TACTICS PROJECT DELIVERABLE

SEVENTH FRAMEWORK PROGRAMME

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

TACTICAL APPROACH TO
COUNTER TERRORISTS IN CITIES

TACTICS

Tactical Approach to Counter Terrorists in Cities

Deliverable details	
Deliverable number	4.3
Title	Privacy, Ethics and Human Rights report. The main challenges of counter-terrorism in cities
Author(s)	PRIO, TNO
Due date	30/11/2014
Delivered date	16/03/2015
Dissemination level	PU
Contact person EC	Mr. Ngandu Mupangilai

Cooperative Partners	
	TNO
	ITTI
	LERO

Disclaimer

This document contains material, which is copyright of certain FP7 TACTICS Project Consortium parties and may not be reproduced or copied without permission. The information contained in this document is the proprietary confidential information of certain FP7 TACTICS Project Consortium parties and may not be disclosed except in accordance with the consortium agreement.

The commercial use of any information in this document may require a licence from the proprietor of that information.

Neither the FP7 TACTICS Project Consortium as a whole, nor a certain party of the FP7 TACTICS Project Consortium warrant that the information contained in this document is capable of use, or that use of the information is free from risk, and accept no liability for loss or damage suffered by any person using the information.

This document does not represent the opinion of the European Community, and the European Community is not responsible for any use that might be made of its content.

Copyright notice

Table of Contents

Executive Summary

This report has two distinct segments. The characteristics of urban areas relevant to understand how privacy and civil rights apply there are analysed in the first part of the deliverable (sections 2 and 3). Knowledge about the tactics, techniques and procedures necessary to understanding terrorist threats and how they are targeted by governments is provided, and linked with principles and standards of civil and individual rights. In the second part of the report (section 4), the legal and the rights issues that will come into play through the eventual implementation of technological systems for monitoring and documenting activities in urban areas are analysed. A surveillance impact assessment (SIA), conducted on the TACTICS system in 2014, is presented and commented, in order to give a solid basis for this section.

1 Introduction and caveats

This deliverable (D4.3) provides a report of the main challenges of counter-terrorism in cities, in particular from a privacy, ethics and human rights perspective. While presenting some of the most salient implications of counter-terrorism in (European) urban environments, it mostly focuses on the peculiar issues at stake in relation to the development, and the potential deployment, of a TACTICS-like system.

Furthermore, this deliverable offers a summary of the Surveillance Impact Assessment (SIA) that the TACTICS research team has carried out together with the SAPIENT project.[1] It also lists the main solutions identified so far, as well as some general comments on the overall experience of carrying on a SIA. Indeed, the completion of the SIA, under the guidance of the SAPIENT project and following their draft SIA Handbook,[2] should be considered both part of the TACTICS Privacy by Design approach and the occasion to test a potentially important tool that was still under finalization.

This report has no ambition to provide an exhaustive analsis of all ethical, legal and socio-political aspects potentially linked to TACTICS. While it builds upon the activities of the work-package (WP) 4 “Threat decomposition”, it rather functions as a general introduction. Other key aspects of the TACTICS system and the TACTICS project are presented and discussed in two parallel deliverables: D5.4 – Privacy, ethics, human rights, legal conditions; and D6.2 – Privacy, Ethics, Human Rights.[3]

Furthermore, it should be noted that these reports should not be considered as an ethical and/or legal validation of the TACTICS system, but rather as a ‘companion’ to the work carried on within the TACTICS project. As such, they aim at highlighting challenges and formulating possible solutions and recommandations. The main reason is that the very purpose and scope of TACTICS-like systems necessitates an adoption at national level, and therefore a preliminary adjustment, and verification, of its design to specific national legal requirements and administrative constraints. While the European Union (EU) and the international legal frameworks provide essential references and guidance, the conditions of possibility and legitimacy of counter-terrorist systems are highly dependent on national legislations and regulations. Therefore, the decisions taken in each specific implemention of TACTICS would be crucial for the ethical and legal validation of the system, and each time a tailored, and thorough, assessment will be needed.

The present deliverable is divided into 5 sections. Section 2 briefly describes the key features of the TACTICS project and of the TACTICS system. Section 3 highlights the

[1] SAPIENT – Supporting fundamentAl rights, PrIvacy and Ethics in surveillaNce Technologies – is a collaborative project funded by the European Union (EU) Framework Program (FP) 7, which “provide[d] strategic knowledge on the state of the art of surveillance studies, emerging smart surveillance technologies, and the adequacy of the existing legal framework”, cf. http://www.sapientproject.eu/about.html#_Toc290046988

[2] The SAPIENT project developed a “Surveillance Impact Assessment Manual” (or SIA Handbook), which has been designed by consortium partners on the basis of the research done, and the testing of a draft version on other projects. As discussed further in section 4 below, the TACTICS project accepted the invitation to test the draft SIA Handbook. The final version of the SIA Handbook is publicly available online: http://www.sapientproject.eu/SIA_Manual.pdf.

[3] The other two ‘ethics reports’ – D5.4 and D6.2 – are public deliverables available online on the TACTICS website: http://www.fp7-tactics.eu/news.html.

characteristics of urban areas that are relevant to achieving a better understanding of how privacy and civil rights may apply in counter-terrorism. Section 4 summarizes the SIA process undergone by TACTICS and the next solutions identified so far. Finally, section 5 provides a final list of considerations and possible further steps to be considered after the end of the project and before any implementation of TACTICS-like systems.

2 The TACTICS project and the TACTICS system(s)

TACTICS is a 36 month research project funded by the European Union under the EU 7th Framework Programme FP7-SECURITY.[4] Its overall objective is to develop a TACTICS Decision Support System, able to support counter terrorism in urban environment, while respecting high level of standards of protection of human rights, and in particular privacy and personal data protection. Indeed, as stated in Deliverable D3.1 – "Conceptual Solution Description (White Paper)", the main goals of the TACTICS project are:

1. to make security forces capable of responding quicker, without being biased in decision making and to be more precise in the kind of information they request and the orders they send out by providing expert knowledge at the fingertips of the professionals of the security services at the time of an actual threat in urban environments (threat management);

2. to improve preparedness of security forces by decomposing threats into observable terrorist behaviours specific for urban environments (threat decomposition);

3. to improve the capabilities at security forces' disposal by improving their management, efficiency and their cooperation in urban environments (capability management);

4. to facilitate a cross-European approach by offering a 3-levelled strategy on the tactical, operational and strategic level.

As such, the TACTICS project does not aim at building from scratch a new law enforcement and/or surveillance system, but rather designing a sort of system-of-systems. Ultimately, the promise is to facilitate and optimise the coordinated use of, and access to, already existing systems. Yet, the design, the set up, and the eventual implementation, of a system-of-systems should not be considered as a mere technicality, or just a process of rationalization, modernization or optimization. While there are crucial differences between the creation of an *ex novo* system and the development of a system-of-systems, both present important ethical, legal and socio-political implications. As noted through this report and the parallel deliverables D5.4 and D6.2, this is especially the case for a system-of-systems supporting counter terrorism in cities. For example, by connecting systems previously kept separate, this kind of system-of-systems may further the intrusion in the private lives of several innocent individuals. Moreover, the possible connection to, and use of, information acquired by, or through, commercial systems may prove problematic not only from a technical point of view but also from an ethical and legal point of view.[5]

It is useful to make a first distinction between 'TACTICS as a project', or 'TACTICS as a validation system', and 'TACTICS as a Decision Support System' or 'Tactics as a system (of systems)'. Indeed, on the one side, among the goals of the TACTICS as a project is not only the design of the TACTICS Decision Support System,[6] but also its validation. The present report does not cover the validation process, as it is still on-going. On the other side, it should be noted that the TACTICS Decision Support System is not designed as a ready-made tool, to be automatically implemented, but it will be the result of a research project aimed no higher than Technology Readiness Level (TRL) 5. Hence, it will not be used in any concrete threat situations, nor will be automatically adopted by any European

[4] http://www.fp7-tactics.eu/index.html.

[5] This is discussed in D5.4, sects. 6.2-6.3.

[6] For a more detailed overview of the prospective TACTICS Decision Support System, see D 3.2.

or national institutions as such. Yet, it is possible that it will prove inspirational for the concrete design, and eventual implementation of similar, TACTICS-like, systems. For this reason, while the prospective TACTICS-like systems are out of the scope of this report, the deliverable includes considerations that decision-makers may want to consider when discussing the adoption of similar systems.

Finally, it should be reminded that several TACTICS project deliverables are deemed sensitive, and thus the applicable dissemination level is often ‘Restricted’ (RE). This does not permit to delve into the details of the functioning of the TACTICS system. Nevertheless, the descriptions of the TACTICS system provided in the public deliverables D3.1 and D3.2 already offer a quite substantive glance and its main purposes and features.[7] Also, the full version of the SIA carried on in conjunction by the TACTICS and the SAPIENT projects is restricted. However, this is due not to the SIA report itself, but to the default rules applying to both projects.

