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

TACTICS

Tactical Approach to Counter Terrorists in Cities

Deliverable details	
Deliverable number	5.4
Title	Privacy, Ethics and Human Rights report
Author(s)	PRIO
Due date	30/11/2014
Delivered date	26/01/2015
Dissemination level	PU
Contact person EC	Mr. Ngandu Mupangilai

Cooperative Partners	
	ITTI Sp. z o.o.

Table of Contents

Executive Summary

Making use of several kinds of information about a person induces several issues regarding privacy, ethics, human rights, legal conditions. This report accounts for the international privacy and data protection regulations most relevant for TACTICS, in particular related to the capability management tool and process. The report explains the characteristics of and the most relevant challenges associated with the capabilities, with the purpose of creating a specific tool that may accompany the CMT when suggesting capabilities to the threat manager (TM). The tool itself is not developed in this stage of the TACTICS system-of-systems. In this report, however, the future tool function is implemented in terms of suggestions of the pop-up function of legal, privacy and ethical issues that must be taken into account when applying the system.

The report focuses on *international* legal instruments, since the future implementation of TACTICS require specific adjusting to the national framework respectively. A definition of 'terrorism' as such is, however, suggested, for the future implementation research project to have a common baseline.

Some legal thresholds and requirements are applicable to all TACTICS capabilities, and these are accounted for along with the general data protection principles that must be adhered to. The permissible limitations test is explained and suggested as a standard accompagnement to the potentially privacy intrusive capabilities.

After the more general principles and requirements have been targeted in section 4, essentials related to specific capabilities are accounted for, and the most significant challenges that the CM must consider are emphasised. Particular focus is given to instruments/tools/measures that deal with visual data collection and analysis, such as intelligent cameras and UAVs; to database or web analysis tools or measures such as the Schengen Information System (SIS) as a prominent example of both national and international police databases; and on invasiveness and instrusiveness following assemblage of information, *inter alia* focusing of the challenges related to combing of measures and interoperability of databases. When TACTICS later will be developed into a full-fledged tool, these descriptions form a good basis for the extensive level of detail in legal threshold 'pop-ups' that will be automatic in the CMT.

Section 6 of the report discusses the main ethical issues of the TACTICS CMT. It is easy in a terrorist attack mitigating situation to consider the risks as overriding any concern related to privacy or other civil rights. Emphasis is in this section put on the ethical awareness that needs to be present in the general use of the CMT. This is discussed in the light of the broader picture of security policies in a societal perspective. Special focus is put on the potential expansion of the system, including the future enclosure of all present 'ordinary' security resources into counter-terrorist assets.

In the Conclusions of section 7, the report sums up the legal and ethical guidelines that should be basis for the use of the TACTICS system in general.

1 Introduction to the TACTICS system

TACTICS is a 36 month research project funded by the European Union under the EU 7th Framework Programme FP7-SECURITY.[1] 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 (*D3.1* TACTICS (2013), p. 2):

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 D4.3 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.

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,[2] 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. Hence, it will not be used in any concrete threat situations, nor will be automatically adopted by any European 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 these reasons, while the prospective TACTICS-like systems are out of the scope of this report, the report includes considerations that decision-makers may want to consider when discussing the adoption of similar systems.

.

2 Introduction to the report

This report (D5.4) provides a report describing the main challenges of the TACTICS Capability Management Tool (CMT), in particular from a privacy, ethics and human rights perspective.

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

[2] For a more detailed overview of the prospective TACTICS (2013): "Decision Support System, *D3.2*

The purpose of the TACTICS CMT is to improve the knowledge on the available capabilities at security forces' disposal when alerted of a terrorist threat. In this report, the privacy, ethical, democratic and legal aspects related to the available capabilities will be considered in relation to the CMT. The privacy aspects related to CMT as such are also analysed.

The suggested functionality of this the CMT is that the pertinent aspects automatically will be advised when the system suggests a capability. This facilitates the users´ attention to the legal and ethical aspects of the capability, and thus also ensures that the TACTICS system has some extent of Privacy by design (PbD) implemented in its functionality, as described in D3.1. In other words, the CMT also assists the threat manager in considering the legal and ethical aspects of the applicable capability alternative. The Capability Management Process and the functional requirements are described in detail in D5.2, D5.3 and D5.5. It follows that the purpose of the capability management is to improve the knowledge of the capabilities at security forces' disposal. Through the capability management process, knowledge is improved by increasing awareness about capabilities most appropriate in a given situation, information about how to access capabilities and their general availability. The CMT also provides a matching function through a management concept for capabilities. This concept matches indicators of a potential threat to available capabilities, i.e. detecting certain behaviour to resources such as security staff or camera surveillance.[3] The combination of overview and knowledge about available capabilities and the matching function is intended to establish an improved detection of circumstances and reduction of biases.

For this purpose to be achieved, it is vital that the CMT and TACTICS-like systems in general operate within the legal limits granted to the responsible public law enforcement agencies. The most prominent legal limits for such systems are those of privacy and or respect for private life, data-protection and non-discrimination. Other legal requirements are presumed regulated in internal national law, and fall outside of the TACTICS research project scope. Such issues must be targeted in connection with the eventual national implementation of TACTICS. Overview and knowledge about the capabilities and resources is incomplete without the connected legal and ethical considerations. The purpose of this report is to contribute with the most relevant legal, i.e. privacy and data protection, challenges to the capabilities and capability matching and assembling in the CMT and by the CM.

The most relevant regulations on the *European* level are the provisions in the European Convention of Human Rights (ECHR) and the EU Charter of Fundamental Rights (CFREU). ECHR Art. 8 obliges the States to ensure respect for individual's privacy, a right that is also enshrined in the CFREU Art. 7. A patchwork of legal instruments govern data protection regulations, prominently the CFREU Art. 8 and the 1995 Data Protection Directive. On the global level, the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) protect privacy rights. The later national regulation of TACTICS will generally have to respect these international provisions. These regulations will be accounted for below.

The capabilities the TACTICS system makes use of are all to some extent invasive in manners raising certain privacy or ethical challenges. The core and the novelty of the system, however, is not that it establishes new forms of capabilities or tools in itself, but that it *assembles* the available capabilities and resources from different sources. The privacy, data protection and ethical analysis in this report is therefore aimed primarily at the TACTICS system as such, not at the underlying capabilities in the shapes of intelligent cameras or police databases, etc. If the TACTICS system is to be implemented in the EU member states, there will in addition to the EU regulations be a set of national laws and directives to implement for the TACTICS system to be lawful and legitimate, both in terms of privacy, ethical, democratic and legal aspects. It is not the aim in this report to assess all the different State's applicable rules for the possible implementation of the possible outcome of TACTICS.

Following this section 2 of introduction and section 3 of definitions of the most relevant concepts, section 4 analyses the most pertinent *general* privacy and data protection aspects or 'challenges' concerning the CMT. The specific 'solutions' or requirements that must be implemented in TACTICS systems are targeted in D6.2. An introduction to the capabilities that may be employed is given in section 5 below. As for the general requirements, some legal and ethical issues must be implemented in the system as such. Examples are regulations of differentiated and restricted levels of access, which should be embedded in the systems structure as such to ensure sufficient data security. The specific requirements are analysed in sections 4.3 and 4.4.

Human rights and privacy issues are primarily legal conditions. There are, however, also ethical aspects that must be considered related to various more or less invasive capability measures. The relevant analysis follows in section 6. This analysis also includes the assessment of bias in the CMT.

[3] See more detailed on the process in D5.2.

This report has no ambition to provide an exhaustive analasys of all ethical, legal and socio-political aspects potentially linked to TACTICS. It builds on the activies of the work-package (WP) 5, “Capabilities Management”, but must be seen in connection with key aspects concerning privacy, ethics, human rights, legal conditions of TACTICS as a system and the TACTICS project which are presented and discussed in two parallel deliverables: D4.3 – Privacy, ethics, human rights, legal conditions; and D6.2 – Privacy, Ethics, Human Rights.

Furthermore, it should be noted that these reports should not be considered as an ethical and/or legal validation of the TACTICS system, but a sort of ‘companion’ to the work carried on within the TACTICS project. As such, they aim at highlighting challenges and formulating possible solutions and recommendations. 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 implemantion 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.

3 Definitions

3.1 Of the most central concepts

A few of the most central concepts are defined here. The other relevant definitions are given throughout the report where necessary. 'Terrorism' is defined at greater depth in section 3.2.

Capability: The ability an organization, person or system possess, providing a combination of one or more resources. Capabilities are typically expressed in general and high-level terms and typically require a combination of organization, people, processes and techonology to achieve. Capabilities must contain the required attributes with appropriate measures of effectiveness, and capability definitions must be general and not inluentioal in deciding in favour of particular means of implementation. The definition should just be specific enough to evaluate the alternatives to the capability. (See more in D5.2 p.5.)

Resource: A physical asset, organizational or physical entity that may contribute to towards fulfilling a capabtility (D5.2 p.5). A resource may be *human*, such as a police officer, security personnel, or *technical*, such as camera systems or other types of sensors, and finally the urban environment itself, such as an open square and the physical features within it.

Privacy: See below in ch.4.1.

Ethical: The field of ethics has by Gert (2002) been defined as the systematic reflection of existential questions relating to the 'good life', moral obligations and 'just' society. There are various sub-disciplines of the field, but the relevant for TACTICS is the *normative* ethics, prescribing for example what is right and wrong, good and bad or just and unjust in specific cases. The ethical considerations and alternatives are returned to below in section 6. See also D4.3.

Personal data: Any kind of information (a single piece of information or a set of information) that may personally identify a person or single him or her out as an individual, such as name, address, photograph, credit card numbers, or an IP address. Also information that may be used to 'single out' a person from other people, without providing other identification, is considered personal data (European Digital Rights papers (EDRi) 2013)

3.2 Of terrorism

The TACTICS system in general and thus also the CMT in particular is designed to prevent and stop terrorist attacks. It is necessary for the tools and processes to have implemented an at least point of departure definition of what terrorism is, and what constitutes a terrorist attack. In the TACTICS system, and thereunder the capability management process/tool, it is vital in order to assess whether the capability in question is necessary and proportional (2/3 of the permissible limitations test, see more below) that it is assessed *against* something. This something is the terrorist attack (that has happened or is deemed to happen), constituting a threat to national security. To assess whether a terrorist attack is about to happen or is happening, terrorism needs defining. The key characteristics are necessary in order to determine to what extent terrorism is detrimental to security, and whether the activity in question is a threat to national security. The particular *acts* comprising the activity will normally be regulated in national criminal laws, such as (planning or conspiring to) murder, arson, etc. Some international treaties exist defining acts of terrorism that will be criminalized in the States' national law. Acts of hijacking of civilian aircraft and ships, hostage-taking, terrorist bombings and threats of nuclear terrorism from non-state actors are all dealt with in international treaties.[4] Contrasting to ordinary criminal law, the terrorism 'stamp' justifies extraordinary measures; here, a

[4] Convention on the Offences and Certain Other Acts Committed on board Aircrafts (1963); Convention for the Suppression of Unlawful Seizure of Aircraft (1970); Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971); Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, Including Diplomatic Agents (1973); International Convention Against the Taking of Hostages (1979); Protocol for the Suppression of Unlawful Acts of Violence at Airports Severing International Civil Aviation (1988); Supplementary to the Convention for the Suppression of Unlwaful Acts against the Safety of Civil Aviation; Convention for the Suppression of Unlawful Acts against Safety of Fixed Platforms Located on the Continental Shelf (1988); Convention on the Marking of Plastic Explosives for the

'deeper' interference into the general privacy of a person.This report does not set out to analyse the full scope of terrorism definition[5], and there is no universally agreed upon definition of 'terrorism'. An array of international, regional and national regulations exists of the contents of the term. It is, however, necessary here to supply a definition of terrorist activities in contrast to other criminal activities. A commonly acknowledged academic consensus has been formulated by Schmid in *The Routledge Handbook of terrorism Research* (Schmid 2011), consisting of 12 elements:

"1. *Terrorism refers, on the one hand, to a doctrine about the presumed effectiveness of a special form or tactic of fear-generating, coercive political violence and, on the other hand, to a conspiratorial practice of calculated, demonstrative, direct violent action without legal or moral restraints, targeting mainly civilians and non-combatants, performed for its propagandistic and psychological effects on various audiences and conflict parties;*

2. Terrorism as a tactic is employed in *three main contexts*: (i) illegal state repression, (ii) propagandistic agitation by non-state actors in times of peace or outside zones of conflict and (iii) as an illicit tactic of irregular warfare employed by state- and non-state actors;

3. The physical *violence* or threat thereof employed by terrorist actors involves single-phase acts of lethal violence (such as bombings and armed assaults), dual- phased life-threatening incidents (like kidnapping, hijacking and other forms of hostage-taking for coercive bargaining) as well as multi-phased sequences of actions (such as in 'disappearances' involving kidnapping, secret detention, torture and murder).

