance with what was allowed under Article 5 (to bring the suspect before a competent court). Also on this point the Court rejected the applicant's argument. The Court ruled there had been no violation of Article 5 in respect of the 'first applicant' (paragraph 70). Also on the alleged breaches of Article 8 of the Convention, the Court held that there had been no violations.
Relevance for TACTICS	The case is particularly relevant for counterterrorism because it concerns arrest and detention, and it does so from both the perspective of Article 8, Right to respect for private and family life, and Article 5, Right to liberty and security.
Lessons for TACTICS	The dissenting opinions in this case are interesting. Specifically the joint dissenting opinion from judges Loizou, Morenilla and Makarczyk, stating among other things that they do not agree there has been no Article 8 breach and stating clearly that in their view there has been an explicit breach of the fundamental rights of liberty, security and privacy when the armed forces conducted a search of the applicants and their house/property at 7 a.m. without a warrant. This dissenting opinion is especially interesting for TACTICS as it discusses how, even if the case is one that pertains to special circumstances due to its nature of involving issues of terrorism, the dissenting judges still set high standards for how far they are willing to stretch the law in order to privilege security over civil liberties.

Case study	**Liberty and Others v UK (no 58243/00), 2008 – ECHR**
Case issue and facts	Liberty (the Irish Council for Civil Liberties) and several other British non-governmental organisations challenged the Interceptions of Communications Act 1985 giving provision for the surveillance program (Electronic Test Facility, ETF). The issue was whether this Act was in breach of fundamental privacy rights – provided by Article 8, ECHR.
Holding	The ECHR made several conclusions: The Court held that the Act was in breach of rights under Article 8 and thus violated the Convention. The rationale for the decision emphasized how the 1985 Act provided far too great a discretion to authorities – a discretion that was virtually unfettered and therefore widely susceptible to misuse. Additionally, the Act did not demonstrate sufficiently neither the necessity of the legislation nor the objective for providing as wide discretion as it did. In the end, the final blow to its validity was the failure to provide safeguards, protecting individuals against abuse of power from the authorities, in terms of government surveillance that was not in accordance with the law. Its lack of transparency was also criticized, as the legislation did not make provision for the measures to be scrutinized by the public; indeed, it made it so that no part of the surveillance procedure (selection, storing, processing of data) was available to the public.

Relevance for TATICS	The decision provides important guidelines for counter-terrorist legislation. It highlighted that the legislation allowing the ETF surveillance program in UK in the 1990s was far too vague and ambiguous, failing, first, to meet the 'in accordance with the law' test and the procedural requirements for surveillance laws under the Convention, and second, the much more important substantive test of being 'necessary in a democratic society'.
Lessons for TACTICS	The case reaffirms Strasbourg's strict approach when it comes to surveillance cases and the balancing of civil liberties and security concerns. Any legislation that provides for secret surveillance is in itself a violation of the Article 8 under the European Convention on Human Rights.

Case study	**S and Marper v UK (no. 30562/04 and 30566/04), 2008 – ECHR**
Case issue and facts	The case originated in the UK, and was brought by two individuals who took legal action to have their DNA records removed from the relevant databases. The issue of the case was whether or not the retention of biometric data, such as DNA and fingerprints, from innocent people was inconsistent with the fundamental rights laid down by the Convention.
Holding	The Court upheld the argument of the applicants and ruled that the retention had been in breach of Convention rights. On the matter of Article 8, the Court concluded there had been a violation, stating 'the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard' (paragraph 125). Accordingly, the Court decided the retention did not meet the criteria for interferences with fundamental rights, seeing as it was not proportionate with the applicants' right to respect for private life and that it could not be seen as something necessary in a democratic society.
Relevance for TATICS	In its decision, the ECHR stated that the retention of biometric data, such as fingerprints and DNA, constitutes and infringement upon the fundamental human rights, especially the right to respect of private life as per Article 8 of the Convention. Such a decision had a significant impact upon counterterrorism legislation in Europe, and particularly in the United Kingdom, which as a consequence had to reform their statutory scheme (the PACE Act) which in part led to the enactment of the Protection of Freedom Act 2012.
Lessons for TACTICS	It is important to note that the Court stated that it was the mere storing of the data relating to the private life of an individual that amounted to an interference with the rights under Article 8, and not the effect such retention had in practice. In the Protection of Freedoms Act 2012, the UK coalition government reformed the law that allowed for retention. The reformed law and was called a significant progress – at least relative to the old regime. One point that was particularly criticized was the fact that even if the law has changed for those who are innocent, those who are convicted still have their data retained for an indefinite period of time.