[7] D3.1 and D3.2 are available online at: http://www.fp7-tactics.eu/news.html.

3 Urban areas, terrorist threats and civil rights

In this section, the report documents and analyzes the characteristics of urban areas relevant to understanding how privacy and civil rights apply in relation to the design and possible functioning of a TACTICS-like system. It links knowledge about the tactics, techniques and procedures necessary to understanding terrorist threats, with principles and standards of civil and individual rights. In the subsequent section, PRIO analyzes and documents the legal and rights issues that will come into play through the eventual implementation of technological systems for monitoring and documenting activities in urban areas, focusing on the risks related to the TACTICS system as a research project and as a system-of-systems.

3.1 Introduction

A core characteristic of the urban area is the density, the crowdedness, the possibility to be ‘lost in the crowd’. Urban communities are composed of a greater variety of people than the more rural ones. This implies among others that the perception of central civil values diverges more than in more homogenous communities. On the one side, the issue at hand is the state’s obligation to provide a sufficient level of security and freedom in its urban areas. On the other side is the state’s negative obligation to provide security and freedom, understood as the obligation not to interfere unnecessarily in individuals’ lives. An increase in the intensity of the various tactics and techniques applied to fight terrorism may *de facto* lead to more secure urban areas. Visible or publicly announced tactics or techniques may lead to a *perception* of more secure urban areas, regardless of the actual effects of the measures. This all relates to how the values of the urban areas are defined and understood, and how the balancing act is carried out between the values of the diverse members’ of the urban communities.

This chapter starts off with documenting and analysing the characteristics of urban areas that are relevant to understand how privacy and civil rights apply in these areas. Following the account of urban characteristics, the application of privacy and civil rights within these areas is discussed. The applicable privacy and civil rights will be analysed, but mainly conceptually in relation to their value. The legal specifics are accounted for in depth in D5.4 and D6.2, in relation more specifically to the TACTICS tools.

3.2 Urban characteristics

A comprehensive description of all the possible assemblages of urban elements, from natural to architectural, from socio-economic to political and symbolic, is not possible within the scope of this deliverable. In other words, despite some common characteristics, each urban environment is highly specific, and the same urban environment is often perceived and ‘lived’ differently by diverse institutions and people.

Some of the possible ‘combinations’ of these different natural, cultural and material elements have been explored elsewhere (cf. Deliverable D2.1), but even there the goal was not to provide an exhaustive taxonomy but rather identify particularly relevant scenarions. In this section, the aim is to attempt identifying some salient, and recurrent urban characteristics. However, the specific complexity of each urban environment is a key element to be considered both at the level of the design and of implementation of a TACTICS-like system. This has immediate implications in the existence, availability and functioning of specific capabilities. But it has also less evident, but potentially far-reaching implications in terms of the impact of the attack(s) to be handled and the counter terrorist response itself.

In general terms, urban areas are characterized by higher population density and (more or less) vast metropolitan features as compared to their surrounding areas. Urban areas may be cities, towns or regional conurbations, but the term is not commonly extended to rural settlements such as villages and hamlets. Yet, while the urban tends to imply the exclusion of the rural, it still describes a vast variety of diverse material and social arrangements, and different possible relations with nature and economics. In such policy-making urban terror attacks are viewed as inevitable and unavoidable, but the nature of such attacks is seen as fluid (Coaffee 2000).

Cities are in this context not only the landscape or background of attacks, but also the issues at stake, and the targets (symbolic and material) of the attacks themselves. The urban area is not just another *scenario*. It is the target but also the crucible of political violence (Coward 2006; Graham 2001), and is vulnerable as densely populated political, economic and cultural centres (Coaffee 2013; 2000). In the language of some security agencies: urban areas are rarely sanitized environments, but rather sites embedded within more or less ordered streams of social, political and economic activities.

Dealing with (possible) terrorist attacks or any insecurity factor implies the potential involvement of several kinds of actors: from by-standers to private companies, from religious and political representatives to law enforcement agencies with different levels of competences and specialisation.

A way of approaching the complexity and multifacetedness of the urban areas, and the realtion to terrorist threats and other insecurities, is through the notion of ‘urban resilience’. This notion has gained significant force the last 15 years or so; before being reserved for protection and recovery from ‘natural’ or ecological hazards (Coaffee 2013, 243). Urban resilience and security is one of the central foci in the following. First, however, a discussion of the security threats and perceptions in various areas is made.

3.2.1 Crime and security: national, urban and rural localisations

All over the world, “urbanization grows, the cities become globalized and crime increases in complexity. This evolution forces us to reinvent the co-production of security in new contexts, with the participation of both state and local actors such as civil society” (Vanschueren 2013). Moreover, crime in general and terrorist related crime in particular is “increasingly polymorphous, complex and difficult to contain through the spontaneous social control which characterizes rural areas and small towns”, Vanschueren argues (2013).

The threat of terrorism in urban areas is subject of interest of politicians, security personnel and projects such as TACTICS because the risk it poses to the security of individuals in urban areas and the areas themselves, in terms of infrastructure, stability, etc. Threat to security is in this relation understood as the threat from various forms of crime, be it organised crime, theft, sexualised crime or terrorism crime committed with certain criminal purposes of spreading fear and anxiety. On a general basis, crime increased exponentially throughout the world from the 1960s to the 1990s (Findlay 1999). As Sergio Adorno has put it: “in a span of 30 years we have gone from a chronicle of crime as an exception to a chronicle of everyday crime and […] images of innocence are replaced by permanent and imminent danger” (Adorno 1997 quoted in Vanderschueren 2013). Nowadays, while crime in general may have seen a stabilization and even decline, the occurrence of serious crime such as terrorist related crimes is considered to be of such a serious nature that it requires increased efforts in terms of security measures.

There are, however, a multitude of reasons that security threats arise.

> The phenomenon of urban crime is multi-causal and derives from different variables depending on the urban context […]. In effect, it is the social fabric and the institutional and historical dimension of each city that may explain the variation of crime rates in a determined period. (Vanderschueren 2013)

Terrorist attacks or terrorist related crime may stem from *outside* the location in questions, but there are in an increasing degree local people involved.[8] What is necessary to consider is therefore whether the measure in question actually *may* provide increased security in the urban area. Counter-terrorist measures such as TACTICS systems and other anti-crime measures may be more or less effective in controlling, preventing or stopping security risks. It is in this relation crucial to recognize that different forms of crime have specific explanations. Nevertheless, there may be other more efficient or more appropriate measures or actions to ensure or promote urban security than those targeting crime or terrorist activity. TACTICS is as a point of departure being developed purely as a system-of-system to be used only in situations where a terrorist attack is imminent or on-going. Terrorist attacks are, fortunately, relatively rare. If the TACTICS system-of-system model is developed and implemented in national jurisdictions, it is likely that the scope of the system will be requested at least by some groups to expand also to other types of security threats, such as property crime, urban disorder or public violence. A more extensive use of TACTICS or related systems could have the consequence of taking the focus away from other less intrusive security measures than those of crime control, such as social and welfare measures focussing on institutions of socialization, such as the families, the schools and the neighbourhoods (see e.g. Mawby and Simmonds 2004).

Another aspect related to understanding why particular tactics, techniques and procedures are applied in urban areas may be found in what is known as the ‘securitisation’ trend, which started in the early 1990s. Buzan argued that security at the state level implied the absence of threats against the survival of the state itself. He emphasized security as a fundamental need for communities as well as individuals (Buzan 1991). Then, securitization entails an expansion of the security focus to include the security of the nation state (Bigo 2000, 343), and it tends to include a wider range of issues, thus including those that were traditionally considered out the realm of state security. In the same tradition, Huysmans noted that security often is defined merely by its opposites: the threats are described, without an explanation of the ideal secure situation (Huysmans 2006). This seems to apply to many cases of ‘new threats’ assumed to arise both internally, from society itself, and externally, from migrants (Buzan and Wæver 2003; Bigo 2000, 345).

In this report, it is not the *state* level, but the *urban* level of security that is targeted. Still, as Recasens *et al.* (2013, 370) note, the processes of globalization of security – and especially global terrorism, has increasingly introduced into European security policies the discourse of the ’primacy of repression’, the ‘criminal law of the enemy’ and the concept of a ‘war against crime’.