4. The public (-ized) terrorist victimization initiates *threat-based communication processes* whereby, on the one hand, conditional demands are made to individuals, groups, governments, societies or sections thereof, and, on the other hand, the support of specific constituencies (based on ties of ethnicity, religion, political affiliation and the like) is sought by the terrorist perpetrators;

5. At the origin of terrorism stands *terror* – instilled fear, dread, panic or mere anxiety - spread among those identifying, or sharing similarities, with the direct victims, generated by some of the modalities of the terrorist act – its shocking brutality, lack of discrimination, dramatic or symbolic quality and disregard of the rules of warfare and the rules of punishment;

6. The main direct *victims* of terrorist attacks are in general not any armed forces but are *usually civilians, non-combatants or other innocent and defenceless persons* who bear no direct responsibility for the conflict that gave rise to acts of terrorism;

7. The *direct victims are not the ultimate target* (as in a classical assassination where victim and target coincide) but serve as message generators, more or less unwittingly helped by the news values of the mass media, to reach various audiences and conflict parties that identify either with the victims' plight or the terrorists' professed cause;

8. Sources of terrorist violence can be individual *perpetrators*, small groups, diffuse transnational networks as well as state actors or state-sponsored clandestine agents (such as death squads and hit teams);

9. While showing similarities with methods employed by organized crimeas well as those found in war crimes,terrorist violence is *predominantly political* – usually in its motivation but nearly always in its societal repercussions;

10. The immediate *intent* of acts of terrorism is to terrorize, intimidate, antagonize, disorientate, destabilize, coerce, compel, demoralize or provoke a target population or conflict party in the hope of achieving from the resulting insecurity a favourable power outcome, e.g. obtaining publicity, extorting ransom money, submission to terrorist demands and/or mobilizing or immobilizing sectors of the public;

11. The *motivations* to engage in terrorism cover a broad range, including redress for alleged grievances, personal or vicarious revenge, collective punishment, revolution, national liberation and the promotion of diverse ideological, political, social, national or religious causes and objectives;

Purpose of Identification (1991); International Convention for the Suppression of Terrorist Bombings (1997); International Convention for the Suppression of the Financing of Terrorism (1999); International Convention for the Suppression of Acts of Nuclear Terrorism (2005); Amendment to the Convention on the Physical Protection of Nuclear Material (2005); Protocol of 2005 to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigations; Protocol of 2005 to the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf of 1988.

[5] See in depth O'Neill,2012, and for example the FP6 funded research project "Transnational Terrorism, Security, and the Rule of Law" Deliverable 4 in WP 3 which discusses the concept in depth (http://www.transnationalterrorism.eu//tekst/publications/WP3%20Del%204.pdf [18.11.14]).

12: Acts of terrorism rarely stand alone but form part of a *campaign* of violence which alone can, due to the serial character of acts of violence and threats of more to come, create a pervasive climate of fear that enables the terrorists to manipulate the political process."

This comprehensive definition is in concord with the academic literature, where the clear common denominator is the intention of creating fear in a population, and impacting on the population's enjoyment of basic human rights (Hilst. 2013 p.106; Hoffman 2008; also the UN High Commissioner for Human Rights, Fact Sheet no.32). Controversy remains concerning the questions of whether a State also may be a terrorist actor, and how (some level of) legitimate national liberation movements fit into the description. These challenges are deemed less significant in the TACTICS system, and are not discussed further here. The definition as described should, however, be implemented in the threshold of commencing the system.

The EU Framework Decision to Combat Terrorism also emphasizes the motivation behind the activity when considering whether it is an act of terrorism or an ordinary offence. The Commission epmhasises it is a terrorist offence when "motivation is to alter seriously or to destroy the fundamental principles and pillars of the state, intimidating people, there is a terrorist offence. This point of view has been incorporated in Member States legislation concerning terrorism. Although the wording is different, they are essentially synonymous with each other."[6] In other words, if there TACTICS and the CMT is to be 'set in motion', the decision maker must have assessed the motivation of a (potential) perpetrator, not only whether a serious crime is or will be taking place.

To sum up, a necessary distinction between terrorism and other serious crimes is the distinct motive of the (to be) perpetrator, which must be political or ideological (Moeckli 2008 p. 35), and with a motive to spread fear among the society in which the act of terrorism is committed (Hilst 2013 p. 119). The objective requirements for establishing when there is a terrorist attack are: certain kinds of serious crimes such as murder, arsen, bombings, etc. Subjective requirements, i.e. *mens rea* is the intention of the act or planned act must be political and ideological, with a motive of spreading fear among the society. The threshold for anticipating when a terrorist attack is sufficiently high in probability to happen for the TACTICS system in general to commence, is dealt with in D.6.2.

[6] As also described by the Commission in the Proposal (COM (2010) 386 Final, no.3). See also definition related to the European Arrest Warrant, stating that terrorist offences are "intentional acts" which in "nature or context, may seriously damage a country or an international organisation where committed with" certain listed aims, e.g. destabilising or intimidating peoples or governments. The acts are also listed, involving e.g. attacks on a person's life that may cause death, serious physical integrity encroachment, kidnapping, seizure of aircrafts etc., and other serious crimes. Threatening to commit such crimes; inciting, aiding, abetting and attempting; and committing certain property crimes (e.g. theft) linked to the list of crimes; are all also within the terrorist offences. The 2008 amendments added e.g. recruitment to and training for terrorist activities (OJ L [2008] 330/23 Art.4).

4 Challenges of the CMT

In this first section, the relevant issues concerning privacy, ethics, human rights and legal conditions of the TACTICS CMT are targeted. The report does not consider legal conditions outside of those related to privacy and human rights. The contents of these notions will be elaborated on below.

The assemblage of several capabilities in the TACTICS system takes place in situations that border to states of exception. Where there is suspicion that a terrorist attack will take place and it needs to be mitigated, when an attack is *currently* going on and needs to be stopped, or an attack has happened and possible follow-up attacks need to be mitigated. In all three situations, the threat or criminal activity is of such a serious nature that the threshold to interfere in individuals' private spheres is significantly lower than normally. This is not, however, an open-ended authority, and the range of individuals who may have their privacy interfered in, and the extent to which the interference should reach, will differ.

4.1 Relevant privacy and data protection legal regulations in counter-terrorism measures

CMT is an information system with its major goal to provide the threat manager (TM) with information on available resources and capabilities (D5.5, p.3). The CMT relies on a pre-existing database of resources and capabilities that TACTICS and the CMT are 'switched on' to allowed access into, in the situation where a terrorist threat has been alerted. The CMT may also upload and read databases and files during operations. This implies a 'total' database, a system-of-systems, with the possibility of adding additional databases and files during operations. Much of the data submitted and extracted by the CMT has fno relevance for the privacy and data protection, for example the description or information of resources or capabilities.[7] Further, police work in terms of information-gathering does not need a legal basis unless such gathering implies an encroachment into a person's personal sphere, according to the principle of legality, protecting the individuals from illegitimate governmental interference. (e.g. Andenæs 1998 pp.176-180; Lund 1996 pp. 72-3; 302-304; Eckhoff and Smith 2006 ch.23). However, the collection and registering of various capabilities and resources containing information on persons, will almost always trigger the legal restraints protecting the individuals' privacy.

TACTICS is developed primarily in a European context, under the budget of the EU Commission FP7 framework. The main focus in this report is on the European instruments of data protection, privacy, legal and ethical regulations. Since the European Convention of Human Rights (ECHR)[8] is the primary source of human rights law in Europe, and is adhered to by the EU[9] in general and all its Member States in particular, this Convention and the Court's practice receives a main focus in the Report. Privacy is a fundamental right, protected as a constitutional standard in European democracies, and enshrined in the ECHR and in the EU Charter of Fundamental Rights (CFREU). The right is also supposed to conform throughout national laws in the EU Member States. The European Court of Human Rights (ECtHR) and EU Court of Justice (CJEU) observe uniform application of the Convention and the Charter. The concept of privacy should therefore be considered as being of a uniform nature within each of these systems.

Privacy is a concept that does not have a single accepted definition, as described in D2.1 section 1.2. Data protection and privacy are often conflated values, but data protection concerns only one form of privacy, namely informational privacy. Data Protection *outside* of privacy concerns e.g. the data protection principle of 'data quality', which may be argued to primarily aim at securing the overall usability of the data (Hilst 2013 p.68) Similarly, while personal data is an important element in privacy, other privacy areas have little to do with such data. The difference is emphasized by the enacting of the Right to Data Protection in the CFREU Art. 8 (more below). The difference is not crucial in the present context, but needs to be kept in mind upon later implementation of TACTICS in national jurisdictions. In the following, a brief overview over the legal standards of the most relevant international sources are described, before the specific issues related to the

[7] These may incur other *legal* aspects, for example related to whether the law in the pertinent State allows the use of UAVs, under which situations, to what extent, etc. The questions of national regulations are not assessed in TACTICS, since such an assessment would reach beyond the Description of Work.

[8] Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950.

[9] The EU will also most likely be an institutional member itself. See e.g. Lock 2012

TACTICS CMT are presented in section 4.3. The States do, however, have a margin of appreciation, and the right to privacy is not absolute. In the next sub-section, the general thresholds and requirements of data protection principles are accounted for, before the purpose limitation principle and proportionality test related to the TACTICS are presented. Following the initial presentation of the relevant privacy and data protection legal framework, it is necessary to target the core concept of terrorism and counter-terrorism measures, since these are those primary in focus of the TACTICS system.

4.1.1 The European Framework

As already mentioned, ECHR provides a right of privacy in Article 8. Article 8(1) declares that "[e]veryone has the right to respect for his private and family life, his home and his correspondence." In addition, the Charter of Fundamental Rights of the European Union (CFREU) calls for the respect of privacy in Article 7, which states that "[e]veryone has the right to respect for his or her private and family life, home and communications."

There is a significant amount of jurisprudence concerning the right to privacy from the ECtHR, and through this case law, the content of the right has been clarified and developed. "Private life" within the meaning of Article 8 represents a broad concept "not susceptible to exhaustive definition" (P.G. & J.H. v. the United Kingdom (2001), para. 56) Cases involving subjects such as name, gender, sexual orientation and sexual life, identity, personal development, and the establishment and development of personal relationships have been recognized under Article 8 (*ibid*). As with the ICCPR (see below), the ECtHR has also recognized the inclusion of business or professional activities within the remit of Article 8 (E.g. Niemietz v. Germany (1992)) The Court has stated that there is "a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'" (P.G. & J.H. v. the United Kingdom, para. 56) Inevitably, the protection of private life also often overlaps with the other spheres covered by Article 8—home, family and correspondence (Reid 2007 p. 481)

The requirements in the European framework for the State's interference into these rights is accounted for below.

4.1.2 EU

The processing of personal data in counter-terrorism security activities is covered by a patchwork of instruments. As mentioned in Deliverable D2.1, the three most relevant in a European context are 1) the 1995 Data Protection Directive[10]; 2) the 2008 Council Framework Decision[11]; and 3) Council of Europe's Convention no.108[12].The Data Protection Directive does not apply to counter-terrorism, since counter-terrorism is within operations concerning public security, defence, State security and State activities relating to it's criminal law [Art.3(2)]. It is still relevant because it clarifies and defines many of the most important core principles of data protection in Europe and the Member States in general. The 2008 Framework Decision applies to data protection in counter-terrorism measures, but only *between* Member States, not for measures taken *within* the Member States respectively. However, the national processing of data for counter-terrorism purposes is generally based on the principles drawn from the principles elaborated on in the 1995 Directive, and on the 2008 Decision's provisions.

There are two legislative proposals from the EU Commission to replace the 1995 Directive and the 2008 Decision. The 2008 Framework Decision is limited to cross-border data processing. It was thus not clear whether it should also apply to internal processing of data by police and other authorities, and whether data that initially is domestic may become cross-border.[13] This is remedied in the proposal of a Directive (COM (2012) 9 final) providing consistent and uniform rules on personal data protection for the purposes of police and judicial authorities' data exchange in criminal matters. A Regulation is also proposed, setting out a more general data protection framework with direct effect through the EU Member States (COM (2012) 11 final).

---

[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data.

[11] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

[12] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981 (ETS 108).

[13] Communication from the Commission concerning the proposals (http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_9_en.pdf p.10 [17.11.2014].

While the proposals are not yet finally approved, it is every reason to believe they will be, in a similar form as proposed, after consulting the European Parliament and the Council.