This emphasises the point, that must be understood also in the tactics of TACTICS, that such aspects are related to the *wider* problems of transnational crime, which are not, as yet, part of the ordinary tradition of urban security in European countries. This may imply that the security and safety of a particular urban area traditionally has been decided between the inhabitants of that area, and by the local authorities, but in the increasing

[8] It is for example an increasingly often voiced concern that young European Muslims travel and receive jihadist training abroad, before returning home to perform terrorist acitivities.

trend of globalization of security, these decisions are moved away from the local level.[9] Urban challenges or crimes such as prostitution may be turned into transnational issues of human trafficking (what Recasens *et al.* call ‘glocalisation’ processes: 2013, 374). Such tendencies may contribute to the uncertainties of what is now famously termed the ‘risk society (Beck, 1992; 2002), where the individuals are facing increased insecurity, fear and anxiety because of an overwhelming perception of omnipresent risks and threats. Securitisation processes hinge on certain (professional) actors' construction of (statistical) 'truths,' according to Bigo (2000). It is crucial, as already mentioned above, that the development of new security personnel tools, such as TACTICS, are assessed related to their necessity and proportionality.[10]

To instate a system-of-systems with the potential of mass-surveillance and control over the individuals in a large area has precisely a major *potential* to be applied in greater security-prevention contexts than merely that of counter-terrorism. Who wants the system(s), and for which reason(s)? Globalisation of urban issues may, however, be seen as transferring powers ‘upwards’, leaving the ‘global’ issues in the hands of the state. In Recasens *et al.*’s (2013) work comparing urban security in three of the south European countries, they find that there seem to be diverging perceptions of urban security also depending on whether the local police have strong powers (Spanish and Italian) versus where the local police have only very limited powers, and urban security responsibility lies primarily with the *national* police (Portugal). They argue that this is linked to the fact that what seems to be implied in the notion of ‘urban security’ has more to do with “prevention and the specific problems of coexistence of the everyday life of citizens than with serious crime and offences” (2013, 373). This is of course not an uncontested proposal, as one clearly could imagine that if the population within an urban area were under the impression that they lived under a constant threat of serious terrorist attacks, this would constitute a blatant urban insecurity. However, this may to some extent be the precise impression that inhabitants of the major cities actually have.[11] The recurring question is how the balance is struck between the perception that something is being done about the insecurity related to a (terrorist) threat and the value of personal freedom. This will be discussed more below in section 3.4. First, the report discusses the notion of urban resilience.

3.2.2 Urban resilience

The UK Government delivered over two years (2010 and 2012) strategic frameworks that emphasised that the threat of terrorism was real and imminent, and that it was necessary that a *range* of key partners should cooperate and work holistically to reduce the vulnerability of crowded places, i.e. urban areas. The UK example is typical of western states’ contemporary policy, and TACTICS may be seen as a good illustration of such a more holistically and preventive way of countering terrorism. The resilience policy may be seen as a prominent present-day tactic and technique from governments to maintain secure urban areas.

Resilience is both a conceptual and policy metaphor belonging to an array of academic disciplines, applied until the past decade or so only in theoretical contexts (Coaffee 2013,

[9] This is related to the same point as briefly discussed in D5.4 on the extension on all kinds of resources and capabilities into such *with anti-terror purposes*, and thus potentially making the entire society into a counter-terror resource.

[10] Details on the legal requirements of proportionality and necessity are found in D5.4.

[11] Recasens *et al.* also note differences *within* countries, for example between rural and urban areas, between major and smaller cities and between regions (2013, 375).

242). Resilience in a contemporary urban context may be seen as an organising principle of government action which highlights the impact of and recovery from various disruptive events, allowing the bridging of a long, diverse range of measures and disciplines' 'solutions' in meeting such events (*ibid*). Urban resilience may take the form of visible, fortress-like material security measures at high-risk sites, for example barriers preventing driving into the Government HQ streets of Oslo. TACTICS may be seen as a tool belonging to a later wave of resilience measures. Later waves of such measures are to some extent less physically visible, more preventive in purpose, and to a greater extent including more actors, public and private, in the responsibility to strengthen the urban resilience (*ibid*, 245-6).

In the urban context, resiliency objectives are typically the need for anticipatory and pre-emptive planning, holistic hazard management and integrated governance or response (*ibid*; O'Brien and Read 2005, 353). Former emphasis on *risk* is replaced with one on *resilience*, meaning that the *likelihood* of for example a terrorist attack in the latter way of thinking is less relevant than the 'what if'-policy frame. What this implies is that counter-terrorism measures such as TACTICS – or any security measures – are intended into a worst-case frame of mind. Translated to practice, this may mean that for example setting in motion an intrusive surveillance system-of-system would more easily be allowed at a pre-emptive stage of a (potential) terrorist attack because of the more likely and efficient 'bounce back' of the urban area in question. The value of privacy and other civil or human rights would be of less value in such a context, than that of a secure, resilient urban area.

Another assumption related to the resilient urban area is the holistic-ness by which dangers such as terrorism should be met. This means that not only the security personnel's tools (such as TACTICS) are important to create a secure, resilient city. Resilient urban areas are "constructed to be strong and flexible rather than brittle and fragile" (Godschalk 2003, 137). This means that city-planning, infrastructure, the way the urban environment is designed, etc., are all structured in fashions making them harder to break in the case of a terrorist attack (or other disaster of any sort).

Godschalk points at two central aspects of why urban resilience is important. The first is the unpredictability of precise knowledge of how technological and social systems may accommodate unforeseen disastrous events without critical failure. The second is that resilient cities, both related to people and property, simply cope better in case of disasters such as among others terrorist attacks. "In resilient cities, fewer buildings should collapse. Fewer power outages should occur. Fewer households and business should be put at risk. Fewer deaths and injuries should occur. Fewer communications and coordination breakdowns should take place" (Godschalk 2003, 138). This is, Godschalk argues further, dependant on community efforts and consistent attention to the political and social, as well as the physical, aspects of hazard mitigation. In other words: also the mentality of the individuals within the urban community in question must be made resilience-minded. The introduction of tools, instruments or city-planning is not sufficient in itself. But the mentality could and should be encouraged, as an example from the city of Tulsa shows, where inhabitants are given loans and free home-repair programs to make their homes more resilient. One could easily imagine the same incentives in a more directly counter-terrorism perspective such as TACTICS, for example where the government or city council (or other authority, security provider or such as insurance provider) gave loans to or even set as a precondition of a public service that the person or shop in question would connect her alarm system or CCTV or other type of resource, to the city's, or country's, etc., TACTICS system.

So-called 'community mitigation capacity' is the ability of the community socially to deal with disasters (Godschalck 2003, 140; Comfort 1999). This is only possible with a "strong public policy promiting community involvement", in addition to physical system hazard mitigation functions, for example in assisting threatened neighbourhoods and populations (Godschalk 2003). The latter, one could suggest in the counter-terrorism mitigation perspective, could be to involve and install more counter-terrorist resources in poorer or 'riskier' urban areas.

However, this does not take into account whether strengthening the resilient urban area implies increasing urban resilience but *de*creases the positive urban characteristics. Examples are the ability to be lost in a crowd or not be seen in a city park following the logic that lowered visibility is a risk, thus there should not be areas covered in darkness or not caught by CCTV cameras.

Another perspective, emphasising a more positive aspect of TACTICS, is that it actually makes use of exisiting resources and capabilities, instead of suggesting inserting more, new types of counter-terrorism instruments. It is well known that developed crime control instruments, for example various EU police cooperation instruments, may be seen as being developed without ever being set into force because they either are seen as not bringing any novelties and thus considered useless by the security personnel, or because the developed projects are technically un-implementable such as the different models of the Schengen Information System (SIS) before SISII finally entered into force in 2014.

3.2.3 The pertinence of terrorist prevention in urban areas

Vandershueren's argument (2013) above is not the only perspective on the pertinence of urban v. rural fight against terrorism. In January 2015, there was a major police raid in Belgium towards terrorists, including the so-called "Sharia4Belgium"[12]. The group had its main European headquarter for training and planning in a villa in countryside Belgium. The raid took place in several places, including the capital Brussels, but *primarily* in smaller towns and rural Belgium.[13] In the terror-attack on Norway on July 22 in 2011, the terrorist, Breivik, performed all his substantial planning and preparation in his rented farm in the remote Rena, 90 miles from Oslo. It has been suggested that one way of actually forseeing the planning of his terrorist action would be if local authorities and even neighbours actually checked what the vast amounts of fertilizer Breivik bought were used for (a bomb), since they clearly were *not* spread out on the fields (Ekanger in Ugelvik 2014, 340). The reason for emphasising these facts is to pintpoint the fact that the necessity or efficiency of TACTICS like systems (-of-systems) should be considered differentiated strictly between the preventive use and the mitigating use. Terrorist attacks may *take place* in urban areas, but they are planned and trained for in non-urban areas. *Prevention* or pre-emption of terrorist attacks, which one could well argue is the most important function of counter-terrorism measures, should focus on non-urban areas. Since many of the resources of TACTICS (like systems) are intrusive, their efficiency must be considered. One could imagine, based on these arguments, greater efficiency of TACTICS if it was extended outside of urban areas, basically to any type of area. This may well be a future solution. There are, however, challenges related to connecting all the resources and capabilities across greater areas such as regions, countries, even international 'regions' irrespective of national boundaries. One thing is the aspect of the all-seeing surveillance

[12] http://www.washingtonpost.com/world/why-is-tiny-belgium-europes-jihad-recruiting-hub/2015/01/17/4cc8c3b4-9dd5-11e4-bcfb-059ec7a93ddc_story.html [23.01.15]

[13] See also http://www.theguardian.com/world/2015/jan/16/belgium-terror-raid-jewish-schools-closed [23.01.15]

society. Another, and related aspect, is who would be the users and ultimate decision-makers in the system. The trouble of different national legal regulations and thresholds is discussed in TACTICS Deliverable 5.4. A system-of-systems involves raising the level of surveillance and possible interference in individuals' private life (etc.). This may be acceptable in a specific and limited area because of the common interest of mitigating or stopping an on-going or just happened terrorist attack. In such situations and within these limitations, there will at least as a point of departure be certain public security personnel of a high level within the local or national level having current and ultimate control over the on-going use of the system in the particular situation. In an 'extended' version, not limited to (a particular) urban area, one could envision situations where security personnel situated in for example Brussels, Belgium, having general overview over and the possibility to couple CCTV, police officers and information from an insurance database in for example the Rumenian or Norwegian outskirts? This may seem like far-fetched examples, where real life developments would implement the (perceived or legislative) necessary thresholds and barriers. The point is still strong, however: where, if any place, should the line be drawn for which resources and capabilities to be incorporated into a counter-terrorism system-of-systems?

3.3 Understanding the relationship between terrorist threats and civil rights in urban areas

Wolfendale discusses two assumptions related to the claim that basic civil and human rights must be sacrificed in order to fight the threat of terrorism. First, there is the assumption that terrorism poses a unique and far graver threat than other threats and second, there is the assumption that undermining civil liberties and legal protections is the most effective way to combat terrorism.

There are as already mentioned certain aspects of privacy and civil rights that are particular to or particularly valuable in urban areas. These are partly related to the nature of the cities and urban areas as prominent locations for expression of difference and political, religious and other forms of freedom, what could be termed 'threats to the identity and personal liberty' of a person. Partly, they may also be related to the general privacy aspect of the individuals (Goold 2009, 207).

As already mentioned, a main concern of this report is the relationship between civil and privacy rights in the urban areas and the control of areas and individiduals to prevent or stop terrorist attacks. What is the relationship between data protection and privacy, and socio-political values and practices related to security? This is a much debated field in academic discourses (see for example Bennett 2011, 2008; Lyon 2007; Neocleous 2007; Zedner 2005). A central point is whether the private sphere of individuals and the security of the individuals and/or community are mutually exclusive values. As summarized by Bellanova:

> The so-called balance metaphor conveys the idea that data protection and security would participate to a zero-sum game, where the reinforcement of the one would imply the weakening of the other. This metaphor has been vividly contested, especially because of its normative implications and its conceptualization of both data protection (more often labeled privacy or liberty) and security as homogeneous and 17 monolithic practices. (Bellanova 2014, 16)

Surveillance and overly controlling security measures prevent people from enjoying the benefits that the city has to offer. Mobility, especially, is a key to success for all groups and classes in cities. While these measures do not necessarily imply physical barriers, the psychological barriers in the awareness of all-encompassing control through the networked police capabilities systems, may be significant. 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 weaknesesses and potential unintended consequences of such systems.

TACTICS' success is, from its very conceptualization,considered to be closely linked with the system's integration with urban community needs, perceptions and values. The operational environment of the project will not only be a physical one but also a social and cultural one. It was above accounted for the view that TACTICS like systems may undermine the local impact and control over local insecurity issues in the urban areas, raising these to national or transnational troubles (section 3.2.1). Another spin on this is that TACTICS like systems may aid the local security personnel in their efforts to strengthen urban resilience in 'their' area. Coaffee (2013) argues that the New York, Madrid and London terror attacks have highlighted the importance of sub-national and localized responses to new security challenges. To some extent, one could argue that TACTICS like systems have the potential to apply a greater extent of all local resources and capabilities, and as such making better advantage of the urban areas as such in the response to security challenges. If the system is governed or applied by relatively localized security personnel, it could involve a greater degree of local impact and control over also 'external' security issues. Defining or not defining the various local resources such as CCTV on private or shop property as TACTICS relevant may imply a certain anticipatory responsibilisation of the population and actors within the particular urban area. Active political or other types of action towards such 'involvement' of non-security personnel may be seen as an emphasis of more civic-centered resilience of the area in question. On the other hand, this policy direction may mean that various private actors are given little choice in embedding "foresight, robustness and adaptability" into various local planning activities (Coaffee 2013 p. 241). Resilience policy has, according to Coaffee changed its direction (at least in the UK) from that of nature and disaster among others to that of the preferences of international terrorists, economic recession and renewed localist interest in urban planning. What this means in the context of this report, is that initiatives to establish or change current instruments, strategies or tactics within urban areas may have various and alternate justifications. This is important to bear in mind when assessing the relation between which values are promoted or attended to, for example in considering the value of local self-determinency and influence to individuals' perception of security, versus for example security personnel's belief in the efficiency of a counter-terrorism tool such as TACTICS.

Notably, still, is the fact that these policy currents run concomitantly. There may be a decentralization of responsibility to include actors on diverse levels and across occupations and private/public spheres. At the same time, the *agenda* of how these processes are to be steered, or further such policies developed, may signify a *centralization* of power (Coaffee 2013, 247).

3.4 Understanding privacy and civil rights in urban areas

The concepts of human rights such as privacy are considered in the legal context in D5.4, also more specifically related to the various applicable resources and capabilities for TACTICS. In this sub-section, the focus is on understanding privacy and civil rights and standards as they play out in the urban areas, emphasising more the values embedded in these, especially related to the characteristics of urban life. A centre of attention is the difficult balancing act of weighing positive 'urban freedom', i.e. the freedom to be left alone from (government) interference, versus security, either of the urban area or community as such or individual, implying e.g. privacy interfering control measures (Berlin 2002).

Privacy is often argued to be an important value both for individual well-being in addition the successful functioning of a democratic society (e.g. Chadwick 2005). It has been argued to be at the very essence of the human personality, and thus the core of constitutional democracies in allowing the participation in these with respect to the dignity of each person (Claes 2006). Especially related to preventive counter-terrorism, the so-called 'chilling effect' following the citizens' general perception of being under covert surveillance may contribute to an unproportionate intrucion in society's well-being (Solove 2008, 178). If the citizens perceive themselves as being watched constantly by public authorities, they may eventually lose trust in the security provision from both private and public parties. Such a growing trust may be damaging for democracy and security perception in general, and thus be counter-productive to what counter-terrorism measures such as the TACTICS system seek to promote. The implementation for example of sufficient safeguards for personal data in the TACTICS processes is therefore crucial.

At the same time, democratic societies thrive better when there is an absence of fear. Through the democratic state set-up, where the citizens entrust some of their autonomy to the governing authorities, the States may also be seen to have an obligation to protect the citizens against external threats (national security) and the general security (Wallerstein 2008). And 'security' may be, in its most basic understanding, be seen as an absence of fear which allows a person to live a full and worthy life, which in turn allows for personal development and democratic participation (Hilst 2013, 98).

It is emphasised that the TACTICS system is designed for rare occasions; terrorist attacks do fortunately not happen very often. While it has been argued that security and freedom are not values that may be successfully balanced towards each other, it is relevant to consider whether the added impact of the TACTICS tools on privacy and data protection rights is necessary. Once the system as such is established, it is highly likely that it will be used. To assess the necessity, the probability of the risk of a terrorist attack should be considered. The following starts with analysing how probability of terrorist attacks may be assessed, and how the precautionary principle has become prominent in the security discourse.

3.4.1 Probability and the precautionary principle

The *preventive* part of TACTICS (for example the Capability Management process, see D5.4) may at least to some extent be built on the so-called 'precautionary principle', i.e. the principle implying that it is better to take some kind of action than *not* and suffer the consequences of a terrorist attack. The precautionary principle is often invoked when "scientific information is insufficient, inconclusive, or uncertain and where there are indications that the possible effects on the environment, or human, animal or plant health may be potentially dangerous and inconsistent with the chosen level of protection" (Communication 2000, 7). Counter-terrorism measures are often based on insufficient and inconclusive information as to the damage caused and the probability of the harm occurring (Hilst 2013, 123). Considering the potential harm caused by such an attack, the precautionary principle may with good reason be applied in 'setting off' TACTICS and the CMT. The legal threshold for this is dealt with above. It needs also in this context to be dealt with the societal consequences a too eager use of the precautionary principle may have.