Depending on the capability in question in TACTICS, there are additional, more specific regulations in various EU counter-terrorism instruments and e.g. in instruments concerning measures in police cooperation. The Data Retention Directive was applicable for data processing related to (among others) counter-terrorism. While the Directive was found invalid by the CJEU in April 2014, many of the Member States had already implemented the Directive in their national legislation. The *national* legislation needs to be amended only with regard to aspects that become contrary to EU law after a judgment by the Court. Member States may also oblige retention of data from various may also follow from the e-Privacy Directive (2002/58/EC).

4.1.3 UN

The applicable UN regulations are briefly accounted for in the following, to show the extent of protection of the privacy and family life and shed light on the terms' international meaning. Arbitrary interference in any person's "privacy, family, home or correspondence" is prohibited both in Article 12 of the UDHR and Article 17 of the ICCPR. The latter also prohibits "unlawful interference". Personal honour and reputation is also protected by the UDHR, while ICCPR prohibits "unlawful" attacks on these values. Both instruments impose upon states parties a positive obligation to provide legal protections against arbitrary or unlawful interference with privacy or unlawful attacks on reputation or honour (Art. 12, second sentence UDHR; Art. 17(2) ICCPR)

The concept of privacy is not defined in the ICCPR nor in the Art.17 supplement "General Comment 16" by the UN Human Rights Committee (HRC) (Joseph, Schultz and Castan 2004 p. 477) The General Comment contains clarifications of the terms "arbitrary interference", "unlawful", "family", and "home", and thus contributes to an elaboration of the context. "Home" is the "place where a person resides or carries out his usual occupation" (UN Human Rights Committee, (1988) at para. 5). The General Comment thus suggests that Art.17 applies to an individual's workplace and work-related life in addition to the non-vocational sphere with which the term "private" has more traditionally been associated. "Correspondence" within the meaning of the ICCPR includes telecommunications according to the General Comment (*ibid* para. 8). In other words, for the CMT context, all technologies that transmit information over distances, not only phone conversations, but information transmitted via internet and wireless equipment. The General Comment also adds that "searches of a person's home should be restricted to a search for necessary evidence and should not be allowed to amount to harassment" (*ibid* para. 8)

4.1.4 Specific issues concerning cross-border counter-terrorism measures

Counter-terrorism measures are increasingly international in their scope, and there is a growing number of cross-border instruments for States' cooperating against terrorism. The first step in the capability management process (CM) is to systematically collect and describe security capabilities in a standardized way (D5.2 p.7). Neither the TACTICS system in general nor the CMT specifically target the cross-border nature of terrorism as such or the measures taken to prevent or interrupt terrorist attacks. The main focus of TACTICS is terrorist attacks in urban environments, disrespective of within which country. It is important to emphasise, however, that the CMT could be seen as more of a complete tool if it also took into account capabilities stemming from foreign or international sources. This could be neighbouring countries' police or financial databases or foreign UAVs in private or public ownership, or Europol's databases[14] or other security equipment.

Extending the CMT to include also available international or foreign capabilities/resources is a natural and foreseeable step further in the development of the TACTICS system.

At the EU level, there are several regulations concerning protection of privacy and data protection related to the cross-border security forces' cooperation. The Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters is central, and also the Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement on such data

[14] Europol has access to some of the data in the Schengen Information System (SIS), for example. Europol also has its own extensive databases with broader functionalities than the SIS. The Europol information system, TECS, consists of three components: an information system (EIS, Europol Decision arts.11-13); working registers for analytic purposes (AWFs, Art.14); and an index function (Art.15). See more e.g. in Ugelvik 2014.

(2012/0011 (COD)). A main reference framework for the EU action in this field is the 2005 EU Counter-Terrorism Strategy[15]. The EU emphasizes, however, that it is the Member States that are the key actors in the sensitive policy area that counter-terrorism measures are a part of. At global level, e.g. the UN Resolution 1373 (2001) is relevant.[16]

After this short overview over the most relevant international sources of privacy and data protection regulations, the subsequent three sub-sections go deeper into the general thresholds and requirements applicable for most TACTICS capabilities and resources.

4.2 Thresholds/requirements applicable in all TACTICS capabilities

The TACTICS tools assume that the users (TMs) are knowledgable in the domain under consideration. The CMT provides the user with facilitated overview in the exisiting and available security capabilities, which the user normally will have (some level of) knowledge about. The TM will know for example that intelligent cameras are better at detecting deviances across large spaces and times compared to what security officers can see, and that floor security has the advantage of being able to see very detailed deviances from a very small distance. Also, the people who actually walk around the location are the only sources that are capable of acting directly after they see something deviant (D5.2 p.6). The legal and ethical aspects may, however, be less apparent and known. These are, however, simultaneously crucial for the legal compliance of the use of the system, and for the external legitimacy (that the system and use of the system is perceived fair in the society) of the TACTICS system.

The following principles set out general requirements that apply for all the capabilities that may be provided information of or connection to by the CMT. In other words, for every capability that 'pops up' as an alternative for the TM to apply in the counter-terrorism activity, there should in addition to any particular legal and ethical requirements 'pop up' be a constant question of these general requirements. A good solution would be a 'pop-up' that carries in it a threshold: the TM may not apply the capability before having answered that the use will be legal, necessary and proportionate, with (brief) justification. These requirements are explained in the following.

4.2.1 General data protection principles

EU's Data Protection Directive sets out the general rules of data protection for all data within the Union Member States (including the EEA Member States). According to the Directive (95/46/EC), personal data must be: fairly and lawfully processed [Art 6(1)(a)], collected for specific, explicitly defined and legitimate purposes [Art. 6(1)(b)] and not further processed in a way incompatible with those purposes [Art. 6(1)(b)] (data minimisation) and retained only for as long as is necessary to fulfill that purpose – Art. 6(1)(c) (implicitly). The principle of 'data quality' assures that data is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed [Art. 6(1)], accurate and, where necessary, kept up to date [Art. 6(1)(d)]. Furthermore, there must be a legitimate basis for processing data (Art. 7), and an unambiguous consent of the data subject [Art. 2(h)], meaning that there must be a contract to which the data subject is a party. There must be compliance by a legal obligation of the data controller to protect the vital interests of the data subject, and performance of the task carried out must be in the public interest or exercise of official authority and that legitimate interest is pursued by the controller.

Data must be anonymized and kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed [Art. 6(1)(e)]. Collected data must be secure, meaning that its processing will be done in a confidential (Art. 16) and secure manner (Art. 17) i.e. with appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Finally, subjects shall be completely notified about data processing, meaning that the controller must notify the national supervisory authority before carrying out any wholly or partly automatic processing operation, subject to certain exceptions, e.g. appointing the in-house data protection official [Art. 18(1-2)].

Processing of certain categories of data is prohibited, i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life [Art. 8(1)].

[15] Doc. 14469/4/05 of 30 November 2005.

[16] See more in e.g. Sambei, Polaine and Du Plessis, 2009, ch.9; and Hilst 2013.

Member States may, for reasons of substantial public interest, lay down exemptions in addition to the above mentioned [Art. 8(4)]. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority [Art. 8(5)].[17]

Transfer of personal data to jurisdictions without adequate level of protection is prohibited (Art. 25), unless it is covered by one of the following exceptions [Art. 26(1)]: explicit unambiguous consent of the data subject, contract or pre-contractual measures, contract between controller and a third party in the interest of the data subject, important public interest, vital interest of the data subject, transfer from a public register, authorisation by Member State [Art. 26(2)].[18] This may typically be police cooperation agreements, bi- or multilateral. This means that if the CMT will provide data that may be transferred further outside the EU Member State (presupposing that TACTICS is initially designed within the EU FP7 Programme), an additional level of data protection measures is required. Since counter-terrorism measures, including the assembling and furthering of capabilities in the CMT, frequently may require cross-border transfer of data, the system should have the additional data protection measures built in.

This sub-section constituted a brief overview of general data protection regulations following the overall principles. In the following, the so-called permissible limitations test is presented, where these regulations are 'translated' into a more simplistic, schematic way that may facilitate the on-going acknowledgment of these rules in the CM and TM processes. First, however, some notes on the challenges of information acquisition and data protection issues are presented. The point here is that the permissible limitation test, accounted for immediately afterwards, should be seen as the solution for the challenges of information acquisition and processing in the CMT.

4.3 Information acquisition, data protection challenges and the permissible limitation test

4.3.1 Rule-based processing

What TACTICS CMT seeks to have implemented is what may be called 'rule-based processing'. The tool seeks have a 'pop up' function with 'thresholds' implemented, so that the measure may not be accessed before the query proves that it is consistent with the applicable policy rules/legal requirements. The rule-based processing requires also that the user's query carries with it information on his or her type of permission (i.e. TM, different levels of TM, or similar). For example, a query might indicate that it is pursuant to a search warrant, which would allow it to retrieve certain kinds of data that would be unavailable without a warrant (Taipale pp. 75-76). The data must also be labeled with information about how they may be accessed. Data items might be labeled with "meta data"—data that summarize or describe the qualities of the data—that indicates how the data can be processed. This meta-data label would always be attached to the data and regulate the access to them wherever they reside (*Ibid*; DeRosa 2004 p.19)

A challenge to the rule-based system is which level of legal regulations should be 'attached' to the data, i.e. should it be national (where the data originates from), where it is used, with *also* international binding and non-binding regulations, such as ECHR, EU or UN recommendations. Additional or subsequent labeling of coupled data may also be hard to determine the scope and precision of.

The implementation of rule-based processing when the TACTICS CMT is to be implemented, requires a manner of testing whether or not a capability is challenging human rights in general and privacy and data protection rights in particular.

4.3.2 Permissible limitations test

The purpose limitation test following the ECHR Art.8 provides requirements for when the States may legitimately interfere in the citizens' right to privacy. According to Art.8 (2), the interference must be 1) prescribed in law (i.e. 'legality', 2) necessary in a democratic society ('necessity'), and 3) serve a certain public interest (i.e. 'legitimacy'). This implies in total that the interference must have a firm, clear, explicit and foreseeable legal basis, and it must be proportionate to the legitimate aim pursued, i.e. corresponding to a pressing social need (E.g. De Hert 2005 pp. 69-96; Troncoses Reigada 2012) Counter-terrorism measures and crime-control related to terrorist acitivites fall within the ambit of Art.8 (2), since terrorism constitutes a

[17] The EU Commission must be notified about such derogations, it is thus not something that may be decided randomly and unchecked by States [Art. 8(7)].

[18] The EU Commission determines which jurisdictions provide the adequate level of protection [Art. 25(6)].

threat to “national security” and/or “public safety” (*Case of Klass and Others v. Germany* (1978) paras. 44, 46) On the other hand, the fear of terrorism must imply the lowered threshold of intrusive interference to the degree that the measures are counter-productive. Too much surveillance, too smart cameras and too many unmanned aviation vehicles (UAVs), too suspicious floor security and too much registration in various databases accessed by too many people may lead to a heightened level of *in*security in the societies. The legal limitations described here and in the following are meant to ensure this balancing in the use of the TACTICS system, in particular the CMT. The ethical issues are constantly foundational to the legal regulations, but see also below in section 6. The more specific ethical assessment of the TACTICS system as a whole is found in D4.3.

The ‘permissible limitations test’ or ‘proportionality test’ has become one of the cornerstones of both privacy and data protection in Europe (Bagger Tranberg 2011, Bellanova 2014, De Hert 2005, Troncoso Reigada 2012). According to Hilst, there is a simplistic schematic way that the ECtHR conducts this ‘permissible limitations test’ (Hilst 2013 p.6) This test is valuable when applying the CMT, in order to assess whether the capability/resource in question may or may not constitute a breach with the privacy and data protection rights of the individual(s) involved. As explained in the description of decision-making in D5.2 (p.11-13), it is the TM who assesses how to handle a threat. The CMT, however, is also to supply the most apprioriate capabilities – and the alternatives – to the TM. As such, it is necessary that the legal requirements also are considered in the CMT process.

The first step involves the assessment of whether the capability constitutes an interference. The consideration includes the severity of the encroachment, and the scope is protecting the subject’s family life, private life, home and/or correspondence. For example: the resource a police officer in a public space is not in herself an interference, but coupled with a listening device resource, together constituting a capability, picking up on the conversation of two individiuals nearby, may constitute an interference.

The second step is the assessment of whether the capability/measure is in accordance with law, meaning clear and forseeable national law. A clear legal basis for the security measure the CMT assembles must in other words be present, both formally and materially. This prerequisite implies three requirements: the accessibility of the legal instrument; its foreseeability, or predictability (the possibility for citizens to understand when the measure will apply); and the setup of the necessary safeguards. Sufficient safeguards against abuse must also be present.