The precautionary principle presupposes that the counter-terrorism measure may aid in preventing a terrorist attack from happening, and thereby increase the security and/or safety in the society. This presupposition is not necessarily right, as Schneier argues

(Schneier 2008). It is hard, he argues, to establish what the *next* terrorist attack will be like, where, which *modus operandi*, etc., and it is therefore hard to provide efficient measures against the future attacks. There is a significant risk of over-reacting and instating precautionary measures that actually may be unnecessary or implying wrong sacrifices of freedom and privacy. While TACTICS *per se* is a tool to facilitate and improve precisely the decision on when to intervene or not, it is important to acknowledge that facts generated to the TACTICS database or other databases may incur faulty presumptions on the present or anticipated attack. In other words: Although the cross-linked information surfacing from an input in the threat management process may signal clear resemblances to an occurring situation, a trust in automatic assumptions should not be absolute.

Schneier's argument may be seen as supported by research conducted on the probability of terrorist attacks. Many studies show that there is little danger actually posed by terrorism. Other ways of dying are also emphasised in several studies as far more likely to happen than death by terrorism. Wolfendale has summarised that there is "a significantly greater likelihood of being killed by lifhtning strikes, bee stings, or Do It Yourself (DIY) accidents than being killed in a terrorist attack. The number of annual deaths from sport utility vehicles (SUVs) is reported to be greater than the total number of deaths caused by all terrorist acts combined" (Wolfendale 2005, 92). In other words, one may conclude that the risks of dying from a terrorist attack, compared to other ways of dying, are small.

Statistical analyses may provide diverging results, and may also be problematic to use as basis for whether or not counter-terrorism measures such as TACTICS should be introduced or not. For one, terrorist attacks cause far more harm and distress than 'merely' the death tolls suggest. The number of injured will clearly be higher than dead, in addition to substantial economic damage. For another, and connected to the very purpose which defines terrorism, the societal impact concerning fear, anxiety and grief of the population spreads far wider than to merely those being directly affected by the attack (see also Hilst 2013, ch.4.3.3). Another statistical study has concluded that the risk of another major 9/11 type terrorist happening within the next ten years is 50%.[14] The death toll from the 9/11 attacks was six times larger than the next largest attack in a database of terrorist incidents stretching back to 1968. The researchers explain how attacks are likely to cause many more deaths than the previous due to the way numerous building complexes housing tens of thousands of people and sporting events that regularly gather upwards of 50,000 people into an area not much bigger than a football field. The TACTICS research project and design is produced with the specific focus of *urban environments*. Some of the core characteristics of the urban environments are precisely the crowdedness in public and private (i.e. building complexes) places. Since terrorist attacks are hardly random in their targeting, which provides a safe assumption that som locations – typically (certain) urban locations are more prone to a terrorist attack than others.

3.4.2 Core democratic values: participation

It has been argued elsewhere in this report, and in D5.4, that TACTICS may imply that an array of 'ordinary' security resources are redefined into 'counter-terrorism resources' in order for them to be able to 'fit into' the comprehensive TACTICS system. This may be seen as a negative aspect of the system, since this may be part of a move towards an all-seeing surveillance society. On another side, however, one may see the inclusion resources involving ordinary people and business in the strengthening of urban security

[14] A dataset of over 13,000 terrorist events between 1969 and 2007 has been used to calculate the likelihood of an attack with a death toll equivalent or greater than 9/11 (Clauset and Woodard 2013).

and resilience as a *positive* move in the sense of a strengthened democracy. This view implies that the security situation to a greater extent involving the citizens means a greater emphasis of engagement from the citizens; a renewed focus on what Coaffee calls a more “community-driven, social contract between citizens and the state” (2013, 246). This seems to be built on that ‘enlightened’ citizens want to participate more in the general security of their local urban area, and, presumably, this will also lead to the acceptance of other security/counter-terrorism measures. In contrast, thus, if the citizens are made to take a stand *pro* or *con* their involvement as resilient urban actors, they may also actually be more aware of the on-going security policies, and thus more enabled politically to participate in democratic elections on various levels.

In a UK “Local Well-Being” project, the think tank Young Foundation for example argued that “A model of ‘resilience’, both at the community and individual levels, will potentially help decisions in policy making and local resource prioritisation and enable authorities to develop a better adaptive capacity to adverse events“ (Young Foundation 2010, 34). On another note, criticism has been made concerning government policies that are ‘persuasive’ for being paternalistic, in that they attempt to undermine the individuals’ control over their deliberation and thus ability to think and make free choices (concerning so-called ‘nudge’ tactics’: Hausman and Welch 2010, 130; see also Thaler and Sunstein 2008).

Chandler argues that the inclusion of the individuals into developing a resilient frame of mind, as part of a government framework, constitutes a shift in the dominant security discourse that implies a far more pervasive and widespread responsibilisation of the citizens (Chandler 2012 p. 216; also e.g. Ericson and Haggerty 1997). This may be argued to be a sign of decentralised state-withdrawal in security providing, but it may also be argued to be seen as a new disciplinary strategy, a new way for the state to make the urban dwellers participate in self-governing on behalf of the state.

While this is not uncontroversial either way, this may serve to emphasise the importance of the individual’s role in the security of the urban area, whether related to its role as a resilient ‘piece of the puzzle’ or/and as a dis/satisfied inhabitant of the urban area.

3.4.3 Core ‘urban values’

Core values of urban areas consist among others of the freedom to be different and express individuality and opinions, to escape tight social control, and the importance of open, public venues for dissensus. The urban sphere has the potential of fostering participation, creativity, social capital and accountability. Due to security developments, in particularly those in the name of counter-terrorism, Clavell argues, this potential is now meeting a practice of revanchism, exclusion and punitivism (Clavell 2012, 121; also Garland 2001). Urban areas are increasingly becoming spaces for eliminating risks towards homeland security, collapsed with community safety, which may imply a lowered tolerance of diversity – a core value of the cities.

Recasens *et al.* argue that an increasingly worrying phenomenon is the growing number of public disorder related to street demonstrations (2013, 375). The increase may be due to the population’s rejection of neoliberal policies that has led to a widespread financial depression amongs urban populations. Public demonstrations are in principle a sign of a well-functioning popular democracy and an engaged (urban) population. The demonstrations are sometimes violent, turning into riots, but this may mostly concern only few of the participants. In the present context, the central point to focus on is whether TACTICS as a system-of-systems may imply a facilitated ‘misunderstanding’ of such events; an easier way of considering public (rising) unrest as a situation growing out of control and turning into possible moments of terrorism. This could especially apply if

TACTICS type systems were standardised, so that such types of activities implied ‘opening’ or ‘triggering’ thresholds in the system, which, as is explained in Deliverable D5.5, as a point of departure only shall be set in motion in exceptional situations. If TACTICS were to be a common system for several countries or regions, one could argue that it needs to be based on a common notion of what urban security is.

3.5 Illegitimate use

Two aspects are highlighted here related to the use of TACTICS or TACTICS like systems that that may be seen as jeopardising civil and individual rights. One concerns discrimination or biased targeting of individuals or groups; the other

It is a central point of TACTICS to avoid biased decision-making. As in all decision-making systems, biases can not be fully eliminated, but more or less effectively acknowledged, managed and reduced. The morphological analysis, which is an important feature in TACTICS and that promises to reduce the risk of biases, may itself be at risk of being biased. Indeed, decomposable realities are *per se* biased and to some extent discriminatory in that they focus on certain elements instead of others. While TACTICS provides a thorough intake to this topic, it is imperative to emphasise this risk related to the tool.

Möckli has argued that counter-terrorism measures such as mass surveillance may more easily be targeted towards specific groups within society on basis of discriminatory assessments (Moeckli 2008). A key concern of preventive counter-terrorism measures is the intrusion into the private life of large groups of innocent people. TACTICS like system may imply an increased intrusion in the urban areas because of the crowdedness and number of available capabilities such as CCTV, personnel etc.

The current purpose of the TACTICS system is the mitigation of terrorist attacks. As such, it is only the most serious of crimes and people suspected of committing or being about to commit such crimes that trigger TACTICS. As discussed in D5.4 and D6.2, this is an extremely important guarantee in terms of respect of fundamental rights, and it is one of the building blocks of its legitimacy and legality. However, there is nothing in the system itself that in the future will hinder it from being customised for other purposes than counter-terrorism. There are a number of possibilities to limit this risk of function creep. Some are of legal nature: for example, the legislation needed to develop and implement a TACTICS-like system at national level (which is a *conditio sine qua non* of its coming into existence) should provide clear limits to the scope of its use, leaving no room for further ‘exceptional’, or ‘administrative’ use. Other solutions are of technical nature: a TACTICS-like operation system may be designed to hamper continuous use, e.g. avoiding continuous connection to other databases and systems.

Yet, despite specific ad hoc solution, the fundamental challenge with the development of a system of system such as TACTICS: once it as been developed, there is no telling to which uses it will be put. The coupling of capabilities and the general purpose of collecting absolutely all available resources for overview and surveillance in one place carries in it a risk of abuse. One aspect is that the system may be put to use in a greater extent than necessary in the particular police operations. Another is the potential undemocratic use of the systems. Undemocratic use could for example be a heightened level of surveillance by the TACTICS system-of-systems, with the purpose of keeping track of people of certain political or religious affiliations. This may amount to illegitimate discriminatory targeting of certain individuals or groups. Training of the system operators and security personnel, including ethical awareness related to bias and prejudice, will be necessary in the future implementation of the system.

3.6 Conclusion

In this first segment of the report, the characteristics of urban areas and the relationship between these characteristics and civil rights and values have been analysed. TACTICS has here been considered as part of the contemporary trend or strategy of urban resilience, and the *pros* and *cons* of these government tactics and procedures have been discussed. The pertinence of targeting *urban* instead of rural areas was assessed. The report suggests that while terrorist attacks primarily take place in urban areas, and thus that the mitigation of on-going terrorist attacks must happen there, the use of TACTICS and other counter-terrorism measures in a *preventive* mode, should in just as great a degree be targeted at non-urban areas.

In order to understand terrorist threats and how they impact on the urban areas, the report discussed how crime and security may be perceived among individuals, how these perceptions are shaped, and how for example civil and privacy rights are affected by these perceptions.

To understand how privacy and civil rights apply in urban areas, some of the most relevant values implied in these rights were discussed in section 3.4. The balancing of the intrinsic urban values of participation, creativity, social capital and accountability versus security through control measures was analysed. Such balancing may be theoretically difficult, because it implies juxtaposing values that cannot really be compared and over-simplifying the matter of the concepts (Moeckli 2008). It is nevertheless vital for the TACTICS project to include the process and values to be assessed, as done in this report, in order to raise awareness and impress the importance upon the future users of the system. TACTICS constitutes a security measure that may interfere in the individuals’ human and civil rights. It is thus not unlikely that actions based on the use of a TACTICS-like system-of-systems may be tried before national and international courts such as the European Court of Human Rights (ECtHR), especially if their use becomes routinized. And regardless of academic difficulty of balancing security and freedom, these courts *must* strike that balance (Hilst 2013, 11).[15]

[15] See for example the Belgian Linguistic Case (1968).

4 A Surveillance Impact Assessment: Rights issues related to surveillance systems in urban areas

In order to analyze and document the legal and rights related issues that come into play through the eventual implementation of technological systems for monitoring and documenting activities in urban areas, the TACTICS project has participated in a surveillance impact assessment (SIA). The SIA was conducted by another EU FP7 project, SAPIENT (Supporting fundamentAl rights, PrIvacy and Ethics in surveillaNce Technologies, project no. 261698), and used in an anonymized form in their development of methodologies to construct a surveillance related impact assessment framework (SAPIENT D4.2, iii).

The main purpose of a SIA is the analysis of the risks that a surveillance instrument, whatever its nature, may trigger for fundamental rights and ethical values. Indeed, according to the SAPIENT D4.4: "[t]his guide describes a method for identifying, assessing (or evaluating) and prioritising for treatment risks arising from the development and deployment of surveillance technologies, systems and applications".

More in general, SIAs are somehow among the most recent evelotions of policy tools that are developed and implemented to support decision-making processes in different fields. Given their scope, SIAs are similar to Privacy Impact Assessments and Social Impact Assessment.[16] This kind of assessments have been renamed by Raab and Wright to surveillance impact assessment in order to catch *all* of the implications raised by a surveillance project – not only privacy (Raab & Wright 2012). The risk assessment addresses the *likelihood* of a certain event and its *potential consequences*, i.e. impacts. A SIA should include stakeholder consultation and, ultimately, lead to mitigating measures as necessary to avoid, minimise, transfer or share the risks. The SIA should follow a surveillance initiative throughout its life cycle. While privacy and data protection impacts are a major focus of an SIA, surveillance affects a range of other fundamental rights and ethical and social principles that may also be relevant in a particular assessment. The SIA method described in this guide subsumes a privacy impact assessment, i.e., there is nothing in a PIA which is not also included here. In other words, an SIA and a PIA do not need to be conducted as separate exercises. Similarly, the SIA subsumes an ethical impact assessment (EIA). Hence, an SIA includes, but is more encompassing than either a PIA or EIA.

Since few years, PIAs are at the centre of policy attention at European level: a Data Protection Impact Assessment (DPIA, which is how PIA have been recently renamed) is made obligatory in the proposed EU Regulation Art. 33(1), and included in the proposal for the modernisation of Convention 108 in Art.8.[17] However, the draft of the proposed Directive, which is supposed to eventually cover the exchange and processing of data for law enforcenement and state security purposes, does not include provisions on the DPIA. It should be also noted that SIAs are not yet widely used, but they are still largely in a phase of testing and progressive uptake. The SAPIENT SIA methodology is one of the

[16] On Privacy Impact Assessments, cf. Wright & De Hert (2012). On Social Impact Assessments, cf. Esteves et al. (2012).

[17] See more: Hilst (2013, 88).

most developed in this domain, but has not yet adopted by potential users, nor has been made mandatory by European authorities.

In other words, the choice of testing TACTICS through the SAPIENT SIA methodology puts the TACTICS project in line with the most advanced practices of impact assessment for security and surveillance systems. For example, impact assessments focusing on privacy (and data protection) are already used by the United States (US) Department of Homeland Security (DHS). Still, it should be noted that the testing was rather mutual: not only TACTICS was 'assessed', but this experience also contributed to the feasibility test of the SAPIENT SIA methodology.

We believe that a SIA can be used to identify and evaluate the positive and negative impacts of TACTICS-like systems, and the appropriate terrorist attack mitigation measures. In this chapter, we build on the SIA experience, and on the SAPIENT SIA report.[18] We aim to offer an overview of the SIA process applied to TACTICS (e.g. identification of stakeholders, results, etc.) as well as to provide some comments on this experience. We also advance few recommendations concerning the possible use of SIAs for a project like TACTICS.

4.1 The SAPIENT SIA process

The full SAPIENT SIA guidelines imply a step-by-step process through three main phases: (i) the "preparatory phase"; (ii) the "risk identification and analisys phase"; (iii) "risk treatment and recommendations phase" (SAPIENT D4.4, 11). Each phase is divided into several steps, for a total of 20 key steps, ranging from "[d]etermine if an SIA is necessary" to "[i]dentify risk criteria" and "[p]repare an SIA report" (SAPIENT D4.4, 10-11).

As the full process could be too burdensome for many potential SIA users, the SAPIENT project has also developed guidelines for a "small-scale surveillance impact assessment" (cf. SAPIENT D4.4, Part II). In the case of the TACTICS project, the two consortia decided to opt for this small-scale process. The small-scale SIA covers the same phases of the extended version, but it reduces the key steps to six:

1. Project description;
2. Identifying stakeholders;
3. Responding to a questionnaire;
4. Design of a risk map;
5. Identification of solutions;
6. Preparation of the SIA report.

The process took place between April and June 2014. It involved members of both the SAPIENT and TACTICS projects, which met in person and through teleconference. From the TACTICS side, the involved partners were: PRIO, ITTI, LERO and TNO. As already mentioned, a full report was produced at the end of the process by the SAPIENT team, based on the data collected through the meetings. This final report was made available to

[18] The SAPIENT SIA report on the TACTICS project is part of SAPIENT Deliverable D4.2. This deliverable is not publicly available.

the TACTICS project. Some TACTICS partners provided feedback on this experience, and we use also this material in the drafting of the TACTICS comments below.

From start, the idea of testing both the TACTICS project through a SIA, and the SIA guidelines through the TACTICS case, was considered a valuable, but challenging experiment for both projects. Indeed, the experience contributed, together with other case studies, to the fine-tuning of the SAPIENT SIA guidelines. As for the TACTICS project, it should be already said that the SIA was probably less interesting for its results than for the very experience.

The SIA proved pretty effective in identifying potential risks and proposing relevant solutions (we briefly discuss them in the section 4.2 below). However, many of them were not different from the more theoretical analysis that had been already carried out within the TACTICS project itself. Yet, the SIA process itself invites to a different approach towards the identification of risks and solutions. In other words, even when it raises questions concerning its very feasibility or its underlying rationale (e.g. when it comes to 'quantifying' and 'prioritizing' risks), a SIA process may permit to engage *differently* with the project at stake.

For example, the SIA process signalled the need to devote further attention, if the TACTICS project is to be developed into functioning TACTICS-like systems, on the notion of *relevant stakeholder*. As mentioned above, the identification of the relevant stakeholders is a key step of the SAPIENT SIA process (and of many other impact assessment exercises). In the case of TACTICS project, the *internal* stakeholders are identified as the research project partners and the end users. Yet, these stakeholders would be pretty different if a TACTICS-like system were to be developed and deployed. Then, the list of internal stakeholders may be very different. While it would surely include the specific law enforcement agencies legally empowered to use a TACTICS-like system, the inclusion of other key actors would not be so self-evident. For instance, what about judicial authorities that may be responsible of warranting the authorization for the use of the system? And what about entities that manage capabilities that may, at least in theory, be connected to, or through, the TACTICS-like system (e.g. private owners of urban facilities like stadiums or conference centres, generally equipped with CCTV operated for non-counter terrorism purposes)?