The third and final step is to consider whether the measure is necessary in a democratic society. Proportionality of the measure is included here. This implies that there must be a legitimate aim of the measure, meaning that it will fulfill a pressing social need. Preventing the threat of a terrorist attack or stopping of such an attack will constitute a pressing social need. The threshold for at what precise time a threat becomes sufficiently ‘pressing’ will be analysed below. It is presupposed here that an attack, expected or on-going, has materialized to the extent that the TACTICS system-of-systems has been ‘set in motion’/triggered. The third step also includes that the measures must be proportionate to the intereference. This means that even though mitigating a terrorist attack clearly constitutes a necessity in a democratic society, it is not necessarily proportionate to wiretap all the mobile phones of the entire population in order to search for perpetrators.

The so-called margin of appreciation implies that the States is allowed “a certain measure of discretion, subject to European supervision, when it takes legislative, administrative, or judicial action in the area of a Convention right” (Harris *et al* 2009 p.11). For TACTICS systems and the CMT, the margin of appreciation underlines how various States may emphasise the public or national security differently when considering the necessary steps to take to counter terrorism. This means that what is allowed in one Member State is prohibited in another. Nevertheless, the ECtHR may assess the proportionality of any State measure, thus ensuring some level of uniformity. The proportionality is returned to immediately below.

4.3.2.1 Necessary

While the States must protect the right to privacy, ECHR Art. 2 provides the obligation also to protect national security and public safety (*Kiliç v.Turkey,* First Section (2000) para.62) The States also have a legal and moral obligation to protect the citizens and the State itself from terrorist attacks. As such, preventing and stopping terrorist attacks is ‘necessary’ to protect citizens and the State.

What constitutes ‘nescessary’ in a democratic society has been developed in courts. According to the Court of Justice of the EU (CJEU); ‘necessary’ is not as stringent as ‘indispensable’. In the *Huber* case, the keeping of a population register was considered sufficiently ‘necessary’ in that is contributed to “the more effective application of that legislation as regards the right of residence of Union citizens who wish to reside in a Member State of which they are not nationals” (Case C-524/06 *Huber* (2008)) According to Bygrave, this reading is in conformity for both the Data Protection Directive Art. 7 and the ECHR Art. 8 (2) (Bygrave 2014 p.150)

The necessity criterion in the same *Huber* case also implied, however, that the database in question *only* contained the information necessary for the application by those authorities of that legislation. And further that storage and processing of non-anynomised data for *statistical* purposes did *not* meet the criterion (*Huber* 2008 paras. 66;68)

Criticism has been raised, however, related to the lack of examination of counter-terrorism measures and the relation to (the perception of) security among the citizens, i.e. whether counter-terrorism measures *work* to enhance necessary security for the citizens.[19] And further – the categorization of a capability as one concerning counter-terrorism instead of e.g. crime prevention or public safety is a relevant issue for the CMT and other counter-terrorism measures. This is relevant because the threshold of deeming a measure (or resource or capability) as 'necessary' is generally considered *lower* when national security is at stake than when the interests 'only' protected in ordinary criminal law are at stake (Hilst 2013 p.96; Zedner 2007). If a measure or capability is *not* necessary to protect national security, but merely to protect e.g. the life of one or more individuals or serious property crime, etc., the threshold is higher to apply the capability in question.

The challenge related to the TACTICS CMT and consequentially into the TM is how to apply the necessity test at the same time as the CMT task at its core is assembling as broad a range of capabilities as possible. According to the necessity test as applied by the CJEU and accounted for here, one could suggest that the CMT should filter access to databases or information from other capabilities that when collected could imply a breach with the principle. This may especially be challenging related to the establishment of temporary databases storing and processing the collected data for use by the TM (and consequentially possibly others in the operational theatre).

The TACTICS systems should solve these issues in two steps central to the CMT process:

1. In order to meet the criterion, there should be a necessity analysis/threshold implemented in the CTM before or as a supplement to providing the TM with the various information from or of a capability.
2. The 'pop up' question: Is the capability/resource necessary to apply in the particular situation? The question is for the CMT to pose, and the TM to take a stand in. The TM must also decide whether those who gain access to the capabilities are only those who *need* it.

4.3.2.2 Purpose limitation

Purpose limitation implies that data should only be used for "specific, explicit and legitimate purposes" that are present at the time of collection of the data. The principle requires any subsequent use of the data to be in compliance with the original purpose of the collection (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, para. 9) If there is a later change of the purpose, this must be clearly notified. The CFREU states this in Art.8 (2), requiring all data processing to be done "fairly" and for a specified purpose. The Council of Europe's Convention on Automatic Processing incorporates the purpose specification principle in Article 5, which provides that any personal data that is subjected to automatic processing must be "stored for specified and legitimate purposes and not used in a way incompatible with those purposes" (Art. 5 (b). The EU Framework Decision also imposes the purpose specification requirement in the context of data transferred between law enforcement or judicial authorities.[20] Article 3(1) of that instrument provides that "[p]ersonal data may be collected by the competent authorities only for specified, explicit and legitimate purposes in the framework of their tasks and may be processed only for the same purpose for which data were collected." The provision further requires that any processing be "lawful and adequate, relevant and not excessive in relation to the purposes for which they are collected."

The purpose limitation sets out an important consideration for the use of the TACTICS CMT. A core of the CMT is to assemble and make accessible various capabilities for the TM to employ. While the legal limits apply as to which capabilities are legal in the jurisdiction in question, many of the capabilities will as a point of departure have other purposes. Typically, information databases such as registration databases for residentials, driving liscences or tax registries are established for purposes that initially are incompatible with counter-terrorism activities.[21] Databases that originally are intended for crime control, such as the Schengen

[19] The difference between perceived and factual levels of security is not dealt with here. This is to some extent discussed, though, in D4.3.

[20] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

[21] See more on this related to data mining in DETECTER WP 8, *D16.3* ch.3.

Information System (SIS) fall within the same purpose category as counter-terrorism, and therefore fall under "compatible purposes".

The principle of purpose limitation in the Convention on Automatic Processing is derogable. Counter-terrorism may typically be an area of derogation in order to provide more flexibility. The other principles, of necessity and proportionality, still apply. States would have to show that complying with the purpose limitation principle of the Convention would hinder their counter-terrorism efforts. Furthermore, the purpose specification requirement of the EU Charter would still apply, subject to permissible limitations. TACTICS users thus would be obliged to define the purpose of the capability making use of personal data for another use than the original, or be able to clearly demonstrate that it was necessary to refrain from doing so and that this was consonant with the principle of proportionality and was genuinely effective (*ibid).*

The principle of minimality, following from the Data Protection Directive Art. 6(1)(c) and Art. 5(c) of the Convention 108 also applies for the CM process, implying that the amount of personal data collected should be limited to what is necessary to achieve the purpose(s) for which the data is gathered, stored and further processed (Bygrave 2014 p. 51). Both provisions require that data is erased or anonymized once it is no longer required for the purposes it has been kept (DPD Art. 6(1), Convention 108 Art. 5(e)). Continous storage of data 'just in case' for counter-terrorism purposes is not permitted.

4.3.2.3 Transparency and accountability

Transparency and accountability, e.g. through logging of the CM and TM processing, is vital to maintain the legitimacy of the system-of-system. The necessary level of transparency and accountability is recommended safeguarded in national legal regulations that are publicly available.

Technology changes very fast, as do threats and environmental factors. The process of collecting, selecting, and requesting capabilities must be future-proof. In addition, the process should help prevent over-reliance on a familiar tool, i.e. the "law of the instrument". The "law of the instrument" is an over reliance on a familiar instrument instead of trying another, potentially more effective instruments. This bias leads to the risk of using the wrong tool for the job. In the context of TACTICS, this could mean using a tool that is not effective, that is too invasive, or that is not efficient.

The process of collecting, selecting and requesting capabilities should therefore describe capabilities and resources in just the right abstraction level, i.e. the level that the Threat Manager needs to know about them in order to be able to decide on their deployment. The first part of this information covers "fitness for purpose". A practical example could be the deployment of (expensive, invasive) own police personnel, where the same task perhaps could be done by private security companies that are already there. The specifics of how this should be implemented in the system follows in D6.2.

4.3.2.4 Consent in counter-terrorism measures

A general rule in the privacy context is that people may expect less privacy protection when they have consented to give out information about themselves (Hilst 2013 p. 92). In other words: it is less unproportional to use sensitive information if the person in question freely has distributed this information in public fora. This may be where the person has agreed on terms and conditions for using online services, or entering into (public) areas where there is ample notification that the area is under CCTV surveillance. This will be a typical scenario in CMT situations. But related to counter-terrorism measures, the issue of consent is problematic, since the resources in question often will be covert. It has been argued that there are no real options to opt out of government surveillance (Fetzer 2003). As Hilst argues, however, the counter-terrorism legislation in itself may be seen as presupposing consent from the people reciding or travelling in a specific country (Hilst 2013 p. 92). The laws of the country are presumed democratically legitimate, and throught the legitimate process, a consenting contract is formed (also Ugelvik 2014 ch.15) In this way, the consent may be considered present also in secretive counter-terrorism measures for those who have participated in the democratic elections, and for those who willingly enter into a jurisdiction where these laws apply. This is controversial for example to the extent that while the police in a country are legitimated by being based in laws enacted through democratic processes, the actions and measures *in practice* set in motion by the police, especially not secretive measures.It should therefore *not* be presupposed as a general rule by the CM that capabilities or resources that exists because of police initiative or generally already is in place in public spaces may be anticipated consented to by individuals.

This sub-section has given account of the general principles of privacy and data protection in the international instruments relevant to the TACTICS CM process. It has explained the permissible limitations test and the requirements therein of necessity, proportionality and purpose limitation of the capabilities that the CMT must take into consideration when selecting resources for matching in capabilities and capabilities presented to the TM. The lowered threshold of interference in the case of consent was briefly discussed. In

the next section, the most relevant specific resources or capabilities are presented, and the most pertinent rights challenges related to these discussed.

5 The specific capabilities

The Capabilities Management Tool will generate information on the capabilities/resources available for public security forces in a terrorist attack situation.The full spectrum of capabilities that may be available will depend on several factors such the current state of technology and the regulations within the State in question. The general applicable legal thresholds were accounted for in the previous section. In this section, some of the central capabilities are presented and the particular legal thresholds and guidelines provided for them respectively. Although there may be other capabilities available for the security forces that are not dealt with here, the legal frameworks are considered those relevant also for similar/same category capabilities/resources. The capabilities are divided into three categories: 1) Instruments/tools dealing with visual data collection and analysis; 2) Instruments/tools dealing with database or web analysis; and 3) Capabilties that are assemblage of several resouces with cumulative potential intrusivenes. Extra focus will be given to the issue of interoperability between police and immigration databases in the EU and Schengen Member States, since interoperability and coupling of information is to be a core feature of a TACTICS system.

5.1 Instruments/tools/measures that deal with visual data collection & analysis

Three resources applied in the CM processes are focussed on here: intelligent cameras, vision by hidden cameras and vision by UAVs. The three partly overlap in the sense that for example an intelligent camera may be hidden or located on a UAV. The point of dividing them in three categories is to highlight the particular characteristics and thus aspects to take into consideration in the CM process.

5.1.1 Intelligent/smart cameras

Security personell is only capable of monitoring a modest number of incoming video streams from CCTV. In a society where the volume of video data grows, the ability of the security personnel with human eyes becomes progressively less effective in processing visual details. Fatigue and long hours may exacerbate the problems connected to traditional CCTV and security personnel resources coupled in a surveillance capability. Intelligent surveillance cameras are cameras with the ability to see and process visual information similarly to humans, for example distinguish between a human and a car, or locating certain symbols or characteristics on human beings. Such systems can be programmed to track only objects identified as human and send an alert when the subject violates pre-defined rules, such as climbing over a wall.

A smart surveillance system is “capable of extracting application-specific information from captured information (be it digital images, call logs or electronic travel records) in order to generate high-level event descriptions that can ultimately be used to make automated or semi-automated decisions” (Wright *et al* 2010 p. 347)

In relation to the TACTICS CMT, the major challenge related to intelligent cameras is whether the programming of the intelligent cameras leads to biased decisions from the CCTV operator. On the other hand, intelligent cameras are less problematic in use when they are programmed to detect and target for example potentially dangerous tools in public places, such as an unaccompanied suitcase or a gun. The potential bias comes when the detection of deviant behaviour is based on parameters distinct and visible behaviour, such as all ‘whole-body behaviours (including movement about a space, excessive body gestures or gait)’, were identified as well as behaviours that are ‘less obvious (such as signs of stress, rapid eye movements, blinking, mumbling and perspiration)’ (Vermeulen and Bellanova 2012)

The Article 29 Working Party of the EU has asserted that the principles of the Data Protection Directive apply to any information **—** including sound and image information **—** concerning ‘an identified or identifiable person’, by any type of surveillance technology (Article 29 Data Protection Working Party, Opinion 4/2004 p. 15). The permissible limitation test thus applies.