Furthermore, identifying precise *individuals* or *groups* that should be considered relevant *external stakeholders* is already challenging at this stage. No external stakeholder has been involved in assessing the project, since no system has been run in real life situations. Adding external stakeholders to the SIA process would have been arbitrary at this point. However, this does not mean that, if a TACTICS-like system were to be fully developed and implemented by national authorities, there would be external stakeholders. On the contrary, a TACTICS-like system would engange with several different groups, besides national authorities. However, it is difficult to predict in advance of the deployment of TACTICS which individuals or groups will be more relevant. Surely, people living in urban areas, or visiting for any kind of reasons, may become concerned by such a surveillance system the moment it is activated. Still, if such a system were to be used under strict limitations and safeguards, it would remain difficult to identify specific groups of stakeholders (beyond very generic categories). No need to say, that it would be very difficult to create a one-fits-all rule to identify the most legitimate representatives of these external stakeholders. Our recommendation (based on exchanges within the consortium) is that local practices of urban governance could provide practical guidelines. For example, if majors or city council are already involved in the management of public order, it is reasonable to consider them relevant stakeholders. But, what of religious communities or political parties, or of groups that lack a recognized representative structure?

Again, undergoing the SIA process did not provide all the answers, but permitted to formulate better some important questions that had already been raised. Another example concerns the very first step of the small-scale SIA process: the description of the project.

As noted above, the ambition of a SIA is to be flexible enough to assess different kinds of surveillance related initiatives. This means that, for example, both a proposed policy tool and a research project can be assessed by a SIA. However, the case of TACTICS underlines that this ambition could be difficult to translate on the field. As discussed in chapter 2 above, the description of what TACTICS is, risks triggering ambiguities. In fact, while TACTICS is first and foremost a research project, it is also the 'working' name of both the concrete results of the TACTICS project and of the hypothetical class of operational systems that could be created on the basis of these results (or that resembles these systems). This distinction is also presented in TACTICS D3.1 and D3.2.

The partial indistinctness and overlap between *projects* and *systems* are quite typical in many similar initiatives, also beyond EU funded research. The underlying rationale of a SIA process is that a project already deserves to be assessed because its eventual development (if any) would probably have fundamental rights implications. In other words, a SIA is conducted on a project not primarly to check its 'deontology', but because the project is perceived as already having societal effects.

During the SIA process we attempted to keep the two separate, but this proved to be quite challenging on both projects' sides. It may prove even harder to keep separate the two kinds of systems that may develop: the specific product of the TACTICS project and similar systems to be more or less 'inspired' by the project's results. Surely, the best solution, from a SIA perspective, is to assess the impact of any future system. From this perspective, this first SIA has nevertheless highlighted the need to tune the next SIA processes on the possible offsprings of the TACTICS project. From a TACTICS point of view, this difficulty signalled the need to further clarify what is at stake with the TACTICS project, and which kinds of results are to be really expected. It invites TACTICS as a project to be more reflexive on what is, and can be, achieved through research.

4.2 The main risks related to the TACTICS system

In cooperation with the SAPIENT project, a number of risks were mapped related to TACTICS. The risks are divided between those concerning TACTICS as a *research project* and as a *functioning system*. When these differ, this is clearly specified in the assessment. The reason for dividing the system (or rather system-of-systems) and the research project, was to make explicit, as much as possible, that what was mainly at stake in the SIA is the design of the TACTICS-like system rather than the TACTICS FP7 project itself.

Several of the risks identified through the SIA process had been already highlighted in the work already done within the TACTICS project (cf. TACTICS D2.1). To a large extent, they are not dissimilar to the risks posed by other systems and systems of systems: necessity of the system in itself, security and quality of the data, the nature and relevance of data subjects' consent, possibility to access data, conditions of the data retention, interference with the freedom of assembly, etc.

All in all, the risk map designed through the SIA process offers guidance not only for the further development of any kind of TACTICS system, from the direct results of the project to the possible implementation of an operational system. It also provides important elements of reflection for the authorities that may be interested in adopting this kind of system(s).

Still, the risk map also highlighted few potential risks as the most pressing for both TACTICS as a project and TACTICS-like systems (table below adapted from SAPIENT D4.4, 12).[19]

Top three concerns of TACTICS	
TACTICS-like system(s)	TACTICS as a research project
The system makes use of unreliable data (quality of data cannot be controlled)	Lack of transparency
Having no time limits on the use of TACTICS (The TACTICS system affecting trust relations because of over-use)[20]	Not having the Ethical, Legal, and Social Impacts (ELSI) partners involved in the validation
Revealing internal secret of organisations	Data being shared outside the EU

For what concerns the three main risks for TACTICS as a research project, it should be noted that the third risk: “data being shared outside the EU” has been double checked after the completion of the risk map step, and resulted in a non-relevant issue. All partners involved in the TACTICS project belong to EU member states or to countries that have been formally recognised by the European Commission as offering an adequate level of data protection.

“Lack of transparency” and the non-participation of ELSI partners in the validation step of the TACTICS project are due to ‘structural’ issues. On the one side, the classification level of many TACTICS deliverables is due to internal rules in the management of EU funded projects in the security domain. On the other side, the non-involvement of the main ELSI partner in the validation workpackage is due to the Description of Work of the TACTICS project. The TACTICS consortium is addressing both risks: the main ELSI partner (PRIO) has been further integrated into the validation and the very decision of carrying out a SIA was part of on-going efforts to keep the TACTICS project transparent.

As for the three main risks related to the TACTICS-like systems, they can only marginally addressed by the TACTICS consortium. In fact, none of them really apply to the eventual results of the TACTICS project (the TACTICS as a validation system). According to both the Description of Work and the current status of the project, the TACTICS system as result of the project would make use only of ‘fictional data’, created to validate the system. Therefore, the question of the quality of the data would not be posed directly, nor the issue of the time limits and the revelation of “internal secrets of [external] organizations”. However, while the TACTICS results won’t directly incur in these risks, the challenge is to ensure that these risks would be reduced if a TACTICS-like system were to become operational. So far, it is too early to assess to which degree the TACTICS results will

[19] SAPIENT D4.2, 10-11.

[20] At closer inspection, some of the identified risks are sort of overlapping. For example, one of the risks was termed ‘having no time limits on the use of TACTICS’, another was termed ‘The TACTICS system affecting trust relations because of over-use’. It can be argued that the risk of having no time limits on the use of TACTICS is exactly a risk *because* it might affect trust relations. These risks could be dealt with jointly.

provide effective solutions in their own design, or how successful these solutions can prove in real-life use (assuming that they are kept in any further development).

In any case, the risk map, including the three main concerns about the TACTICS-like systems, should be considered as a starting point for any further evolution. No need to repeat that any TACTICS-like system would profit from running a SIA process anew. Given that the SAPIENT SIA guidelines have now been tested, it is recommendable to follow the full-scale process, and to run again the process after the first use of a TACTICS-like system.

4.3 Assessment of the SIA experience and recommendations

The decision to test the SAPIENT SIA process should be welcomed. Besides fostering collaboration between EU funded projects, it proved a particularly useful exercise for both consortia. While a SIA 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. More importantly, our experience is that the SIA process invites the team working on a surveillance related project to consider classical ELSI question from a slightly different perspective. In particular, the very interactions with people that do not participate to the project obliges the partners to clarify important aspects that, in the routine of research, often become too implicit and thus not properly explored. Therefore, more than the results, it is the process that should be praised.

The SIA for the TACTICS project was when the project was already advanced (the SIA guidelines were not available earlier). This was probably already too late to take full advantage of the process. Furthermore, given the experimental status of the initiative, it was not possible to actively involve all the key stakeholders. Yet, we believe that any future SIA should be carried on with the participation not only of ELSI partners and coordinators, but also with the full consortium.

From this experience, we can formulate the following recommendations:

- the results of the SIA should be the explicit object of a structured, and potentially regularly held, discussion among TACTICS partners;
- a strategy for the preventive reduction of the risks identified in the risk-map should be developed and possibly integrated into the report on Implications and Recommendations – Deliverable D8.2;
- a clear conceptualization of the difference between TACTICS as a research project, TACTICS as a validation system, and TACTICS-like systems should be drafted and possibly published on the TACTICS website;
- if a TACTICS-like project is to be developed, the running of a new SIA should be a priority. This SIA should take stock of the SIA already done, but should be tailored on the system at stake;
- any new SIA should be run as early as possible, and involve a wide participation from stakeholders, at least internal stakeholders if the identification of external stakeholders proves too difficult;
- SIA guidelines concerning the identification of external stakeholders are both challenging and problematic, especially when it comes to projects that have not been tested in real life situations. Further reflection is needed on how to ensure a meaningful participation of external subjects and groups that may be concerned by a research project.