A way of avoiding the TACTICS CMT being in breach of privacy rights when assembling intelligent camera or other similar resources and capabilities is to anynomize the data. The collected data is still categorized and legally regulated as personal data, since the image may be deanonymised by a public authority for example with the purpose of investigating crimes (*ibid*). In other words: data in the form of text or images collected by a resource such as an intelligent or hidden camera that is anonymized in the storage database of a private security company, may, because of the TACTICS counter-terrorism purpose almost always be

deanonymised. The crucial threshold lies within national legislation of the country of application. This means that in this report, the issue can only be pointed out; the data controller and CM and/or TM in TACTICS must be aware of local/national thresholds.

5.1.2 Vision by hidden cameras

Hidden cameras constitute secret surveillance. Secret surveillance may, according to the ECtHR, be exercised in a democratic society in the interests of national security and/or for the prevention of disorder or crime" (*Klass*, para. 48). The development and increase of terrorist activities in Europe was emphasised as a factor that justified resort to secret surveillance and similar measures. In the relevant case, *Klass*, however, the Court made clear that "adequate and effective guarantees against abuse" had to be in place (para. 50). Similarly in the *Malone* case, "[s]ince the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large", national law had to "indicate the scope of . . . discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference" (Malone v. the United Kingdom (1984) para. 68) Again, we see that the most relevant legal requirements and assessments must take place according to the national law in the country involved. Specific considerations must be done upon implementation of TACTICS in national jurisdictions, where certain safeguards must be in place determining 1) the nature, scope, and duration of possible surveillance measures; 2) the grounds on which those measures would be permitted; 3) the particular authorities that were given the power to carry out and supervise the measures; and 4) the nature of any remedies provided to the subjects of surveillance (*Klass*, para. 50)[22]

5.1.3 Vision by UAVs (drones)

Unmanned aerial vehicles may be defined as "a device used or intended to be used for flight in the air that has no on-board pilot" (Aviation Safety Unmanned Aircraft Programme Office, 2008, cited in McBride 2009 p. 628) This includes all classes of airplanes, helicopters, airships, and translational lift aircraft that have no onboard pilot. UAVs are distinguished from aeroplanes and CCTV because their "mobility and discretion" enable them to be used in many more circumstances, and because they can be combined with other technologies such as cameras devices, Wi-Fi sensors, microphones, biometric sensors, GPS systems, systems reading IP addresses, RFID tracking systems which all offer the possibility to process personal data and make same potentially powerful surveillance tools.[23]

There are some practical danger aspects related to UAVs that need to be taken into consideration by the CM and TM. For example, the circular Unmanned Aircraft Systems (RPAS) Cir. 328-AN/190 addresses among others the concern of risk to other aircraft or third parties, and the restriction of access to airspace. There may for example be instances where the remote pilot cannot respond in the same manner as could an on-board pilot, e.g. flight conditions or sudden meterological changes. The remotely piloted aircraft must be operated in such a manner as to minimize hazards to persons, property or other aircraft and in accordance

[22] The *Liberty* case provides an example of legislation that was found to be inadequate (Liberty and Others v. the United Kingdom (2008)). In *Liberty*, the measures implemented by the UK were found not to be in accordance with the law since the controlling legislation was not sufficiently precise. The ECtHR was also troubled by the wide discretion that was vested in the Secretary of State in terms of providing safeguards and ensuring that they were complied with. As presented to the Court, authorization for surveillance required a warrant that would describe the communication channel to be tapped plus a certificate, which described the categories of information that would be extracted from the intercepted communications (para. 43). Both documents, as a rule, would be issued by the Secretary of State (paras 25 and 43). Warrants permitted interception of broad categories of communications, e.g. all communications travelling on commercial submarine cables between the UK and Europe (para.64). The Secretary of State had the sole discretion in making the determination of which intercepted communications should be examined. Allegations presented to the Court suggested that vague criteria were used such as "all communications implicating national security" (para. 65). Safeguarding of disclosure and reproduction of captured communications as well as observance of the certificate also fell solely to the Secretary of State, who was granted broad discretion to implement measures "as he consider[ed] necessary" (para. 66). Lastly, whereas the German G10 law at issue in the *Weber* case contained provisions relating to procedures, in the UK, procedures were prescribed in internal rules and policies which were not publicly available nor produced for the Court (para. 66-68).

[23] Opinion of the European Data Protection Supervisor (EDPS) on the Communication from the Commission to the European Parliament and the Council on "A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner", 2014.

with the conditions specified in Appendix 4 of the RPAS. There are, however, also privacy and ethical considerations related to the CM's assembling and suggesting of UAVs to the TM. The same test and requirements as for the intelligent cameras apply. Further, it needs to be noted that observering and detecting by UAVs may lead to an increased perception among people of *feeling* observed, regardless of how or whether the information actually is used. This perception may lead to a contrary effect from what the police intends; it may lead to *in*security rather than security.

One of the challenges related to UAVs is that it has strict limitations to crossing borders in and out of other jurisdictions than the operating country. According to the 1944 Chicago Convention Art.8, no aircraft capable of being flown without a pilot shall be flown without a pilot over the territory of a contracting State without special authorization by that State and in accordance with the terms of such authorization. This is in line with the below-mentioned European frameworks. Each contracting State undertakes to insure that the flight of such aircraft without a pilot in regions open to civil aircraft shall be so controlled as to obviate danger to civil aircraft. This means that drones are not allowed directed into the airspace of another state without its permission. Again, the national legislation is the pertinent threshold. This limitation implies that if for example cross-border hot pursuit of a suspected terrorist is an alternative according to the Schengen Agreement Art. 40, UAVs may *not* be used as part of the police operation. The pertinent European regulations include Regulation (EC) No 216/2008 and in particular Remotely Piloted Aircraft Systems (RPAS, i.e. UAVs), when used for civil applications and with an operating mass of 150 kg or more. From the European RPAS Steering Group, a roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System is developed (June 2013), and the so-called EUROCONTROL has established "Specifications for the use of military remotely piloted aircraft as OAT outside segregated airspace" (2007). Finally, a recent Communication from the Commission targets the opening of the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable way (EC, COM (2014) 207 final).

Related to privacy and other human rights, the European Data Protection Supervisor (EDPS) has stated that "the rights to private and family life and to data protection, as guaranteed in Article 8 of the Council of Europe Convention on Human Rights and Articles 7 and 8 of the Charter of Fundamental Rights of the EU, apply" to vision by UAVs. EDPS compare remotely piloted aircraft systems to online technologies considered by the CJEU in the *Digital Rights Ireland*[24] and *Google Spain v AEPD*[25] rulings, which has potential to "seriously interfere with the rights to private and family life and to data protection", and must be considered very carefully (EDPS 2014) Using embedded technology, the UAVs may offer the possibility to collect, record, organise, store, use, combine data allowing operators to identify persons directly or indirectly. Further, EDPS mentions, "this identification could be done by a human operator, by automatically screening the image taken against the facial recognition programme of an existing database, by scanning to detect a smartphone and use it to identify the person, by using RFID in passports, etc." (*Ibid* para. 30). As a result, UAVs may be used to process personal data in the meaning of Article 2(a) of the Data Protection Directive (95/46/EC), and will almost always interfere with the right to privacy and family life according to ECHR Art. 7 and CFREU 8.

For both intelligent and hidden cameras and UAVs operating within the EU/EEA area, whether the camera is filming in a public or private space, is not a relevant criterion when determining whether the right to privacy and the right to data protection apply or not. This was established in ECtHR's *Von Hannover v. Germany* ruling, "the concept of private life extends to aspects relating to personal identity, such as a person's name, photo, or physical and moral integrity; the guarantee afforded by Article 8 of the Convention is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings. There is thus a zone of interaction of a person with others, even in a public context, which may fall within the scope of private life. Publication of a photo may thus intrude upon a person's private life even where that person is a public figure".[26] This implies that in both public and private spaces, all individuals may assert their right to respect for privacy and family life, "i.e. the right not be targeted with a zoom lens or a directional microphone or to protection against the exposure of the totality of their movements to the public, being tracked or the recording of their conversations" (EDPS 2014 para. 30).

Whenever the personal data is used in the framework of police and judicial cooperation in criminal matters, which it will be in TACTICS whenever it is public security personnel using the system, any exchange

---

[24] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others*, 2014.

[25] Case C-131/12 *Google Spain SL, Google Inc.v Agencia Española de Protección de Datos (AEPD),* judgment of the ECtHR of 13 May 2014.

[26] Applications nos. 40660/08 and 60641/08, *Case of Von Hannover v. Germany* (No. 2), (2012) para. 95.

between Member States of personal data gathered through UAVs must comply with the requirements as specified in Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.[27]

The EDPS emphasizes the necessity of *awareness* of the privacy impact of their actions when security personnel is using UAVs. For this to be upheld in the TACTICS CMT, it is necessary that also in the CM process, the necessity and the privacy impact is assessed. It is not sufficient that the UAV is accessible. EDPS for example emphasizes choosing the least intrusive UAV, overloaded with high resolution sensors if those are not needed to meet the objectives in the current situation, and that the security of any collected data is appropriately managed (EDPS 2014 para. 63).

5.1.3.1 Wiretapping

Albeit with sound, not vision, wiretapping is also mentioned here. Wiretapping in this respect refers to generalized wiretapping of larger amounts of people, not wiretapping by the police of one or more individuals one the basis of a court order. The latter cases need to follow internal national regulations concerning use of police evidence material.

In *Kruslin* and *Huvig*, two cases which concerned wiretapping, the ECtHR named specific deficiencies in the national surveillance law which indicated that the law could not be deemed to provide adequate protections against abuse (see Kruslin v. France 1990, para. 35; Huvig v. France (1990), para. 34). These deficiencies were reformulated in *Weber and Saravia v. Germany* and presented as “minimum safeguards”, indicating that they are now regarded as mandatory protective measures to be included in national regulation of communications surveillance. These were:

1) definition of the nature of offences for which surveillance measures are permitted;
2) definition of the categories of persons who may become subject to such measures;
3) limits on the duration of surveillance;
4) procedures for examining, using, and storing data from the surveillance;
5) the precautions to be taken when communicating data to other parties;

the circumstances for the destruction of recorded information from the surveillance (Weber & Saravia v. Germany (2006), para. 95). This list should be implemented as an automatic link in the CM process when wiretapping resources are gathered.

5.1.4 Human resources

Even with automatic and unmanned surveillance devices, there will almost always be human resources involved at some stage of the process. Two types of human resources are mentioned here: floor security and camera operators.

Floor security needs to be trained to minimize the risks of biased decision making in situations. Using international training programmes such as Search, Detect and React is one example (see http://www.isca.org.il/about.html [20.01.15]), but a more likely scenario is that the (public) security personnel is trained generally as police or security officer, or/and particularly as operator of (some part of) the TACTICS system.

Human resources will manage the manned surveillance cameras, and will at least partly select which data from the footage to be analysed further from intelligent cameras. This means that even though an automated filter targeting only e.g. certain types of deviant behaviour or suspicious items in an urban location such as a shopping centre, a police officer checking the generated data may positively and negatively change the data selection from the instruments. S/he is also vital in determining the further steps to take in the situation, for example in the CMT, where the assessment must be made of which capabilities are relevant, not too intrusive, etc. It must be considered an inherent risk that the CM may assess any accessible resource or capability as necessary and proportionate in mitigation of an on-going terrorist attack, simply with reference to the seriousness of terrorism. Following the Privacy-by-Design structure, and the outcome of the

[27] See the Explanatory Memorandum of the European Commission to the 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/2012/010 final - 2012/0010 (COD)), in particular, p. 2 para. 2 (EDPS 2014 fn. 39).

abovementioned ECtHR rulings, it must be considered imperative that the human resources involved are subjected to througouh training before operating and making decisions in the TACTICS CMT.

5.2 Instruments/tools/measures that deal with database or web analysis

The resources and capabilities applied in the CM processes that stem from databases or data collection online are targeted in this sub-section. The EU policy programme of 2004, the Hague Progamme, articulated a clear link between movement, migration and terrorism, emphasising the necessity of a coherent approach and harmonised solutions of data registering in these areas (The Hague programme:1.7.2; Mitsilegas 2009 p. 245-6) One of the measures that was a result of the Programme alongside several anti-terror initiatives, this quite recently after the Madrid bombings and, of course, the other terrorist attacks of the early 2000s, was intended to provide access for law enforcement authorities to immigration databases. The focus here is on databases such as the Schengen Information System, and the challenges related to interoperability between such databases and the (temporary) database that may be established applying TACTICS.

The (temporary) databases created in TACTICS by the CMT may acess databases with so-called 'big data', i.e. vast and complex information databases. Big data is defined by the Gartner Group as "high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making" (http://www.gartner.com/it-glossary/big-data/[16.11.14]) Big data can with modern technology be retrieved from countless sources and scrutinised to discover characteristics that may otherwise remain hidden. It this permits the analyser to create information about data that was never apparent or intended in the source information (EDRi report 2013 p.10). For the CMT, it is particularly relevant to consider whether the TM may or should be allowed access to all the different information in all the different databases. Big data is not the main focus in the following. The main legal challenges are considered similar to coupling of databases alongside interoperability of databases, which is targeted below in sect. 5.2.1.5. The other resources or tools considered key in the CMT are web crawling and (sect. 5.2.3) and data mining (sect. 5.2.4).

5.2.1 Databases

The main focus of EU measures concerning policing has been on facilitating the gathering, transfer, analysis and exchange of information (Ugelvik 2014, p.136) There may be several situations where sharing and comparing data between law enforcement authorities is relevant or necessary through the CMT. Examples may be solving cases by identifying persons in DNA or AFIS (fingerprint) databases of another Member State, linking unsolved crimes to the pertinent terrorist threat in different Member State to the same (yet unidentified) person, establishing the true identity of a person who has travelled in several States, or communicating alerts when a person is wanted (for arrest or trace/location) and/or dangerous. The exchange of information – inter alia by simply talking to another police officer the phone; discussing people, trends, impressions, etc. – may to a large extent happen without any legal basis, as long as the conversation does not imply breaches of professional secrecy. Professional secrecy will further often be lifted when the purpose of the communication is investigating, preventing or averting a criminal offense. As such, much exchange of information may take place informally and without legal basis.[28] Police work in terms of information-gathering does not need a legal basis unless such gathering implies an encroachment into a person's personal sphere, according to the principle of legality, protecting the individuals from illegitimate governmental interference. When the CM gathers information or access to databases, this may increase the transparency and data protection of such processes, in that it is easier to carry out controls of what has been done/which information has been retrieved in these electronic databases.

5.2.1.1 SIS and other police (accessible) databases

The Schengen Information System (SIS) is a database available for the police and immigration authorities of the Schengen member states. The basic purpose of the SIS is "to maintain public policy and public security, including national security, in the territories of the Contracting Parties" (CISA Art. 93) This purpose should be seen in context with the Convention Implementing the Schengen Agreement (CISA)[29] Art. 39 when the SIS is

[28] The division between electronic and manual registers is also shown in the Europol Decision, where the information in the AWF data systems must be deleted after a certain time period, while manual files are not subjected to such rules (OJ L [2009] 325/14 Art.17).

[29] The Schengen *Acquis* consists of the Schengen Agreement of 1985, the Schengen Implementation Convention of 1990, the protocols and agreements on accession of Italy (1990), Spain and Portugal (1991), Austria (1995) and Denmark, Finland and Sweden (1996), the association agreements with Norway Iceland

employed for police purposes, underlining the obligation to assist the other Schengen Member States in the prevention and detection of criminal offences, i.e. what may be termed general police work. Counter-terrorism information has been part of the SIS framework since 2005 (Council Decision 2005/211/JHA)

SIS is very much like a national police register, and is taken in this report, to avoid overload of information, as an example of both this and of other international police databases. SIS shall contain information necessary to achieve the purposes of the Convention's articles 95- 100 (CISA Art. 94), i.e. information on wanted persons for arrest or extradition; third country nationals who are refused re- entry into Schengen; missing persons or persons who need to be put in police custody; people who shall receive summons, act as witnesses and similar in connection with criminal proceedings; data on vehicles or persons with the purpose of putting under surveillance; and finally data on objects sought for the purpose of seizure or for use as evidence in criminal procedures. It is, in other words, in many ways like an ordinary police database. The Schengen cooperation also obliges all overnight places (hotels, guesthouses, etc.) to take personal data from their guests, store this and submit it to the police upon request (CISA Art. 45) (see also the Joint Supervisory Board's 11-05 Opinion Article 45 (2011)) It is thus highly significant for the CM to assemble information from, also because SIS contains interlinked information such that may be particularly relevant in TACTICS. This may typically be that a person whose face is recognized on a CCTV resource is registered as wanted for a robbery, and there is available interlinked information on several missing guns used in the robbery, alongside description of modus operandi. Again, the access-possibilities to the various databases are crucial for the CM to consider. The purpose of the CMT is, as mentioned before, to provide knowledge about the capabilities at the security forces' disposal. When assembling information from SIS or other datbases, it is imperative that the restrictions related to who may, for which purposes, access the information in the later TM process. The 'pop-up' or other legal threshold functionality needs to be streamlined related to each database respectively. Both the threshold for registering and searching in the databases may be relevant for the CM to consider. It could for example be relevant for the TM to register an alert on a particular observed vehicle that is observed close to the site of a terrorist-attack. The SIS rules are briefly accounted for in the following, to serve as an example for what the CM will need to take into consideration when furthering information on the use of the capabilities of police databases, national or international, to the TM.[30]

Search and registration may only take place with the abovementioned purposes, as stated in CISA Art. 39. Further, only a limited group of individuals, when performing certain specific police tasks, has access to information in the SIS. The general rules of access follow from the CISA itself, but it is the structures and arrangements within the member states' legal and administrative system that regulate the specific access within their territory. Here, the Norwegian Act concerning the Schengen Information System is used as an example. According to this Act, the ordinary police in general have direct access to search in the SIS (sect.12), but only select authorised officials, and only when performing border control or "other control" functions ([1]a and [2]). There is an exhaustive list in sect.12(1), of which relevant actors for the CM are a) the police when performing border control and other control; and b) the public prosecutors. Other police authorities may *request* information from the register when performing other forms of control than border control. In addition to the use of national authorities, international organisations have a certain access, either directly or via national authorities such as liaison officers, based for example in CISA Art. 47 and in the EU Framework Decision of 2003 (OJ [2003] L 67/27) The access to e.g. national police registers and to SIS is made by e.g. a national police officer after the normal, national procedures, but the retrieved information may be employed in an international forum or mechanism. EU's police organization Europol also has access to the SIS (CISA Art.101A).[31] The access is, however, restricted to *search*, and is purpose- limited and restricted to certain types of data.

As a control measure enabling transparency and notoriety, all searches in the SIS must be electronically registered, both national searches (Art.103) and those of Europol and Eurojust. One of the challenges that have been raised regarding these organisations' use of the SIS is the possibility of sidestepping the initial restrictions. Europol and Eurojust may cooperate with third parties and relate to their own regulations regarding use of the retrieved information in SIS, for which the information was not originally meant (e.g. Boehm 2012 p.162 ff.) This could even be seen as a possibility for 'illegitimate coupling' of information from the SIS to other information databases or forums (e.g. Europol's own information and analysis databases) these agencies – but not the 'primary' users (i.e. the member states' police) – have access to. This problem

---

and Switzerland, and the decisions and declarations of the Schengen Executive Committee. While all documents are part of the Schengen Cooperation, the CISA is the reference document containing the applicable Articles for the police cooperation such as the SIS.

[30] For an in depth analysis, see e.g. Ugelvik 2014 ch.10.

[31] An extension by Council Decision 2005/211/JHA, in force from 2006 (OJ [2006] L 256/18).

is acknowledged and sought remedied in articles 101A [6b] and 101B [4], which prohibit connecting or transferring of data from the SIS to any other computer system, unless, for Europol, such use is allowed according to paragraphs 4 and 5 of the same article. In other words, the CISA sets up an immediate threshold that the CM must take into consideration when presenting the capability to the TM.

Art. 102 describes the purpose limitation principle, deciding that SIS alerts may only be used for the purposes laid down for each category for alerts referred to in Arts. 95-99. Any derogation from this principle should comply with the conditions set out in Art. 102(3). Any use of data which does not comply with Art. 102 is considered misuse under the national law of the Contracting Parties. A notable specification is that the allowed categories for SIS alerts that primarily relates to TACTICS, Art. 98, makes criminal proceedings a legitimate purpose for releasing such data, but does *not* mention *prevention* of crime. This implies in the case of TACTICS that the CM may not register alerts in SIS with terrorist preventative purposes.

5.2.1.2 Other databases

Other relevant international databases or access regulations into national databases are e.g. in the Prüm Cooperation (Council Decision and the Implementing Decision, OJ [2008] L 210/12). The Prüm cooperation implies that data should be readily available for law enforcement authorities across borders irrespective of which country it is located in.[32]This is obviously a significant resource and potential capability for the CM to assess when the relevant security personnel using TACTICS is within an EU Member State. The VIS (EU's Visum Information System) is another. VIS was established as an immigration control tool with the added particular purpose of "contribut[ing] towards improving the administration of the common visa policy and towards internal security and combating terrorism," with access, for example, for national police departments. The VIS is built up in the same way as SIS, consisting of a central unit for all visa information (Central- VIS), national units for every Schengen member, and a communication structure between these levels. Registered information is alphanumeric data on visa applicants, the applied and obtained/declined visa; photos; fingerprints; and references to previous applications; and fellow travellers of the immigrant. The search key is the fingerprints of the immigrant(s) in question, when such a search is necessary in the investigation of certain crimes (OJ [2008] L 218/60) Police may be allowed search in VIS when this is "necessary" in the sense that the police (MS police and Europol) have "reasonable grounds to consider that consultation of VIS data substantially will contribute to" achieving their tasks, such as counter-terrorism purposes using TACTICS. It is notable that in contrast to Prüm or SIS, only specified parts of national police or Europol organisations may have access. This is nationally specified, and for example in Norway, access may only be given to those with the responsibility of performing e.g. investigation with the purpose of preventing, investigating or unravelling acts of terror or other serious crime: in practice the Norwegian Police Security Service (PST) and the National Criminal Investigation Service (Kripos) (see Ot.prp.nr.36 (2008-2009) pt.7).

The above was a brief overview of the kinds of databases that may be resources and capabilities for the CM to consider assembling for the TM. The point is to show the possibilities and complexity of police and security personnel's access to such databases, which kind of information may be retrieved and registered, and how these databases extend outside traditional, internal databases. The general rules on interference in privacy etc. as mentioned above in sections 4.3 and 4.4 apply in addition to particular regulations both in the international legal documents themselves and in the national implementation regulations when these have been considered necessary. Additional legal aspects that the CM must consider are related to the interoperability of the databases. This issue is dealt with below in ch. 5.2.4.

5.2.2 Web crawling

Web crawlers are programs that automatically find and download web pages. According to Thelwall and Stuart, "web crawlers have become essential to the fabric of modern society. This strong claim is the result of a chain of reasons: the importance of the Web for publishing and finding information; the necessity of using search engines, like Google, to find information on the Web; and the reliance of search engines on Web crawlers to obtain the majority of their raw data" (Thelwall and Stuart 2006 p.1771). For the security forces, this is a powerful tool in achieving information on preparation or planning of e.g. terrorist attacks using online tools of various sorts. The web users do not normally notice crawlers and other programs that

[32] There are three databases for law enforcement authorities that amplified the information exchange through Prüm: A DNA Database network (with DNA profiles; a hit/no hit-system, meaning that if there is a hit, the registering country must be contacted for information); an Automated Fingerprint Identification System (AFIS) database network (fingerprint data, hit/no hit); and Vehicle Registration data network (direct access to alpha data).

automatically download information, which allows investigation to take place without their knowledge. This is thus a form of covert investigation that requires special attention to legal and ethical thresholds.

Privacy issues may appear clear-cut because in terms of web crawling, since everything on the web is in the public domain. Web information may still invade privacy if it is used in certain ways, principally when information is aggregated on a large scale over many web pages (Thelwall and Stuart 2006) The subjects, in this case publishers of the information are not aware of the possibilities of the crawlers. A plethora of virtual connections may make identification and traceability a very difficult task, in other words: Web crawling as a security method makes difficult the checking of whether the investigation has taken place according to applicable legal and ethical regulations. While the measures taken to counter terrorist attack are of high importance, and it thus might be necessary secretly assess web activities of suspects or larger groups of people to *find* a suspect, it is vital to balance the intrusion into the individual's private sphere in order to maintain legitimacy of the security personnel's activities.