5 List of acronyms

ELSI	Ethical, Legal, and Social Impacts
TDT	Threat Decomposition Tool
TMT	Threat Management Tool
CMT	Capability Management Tool
GTD	Global Terrorism Database
MO	Modus Operandi
TM	Threat Manager
TDM	Threat Decomposition Manager
SIA	Surveillance Impact Assessment
SAPIENT	Supporting fundamental rights, PrIvacy and Ethics in surveillance Technologies (FP7 project)
TACTICS	Tactical Approach to Counter Terrorists in Cities (FP7 project)

Bibliography

Beck, U (2002): “The terrorist threat: World risk society revisited”. *Theory, Culture and Society*, vol. 19 no. 4, 39-55.

Beck, U (1992): *Risk society: Towards a new modernity*. London: Sage.

Bellanova, R (2014): *The Politics of Data Protection: What Does Data Protection Do?* Université Saint-Louis – Bruxelles & Vrije Universiteit Brussel.

Bennett, C J (2008): *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge: MIT Press.

Bennett, C J (2011): "In Defence of Privacy: The Concept and the Regime." *Surveillance & Society,* vol. 8 no. 4, 485-96.

Berlin, I (2002): *Liberty: Incorporating four essays on liberty*. Oxford: Oxford University Press.

Bigo, D (2000): "When two become one: International and external securitisations in Europe". Morten Kelstrup and Michael Williams (eds): *International relations theory and the politics of European integration: Power, security and community*. London: Routledge.

Buzan, B (1991): *People, states and fear: An agenda for international security studies in the post□cold war era.* New York: Harvester Wheatsheaf.

Buzan, B and Wæver, O (2003): *Regions and powers: The structure of international security.*Cambridge: Cambridge University Press.

Chadwick, P (2005):”The Value of Privacy”, *European Human Rights Law Review*, 5.

Chandler, D (2012): “Resilience and human security: the post-interventionist paradigm”. *Security Dialogue*, vol. 43 no. 3, 213-229.

Claes, E (2006): “Restoritative Justice and the Right to Privacy” in Claes, E., R.A. Duff and S. Gutwirth: *Privacy and the Criminal Law.* Antwerp: Intersentia

Clauset, A & Woodard, R (2013): “Estimating the historical and future probabilities of large terrorist events”, *Ann. Appl. Stat*., vol. 7, no. 4, pp.1838-1865

Clavell, G G (2012): “Urbanscapes of injustice and insecurity”. Ugelvik, S and Hudson, B: *Justice and Security in the 21st Century: Rights, Risks and the Rule of Law.* London: Routledge.

Coaffee, J (2013): “Rescaling and Responsbilising the Politics of Urban Resilience: From National Security to Local Place-Making”, *Politics*, vol. 33 no. 4, 240-252.

Coaffee, J (2000): “Fortification, Fragmentation and the Threat of Terrorism in the City of London”. Goold, JR and Revill, GE (eds.): *Landscapes of Defence*. London: Addison Wesley Longman.

Comfort, L K (1999): *Shared risk: Complex systems in seismic response*. Oxford: Elsevier.

Coward, M (2006): “Against Anthropocentrism: The Destruction of the Built Environment as a Distinct Form of Political Violence”, *Review of International Studies*, 32, 419-437.

Ericson, R & Haggerty, K (1997): *Policing the Risk Society.* Oxford: Clarendon.

Esteves, A M, Franks, D & Vanclay, F (2012): "Social Impact Assessment: The State of the Art." *Impact Assessment and Project* Appraisal, vol. 30 no. 1, 34-42.

Findlay, M (1999): *The Globalization of Crime.* Cambridge: Cambridge University Press.

Garland, D (2001): *The Culture of Control: Crime and Social Order in Contemporary Society*. Chicago: Chicago University Press.

Godschalk, D (2003): “Urban Hazard Mitigation: Creating Resilient Cities”, *Natural Hazards Review*, vol. 4 no. 3, 136-143.

Goold, B. (2009). Technologies of surveillance and the erosion of institutional trust. In: Technologies of inSecurity. K. F. Aas, H. O. Gundhus and H. M. Lomell. (ed.) Abingdon, Routledge-Cavendish.

Graham, S (2001): “In a Moment: On Glocal Mobilities and the Terrorized City”, *City,* vol. 5 no. 3, 411-15.

Hausman, D and Welch, B (2010): “Debate: To Nudge or Not to Nudge,” *Journal of Political Philosophy*, vol. 18 no. 1,123-36.

Hilst, R (2013): *Putting Privacy to the Test: How Counter-Terrorism Technology is Challenging Article 8 of the European Convention on Human Rights*, University of Oslo.

Huysmans, J (2006): *The politics of insecurity: Fear, migration, and asylum in the EU*. London: Routledge.

Lyon, D (2007): *Surveillance Studies. An Overview*. Cambridge: Polity.

Mawby, R I and L Simmonds (2004): “Feelings of Security in the City: Anxiety over Crime as Spatially Defined”, *Security Journal*, vol. 17, 73–85.

Moeckli, D (2008): *Human Rights and Non-Discrimination in the ‘War on Terror’.* Oxford: Oxford University Press.

Neocleous, M (2007): "Security, Liberty and the Myth of Balance: Towards a Critique of Security Politics." *Contemporary Political Theory*, vol. 6 no. 2, 131-49.

O'Brien, G & Read, P (2005) "Future UK emergency management: new wine, old skin?", *Disaster Prevention and Management: An International Journal*, vol. 14 no. 3, 353 – 361.

Raab, C & Wright, D (2012): "Surveillance: Extending the Limits of Privacy Impact Assessment." In *Privacy Impact Assessment*, edited by David Wright and Paul De Hert, 363-83. Dordrecht: Springer.

Recasens, A, Cardoso, C, Castro, J and Nobili, GG (2013): **“**Urban Security in Southern Europe”. *European Journal of Criminology*, vol. 10 no. 3, 368-382.

Schneier, B (2008): “The Psychology of Security”. *Africacrypt,* LNCS 5023, 50–79.

Solove, D (2008): *Understanding Privacy*. Cambridge: Harvard University Press.

Thaler, R and Sunstein, C (2008): *Nudge: Improving decision about health, wealth and happiness.* New Have, CT: Yale University Press.

Ugelvik, S (2014): *Inside on the Outside: Norway and Police Cooperation in the EU*, University of Oslo.

Vanderschueren, F (2013): “The Evolution and Challenges of Security in within Cities”, *UN Chronicle*, vol. L no. 2, 2013.

Wallerstein, S (2008): “The State’s Duty of Self-Defence”. Goold, B and Lazarus, L (eds): *Security and Human Rights.* Oxford: Hart.

Wolfendale, J (2005): *Writing the War on Terror: Language, Politics and Counter-terrorism*. Manchester: Manchester University Press.

Wright, D & De Hert, P (eds.) (2012): *Privacy Impact Assessment*. Dordrecht: Springer.

The Young Foundation (2010): *The State of Happiness: Can Public Policy Shape People's Wellbeing and Resilience?* London: The Young Foundation (http://www.happymuseumproject.org/wp-content/uploads/2013/02/YF-wellbeing_happiness_Final__2_.pdf [28.01.15])

Zedner, L (2005): "Securing Liberty in the Face of Terror: Reflections from Criminal Justice." *Journal of Law and Society*, vol. 32 no. 4, 507-33.

Documents, reports, cases

D2.1 TACTICS: Factors Overview

D3.1 TACTICS: Conceptual Solution Description (White Paper), publicly available online at: http://www.fp7-tactics.eu/files/documents/D3.1_Conceptual%20Solution%20Description.pdf

D3.2 TACTICS: System Architecture, publicly available online at: http://www.fp7-tactics.eu/files/documents/D3.2_System%20Architecture.pdf

D5.4 TACTICS: Privacy, Ethics, and Human Rights Report, to be released publicly at: http://www.fp7-tactics.eu/news.html

D6.2 TACTICS: Ethical Overview, to be released publicly at: http://www.fp7-tactics.eu/news.html

European Commission (2000): Communication from the Commisssion on the precautionary principle, Brussels: European Commission.

HM Government UK (2010): *Working together to protect crowded places*. London:TSO (http://www.continuityforum.org/sites/default/files/images/working-together-crowded-places.pdf [28.01.15]

HM Government UK (2012): *Crowed places: The Planning System and Counterterrorism*. London: TSO

(https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/375208/Crowded_Places-Planning_System-Jan_2012.pdf [28.01.15])

ECtHR Case "Relating to certain aspects of the laws on the use of languages in education in Belgium" c. Belgium, Application no 1474/62; 1677/62; 1691/62; 1769/63; 1994/63; 2126/64

SAPIENT D4.2: Surveillance Impact Assessment Report #2

SAPIENT D4.4: A guide to surveillance impact assessment — How to identify and prioritise risks arising from surveillance systems, publicly available at: http://www.sapientproject.eu/D4.4%20-%20SIA%20Manual%20%28submitted%2001%20August%202014%29.pdf