5.2.3 Data mining

Data-mining may be defined as "a process that uses algorithms to discover predictive patterns in data sets" and "automated data-analysis [that] applies models to data to predict behaviour, assess risk, determine assosciations, or do other types of analysis" (DeRosa 2004). An essential and sometimes extremely difficult aspect of data mining and automated data analysis is finding the patterns and associations that have value—the ones that actually mean something (Taipale 2003). Data mining can be conducted over a number of databases of varying sizes, provided that certain very low size thresholds are exceeded to provide statistical validity (DeRosa 2004). Data mining may as such be part of a central capability in TACTICS, since a significant added value is precisely the coupling of several databases and resources to retrieve relevant information. For example, subject-based link analyses is a technique using aggregated public records or other large data collections to retrieve links between a subject such as a suspect of a terrorist activity, an address, a weapon registration number or some other relevant information, and other pieces of information. Link analysis is commonly used as an investigatory tool in national security and law enforcement investigation (*ibid* p.6).

A central legal and ethical challenge about data mining, in particular in for the TACTIC CM, is the collection and aggregation of information from several databases into one (temporary) single database that is run by TACTICS. Data aggregation involves 'cleansing' of the collected data, in order to standardize it, and eliminate unuseable or redundant data. The benefit of data mining is then that it may reduce false positives and negatives. This does, of course, hinge on that the aggregation is performed in an adequate manner. Both in external databases where the CM would draw information from, and in the (temporary) databases established during the CM process, it is vital that the information is validated regularly. Information may be outdated, from flawed sources, or deleted from the original source after a request from the individual in question. If TACTICS were through the temporary databases to breach with the regulations concerning storage and rights to access and deletion for registered subjects, either in national law or by international standards, this would imply serious breaches of civil and human rights.[33]

A particular challenge in counterterrorism instruments using data mining is, according to DeRosa, the challenge of finding patterns in relational data, because the terrorist activities are too rare to instigate broader patterns (DeRosa 2004 p.12). This is of course one of the core points of the TACTICS system-of-systems; that it, initially using the Global Terrorism Database (GDT), remedies the lack of data to find links between subjects, activities, etc.

A significant concern with data mining and automated data analysis is that the information may be interpreted faulty, and innocent people are stigmatized as "terrorists" simply because they engaged in unusual patterns of behavior or have some innocent link to a suspected terrorist. Bad data or imperfect analysis models may incur such results. This is thus also a question of data quality, because many records that are gathered from a variety of sources will often contain incorrect or obsolete information, which may lead to incorrect assumptions from the security forces (DeRosa 2004 p.15)

A counter-terrorist measure will often be enforced with great speed and perhaps less consideration because of the potential of great harm from the terrorist attack. In ordinary police investigation, data-mining results

[33] For work on reveal the information while still protecting sensitive data, there are several various methods including randomization, k-anonymity, data hiding and use of LBG design algorithm to preserve the privacy of data along with compression of data. For the latter, quantization is performed on training data that produces transformed data sets. This provides individual privacy while allowing extraction of useful knowledge from data, hence preserving privacy. See e.g. Aruna Kumari, Rajasekhara Rao and Suman 2014.

lead to more analysis or investigation, where false positives are detected before leading to intereference towards the individual. In preventive or mitigating counter-terrorism work, the techniques may be tempting to use as more than an analytic tool.

This may be an inherent risk in the data-mining and analysis tools, also for the CMT, since the situations almost always will be characterized by an emerging catastrophic situation. It is inevitable that the solution is a certain balancing-act. Data mining and analysis do not permit the government any greater access to personal data; they can only operate on data that the government already has. The advantage is that the existing data becomes more useful. An absolute requirement is that the gathering and storage of personal data is regulated by law.[34] One of the challenges at hand is then that the right to not incriminate oneself is put to the test. If information is given freely in an 'innocent' context, the challenge is whether it is acceptable that the information is used in an incriminating context without the person's knowledge. While this needs to be assessed on a case-to-case basis, it is vital that sufficient secure storage and deletion mechanisms are built in to the CM alerting system. While not yet developed, an alternative could be to have alerts or blockings pop-up after certain periods of time a data set has been stored in the (temporary) database. This could require the CM or TM to take action in considering whether the data should be removed, updated or to investigate whether there has been a request for access or deletion to the original data source where the CM has retrieved it.

Remedies and measures within TACTICS to protect data, allow necessary access and other human rights are targeted in D6.2.

5.3 Cumulative impact of the assemblage of information

The TACTICS CMT constitutes a powerful tool for the threat manager (TM) in assembling information on all possibly available capabilities. As mentioned above, the CMT does not in itself imply new capabilities. We have above seen the applicable general requirements for applying privacy intrusive measures, tools and capabilities. Another level of intrusiveness must also be discussed in addition to that concerning the individual resource or capability. The assemblage of capabilities may be seen as implying a significantly elevation of the level of invasiveness into a person's privacy (see D3.1). Some of the functionalities of the CMT assemblage are unproblematic in a data protection and privacy perspective. It follows in D5.5 that the main functionalities of the CMT are to:

- Provide storage, indexing, and query facilities for resource descriptions
- Provide algorithm, allowing for a matching general capability needs with actually available resources.
- Provide a query interface that allows retrieving resources of a certain type, near a certain geographic position or within a certain area with specific features.
- Provide detailed descriptions of resources. This will include position (geo-coordinates), type (e.g. CCTV, Number Plate Recognition, Officer), feature descriptions (resolution, night vision etc.), but also cost and other general QoS (Quality of Service) parameters.
- Provide actual resource status. This includes for instance the actual position of the resource, actual
status information (e.g. online / offline), and other information considered relevant for threat management.
- Provide access to resources (e.g. via network addresses/URLs) and/or credentials for accessing the actual data stream (e.g. video) of the resource (if technically feasible).
- Provide different views on resources, such as lists showing the actual operational status of a resource, layered maps that show actual positions of different types of resources, or combinations of these.
- Provide mechanisms to acquire resource information, e.g. by providing means to read resource information from structured text files (CSV, XML, JSON, etc.) or databases.

These resources, instrument and processes may, however, work differently when being connected. Combining multiple interfering measures and interoperability is targeted immediately below. First, however, processing of data for prediction is accounted for, where primarily localization data is emphasized.

[34] On the international level, for example ICCPR General Comment para.10, which also requires the States to protect such data by the implementation of "effective measures" to avoid unauthorized access or use in a manner contrary to the ICCPR. As with the European frameworks (above), access and control/deletion possibilities is also set out in the Comment.

5.3.1.1 Processing of data for prediction

Digital data can only be deleted if it has never been shared between different (online) devices, and only with certainty through the physical destruction of the carrier of the data. All digital data has thus what Hilst has termed an "inherent retentive character" (Hilst 2013 p. 75). This implies that maintaining control over digital data is difficult. A question to be asked is whether the right to privacy is less when data is voluntarily shared or generated. Location data, traffic data, electronic financial data, web-surfing data, Passenger Name Records (PNR) and Open Source Intelligence (OSINT) have many issues in common related to the discussion of their potential privacy interferences. The focus here is on location data.

While all the capabilities within this sub-section in themselves are mere lists or series of coordinates that give little information on a person, the coupling and/or the storage and analysis over time may provide an array of personal information. Passenger lists and hotel guest lists may provide information on when and where a person was, who he or she was sitting next to and/or travelled with. The localisation data from mobile phones etc. reveals the same, and also the habits and thus probable future movements of the person (e.g. González, Hidalgo and Barabási 2008). GPS coordinates give information on addresses, revealing organisation or religious fora that the person frequents. The level of details and intimacy level of this information put together, makes it sensitive information.

The Article 29 Working Group gave an opinion on the Geolocation services on smart mobile devices in 2011, where the clear point of departure is that the users of this technology shall have given consent if their geo data is to be used for purposes not specifically asked for by the user (http://ec.europa.eu/justice/policies/privacy/index_en.htm [20.11.14]) The following discusses analysis of localisation such as GPS and GSM data.Location data is as a point of departure 'innocent' data without inherently privacy intrusive aspects. Aggergated and combined, however, they may be revealing and thereby privacy intrusive (Hilst 2013 p. 143).

Location through mobile phones

Retention of location data gathered through the use of mobile phones was regulated in the EU under the Data Retention Directive (Directive 2006/24/EC). As mentioned above, the Directive is invalid after the CJEU ruling in Aparil 2014. Also Council of Europe instruments provide guidelines for the retention of such data, e.g. the Recommendation (2005)10 of the Committee of Ministers. The Recommendation Art.10 of the appendix, on the use of 'special investigation techniques' in relation to serious crimes, including terrorism, requires Member States to "ensure, to an appropriate extent, retention and preservation of traffic an location data by communication companies, such as telephone and Internet service providers, in accordance with national legislation and international instruments, especially the European Convention on Human Rights and the Convention for the Protection of Individuals with regard to Automatic Prosessing of Personal Data (ETS No.108).

Location through IMEI, IMSI

Pre-paid or pay-as-you-go mobile phone systems provide a customer with a phone and call credit are less traceable for security services because they are not (necessarily) registered with a contract on a particular person. Any phone still identifies itself when it connects to a mobile phone network. These identification codes may be intercepted by law enforcement personnel with IMEI Grabbers or IMSI Catchers. If the security personnel knows in which area a person of interest is located at a certain time, the codes may be used to identify the phone and thus the human target.[35]

ANPR

Automated Number Plate Recognition (ANPT) may automatically recognize which vehicles have been driving where at what time. ANPR is, similar to face recognition technology, CCTV technology enhanced with features that shall distil number plates from photos/videos of passing cars. Knowing just that a car has passed at a certain location at a certain time does not in itself provide information that in itself is particularly privacy intrusive. The usability of the ANPRN system depends on the ANPR database that the information is connected to. This will vary between countries, and there will often be a number of connected databases. This will typically be the database for stolen vehicles, motor vehicle insurance databases, and foreign registration databases (Hilst 2013 p.151)[36] For the CMT, this would of course be an added level of coupling, since the terrorist purpose in most cases would allow access to all of these databases. The lisence plate, or

[35] See more details in Hilst 2013 p.149.

[36] See more on the interoperability between databases also in ch.4.1.4.5 above.

connected registered data, can be 'flagged' for various purposes, e.g. that the car is wanted as evidence after a hit-and-run, or is registered on an immigrant wanted for expulsion from the realm.

The legal challenges related to ANPR primarily concern the retention of large amount of data also on people (often included in the ANPR photos) and liscences that have nothing to do with a criminal, let alone a terrorist offence. For the time being, the retention of these data varies between countries, e.g. for up to two years in UK and four weeks in the Netherlands (Hilst 2013 p.152)

Similar challenges arise concerning analysis of financial transactions and of billings (e.g. credit cards). The EU Commission have underlined that "terrorist finance threats change constantly, and vary greatly across customers, jurisdictions, products, delivery channels, as well as over time. This means that the response to financing of terrorism needs to be as supple as the terrorists themselves" (European Union (2008) Revised strategy on terrorist financing). Increase attention is therefore recommended. A well-known use of pattern-based searching involves credit card fraud (DeRosa 2004). Banks search databases of credit card transactions, some of which are known to be fraudulent, and determine, through data mining or otherwise, the patterns of fraudulent activity. A simple example of such a pattern is use of a stolen credit card for a small purchase at a gas station—done to confirm whether the card is valid—before making a very significant purchase. The banks then use these patterns to identify fraudulent activity in databases of ongoing credit card transactions and take steps to stop that activity. According to Amicelle, current practices of financial surveillance involve a range of different actors with different interests and know-how who now have to interact with each other.[37] Financial actors are obliged to verify the identities of their clients, to report 'suspicious transactions' to the police, to keep detailed records of their business relationships for a specified amount of time, and to respond to enquiries from competent authorities (see OJ [2005] L 309, Directive 2005/60/EC). he banks participate in security providing to the extent that they have not only to maximize but also to filter financial mobility, paralleling in a fashion 'the twin and apparently contradictory aims of the airport' in relation to the mobility of people and goods (Amicelle 2011 p. 162; Lyon 2007 p. 123).

Proactive logics, profiling techniques and practices of tracing financial flows may be problematic and unsuccessful in counter-terrorism, Amicelle and Favarel-Garrigues argue (Amicelle and Favarel-Garrigues 2009) An uneasiness of regulated institutions and the managerial focus on technological extrapolations from data may lead to principles of action that discriminate against particular groups or individuals. They support their argument on the Financial Action Task Force (FATF)'s guidance document (Financial Action Task Force (2007)), which declares that

> an over-zealous effort to counter the risks could be damaging and counter-productive, placing unreasonable burdens on industry, and act against the interests of the public by limiting access to financial service for some segments of the population.

The solution is then linked to new 'public–private' arrangements in the field of financial intelligence – that is, new forms of cooperation between professionals of security and professionals of finance to manage the 'risk' of terrorist financing, Amicelle suggests. In a TACTICS perspective, this means that the resources that may and should be gathered in the CM process stem from an array of sources that may be relatively unregulated and thus harder to check the notoriety of. This may, of course, be remedied to some extent with enhanced notoriety in the CM process, but the underlaying sources may be biased or otherwise flawed.

5.3.2 Combining multiple interfering measures

In the case of *Uzun v Germany (Uzun v Germany* Fifth Section (2010)), the ECtHR assessed the fact that the applicant had been subjected to *several* interfering measures as aggravating the interference. The applicant had been subjected to a multitude of "previously ordered, partly overlapping measures of observation. (…)". The person had been subjected to the same surveillance measures by different authorities, which implied, according to the Court, a more serious interference with his private life, in that "the number of persons to whom information on his conduct had become known had been increased" (*Uzun v Germany* paras 79-80). The rule of the Court has been interpreted thus that the severity of interference increases the more people have access to the data gathered by a privacy-interfering measure (Hilst 2013, ch.8.4.1.4.3) The *combination* preventive counter-terrorism measures is also seemingly aggravating to the privacy interference. The importance of developing a sound, detailed and complete data protection mechanism lies in that fragments of data may not have much of a meaning, let alone "sensitivity", when seen in isolation, but due to a never-ending increase in the interoperability and interconnectedness between the systems, each bit of information can potentially contribute to form a greater picture. Even fragments of information thus become potentially sensitive. This perspective does, however, not seem to have been taken

[37] See more on anti-money laundering and financial surveillance e.g. in Amicelle 2011.

very far by the Court, which instead has focused more on procedural aspects such as the existence and adequacy of safeguards of abuse (Hilst 2013 p.273).

This has two implications to the CMT. 1: Although the capability in itself, alone, may be deemed of little or acceptable privacy interference related to the situation in question, the assembling of the capabilities into the CMT increases the level of interference. This implies that an additional assessment of proportionality must be made related to the assemblage of the capabilities. 2: Since the number of people gaining access to the data, increases the level of interference, it is vital that the access to the assembled capabilities is limited and controlled. The safeguards/solutions are returned to in Deliverable 6.2. The added implications of *interoperability* of system-of-systems are also dealt with below in ch. 4.2.4.

5.3.3 Interoperability

In section 3.5.1 above, the report discussed the increase in interference into the private life of an individual when several intrusive measures were combined. Here, the increase in interference related to the interoperability between databases the CM may provide knowledge to the TM on. The focus here is on the interlinking of law enforcement databases and immigration control databases, or allowing police access to the latter for criminal investigation purposes. These serve as examples of a presumed general challenge for the CM in TACTICS, since the issues of these databases will be similar when the CM assembles knowledge of/from other administrative databases or databases with other purposes than crime control. Because of several shortcomings of SIS (II), VIS and Eurodac, including under-exploition of these, providing law enforcement authorities access to for example immigration databases, i.e. establishing interoperability between police and immigration authorities databases, followed the EU's Hague Programme. The reason was that "[i]mproved border controls and document security play an important role in combating terrorism" (EU Council Declaration on Combating Terrorism). The asylum, immigration and visa data that existed could before the change be used for internal security purposes (COM (2005) 597 final p. 4-7). Interoperability between various data systems was a key feature, defined as the "ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge"(COM (2005) 597 final p. 3). As such, TACTICS follows a lead that the EU has mapped out, in improving the functionality of various sources of information by combining them for security personnel in countering terrorism.

There are, however, some added challenges to privacy and data protection when making databases and systems interoperable. There are, for example, different regulations for the various systems regarding access and contents.

5.3.3.1 VIS

The Visa Information System (VIS) was established as an immigration control tool with the added particular purpose of "contribut[ing] towards improving the administration of the common visa policy and towards internal security and combating terrorism," with access, for example, for national police departments.[38] The police do, however, also have access to the immigration databases that do *not* have a crime control purpose embedded in them.

Traditionally, the police access to administrative databases such as immigration registers has been very restricted, and the two types of databases have been clearly separated. One of the reasons for the separation is the purpose limitation principle as was explained above (ch. 4.4.2.2), implying that information given or taken only shall be used for the initial purpose of which it was gathered. A primary concern is, according for example to Mitsilegas, that this 'blurring of boundaries' between databases containing information collected concerning 'innocent' and suspected/convicted people may decrease the scrutiny and democratic control of the use and application of the data (Mitsilegas 2009 p.246, and the EDPS Opinion 29.04.13, with reference to previous Opinions with similar concern of 2005; 2006; 2009 (fn.27)).

In the Schengen Information System (SIS), the registration of data is decided to a large extent by the Member State (MS) in question. In contrast, VIS implies a more stringent common policy since the open, borderless area is 'free' for all individuals. This in turn means that all MS' may be affected by other MS' visa (mal)practice. The information in VIS is wider than that in SIS, including for example information from the obligatory visa interviews. Information from such interviews used by the TM (or other security personnel) may imply a breach of the right not to self incriminate, emphasised *inter alia* by the ECtHR (Murray v. UK, (1996) para. 45). The Eurodac Fingerprint System was an EU immigration tool, but law enforcement authorities gained access in the new framework decision of 2013. The purpose of the database was

[38] According to the EU Justice and Home Affairs (JHA) Council in their preliminary conclusions (referred to by Mitsilegas 2009 p. 247).

originally only to facilitate the implementation of the Dublin cooperation, which regulates which country has jurisdiction over an asylum application.[39]

The following focuses on the types of information that can be found in these databases, and explores under which conditions the police, nationally and internationally, may retrieve this information.

The VIS is built up in the same way as SIS.[40] The Member States are obliged to register and transfer information on alphanumeric data on the applicant, the applied and obtained/declined visa; photos; fingerprints; and references to previous applications; and fellow travellers of the immigrant (IA sect.102 a-b).[41] The search key is the fingerprints of the immigrant(s) in question, when such a search is necessary in the investigation of certain crimes. The information available, in addition to fingerprints, is the same as in most such databases, i.e. names and personal details.[42] However, if there is a hit in the database after the police search, additional information may be supplied: photo and any other information in the visa application such as the abovementioned visa interview; and any commentaries noted in the application process. The police are, as with SIS, only permitted searches in the immigration database; not registering of e.g. a wanter notice.

The police may request access to information in the VIS concerning a person, on conditions that are similar to the legitimating of any measure interfering in an individual's personal life. This includes specificity of the search; the police may not 'randomly' or with risk-assessment purposes search more generally. This is an unlikely issue in TACTICS. The search must also be "necessary" in the sense that the police have "reasonable grounds to consider that consultation of VIS data substantially will contribute to" achieving their tasks as allowed in the VIS (OJ [2008] L 218/60 Art. 3(1); OJ [2008] L 218/129 Arts.4; 5(1)) This may be translated to the requirement of necessity. For the CM, the challenge is to establish whether or not the criminal procedure standard of 'reasonable grounds,' which is applicable since the TM access in question clearly concerns criminal measures, is met in the particular case having set TACTICS 'in motion'. The threshold for example in Norwegian law is explained similarly to the threshold for when the police may start a criminal investigation. This follows from the Norwegian Criminal Procedure Act sect.224 (1), and the criterion is interpreted to have three components: 1) the decision to investigate shall be factually justified; 2) the circumstances indicate with some probability that a criminal offence has been committed; and 3) that it is proportional, considering all elements in the situation, to subject the suspected person to investigation, and to employ investigative resources on the matter (Myhrer 2001; RA 99-238). The applicable crimes are terrorist offences and serious criminal offence. This implies "offences under national law which correspond or are equivalent to" the offences in the EU Terrorist Combating Decision Art.1-4, and the European Arrest Warrant (EAW) Art. 2(2) (OJ L [2008] 218/129 Art.2(1) c-d cf. OJ L [2002] 164/3 (amended in 2008) and OJ L [2002] 190/1)[43]

Both member state police and Europol may get access to VIS, but the access is limited to specified parts of the organisations. Norwegian law states that access may only be given to those with the responsibility of performing e.g. investigation with the purpose of preventing, investigating or unravelling acts of terror or other serious crime. The police access must be approved by the national VIS contact point, after a reasoned request. In urgent matters, which often will be the case in TACTICS situation mitigating an ongoing attack, information may be delivered without a prior legal assessment (but *post* checking for notoriety purposes). It

---

[39] The Dublin Regulation is also revised (from 2014) (OJ L [2013] 180/60), but the reference here is to the current OJ L [2003] 50/1. Dublin is part of the Common European Asylum System (CEAS) with general treaty basis in Art.78 TFEU.

[40] The system consists of a central unit for all visa information (Central-VIS), national units for every Schengen member, and a communication structure between these levels.

[41] The Norwegian Data Protection Agency expressed concern among others because of the taking of fingerprints of children (Ot.prp.nr.36 (2008-2009) pt. 6). 12 years of age is the minimum for registration of children's fingerprints. In the Eurodac fingerprint system, children from 14 years of age shall be registered (Norwegian Immigration Act 2008 sect.101; Immigration Directive 2008 sect. 18-5).

[42] In full: Name, sex, birthplace and -date; nationality; travel documents; data on the travel (purpose, duration, dates, arrival place or transit route); place of residence; fingerprints; visa data (type, number), identity on the person inviting or guaranteeing for the applicant (OJ [2008] L 218/60).

[43] 'Serious crimes' are those listed in the EAW article that are also punishable under national law with a custodial or detention order for a maximum of at least three years, e.g. participating in a criminal organisation; rape, forgery, racism and grievous bodily injury (OJ L [2008] 330/23 Art.4). For 'terrorist offences', see above in ch.3.2 fn.28.

may be notable that if the mitigation of a terrorist attack (also) concerns *border control* tasks, e.g. checking identification to establish the identity of a foreign-looking person, also ordinary police have purpose-limited access, but the access is purpose-limited (Norwegian Immigration Act 2008 sect.102c)[44] It is, in other words, a complicated picture of the possibilities for the police to access the initially non-criminally related databases.

5.3.3.2 Eurodac

The general rule of Eurodac is that *all* asylum seekers aged 14 years and over, and every non-EU citizen or citizen of a non-Eurodac member state who crosses these borders illegally, or whom are found illegally present in the realm, shall have his/her fingerprints taken (OJ [2003] L 50/1 Art. 4). The fingerprints are then sent from the member state to the Central Eurodac System, where the prints are checked against previously transmitted prints from any member state, to check whether and where the person has applied for asylum before, and therefore should be dealt with in accordance with the Dublin agreement (Arts. 3-10). The final identification of data, i.e. the linking of the fingerprints and the individual, is the responsibility of the member state alone (Art.4[6]); it works in other words as a hit/no-hit system. There are no articles giving access to the police to the Eurodac in the original Eurodac Council Regulation, but this is changed in the new Regulation, which in force from 2015 (OJ [2013] L 180/1). Eurodac has only been accessible for asylum purposes. The new Regulation, however, gives member states' police and Europol access to compare fingerprints (alone) in criminal investigations with those registered in Eurodac. Only designated national authorities (and similar separated authority in Europol [Art.7]) are authorised to request comparisons with the Eurodac data, when there is "substantial suspicion" to believe that a person has committed or will commit crime, and the information in Eurodac is necessary for the "prevention, detection and investigation of serious crimes and terrorism" (*Op.cit.* arts.5-7 cf. Art.1(2); quote from the preamble (13)). [45] Only a specific verifying authority of the police may, as with VIS, request access to Eurodac via the National Access Point, confirming that all conditions for comparison in Art.20 or 21 are met (Art.6 no.2 cf. Art.19). There are urgency procedures allowing the conditions to be checked ex-post, but never outside of the verifying authorities' channel (Art.19[3]).

Specific safeguards are implemented in the conditions. In contrast to VIS access, Eurodac access requires that the law enforcement authorities shall have exhausted all available criminal records databases, in addition to the Prüm and the VIS databases (Art.20[1]).[46] The search may only concern specific, singular cases, and it must be a last resort for the police (Art.20 [1]a and b). The searches should be delimited to those suspected only of the most serious crimes such as murder and terrorism, since these "mean[…] that there is an overriding public security concern", which makes the police's access to the database proportionate (*op.cit.* a). The final condition is that there must be "reasonable grounds" to believe that such a comparison will "substantially contribute" to the prevention, detection or investigation of the offences in question (*op.cit.* c). The reasonable grounds are specified in the article as present when there is "as substantiated suspicion" that a search may lead to findings in a category of the Regulation concerning perpetrator, victim or suspect of the relevant crimes.[47]

---

[44] It does not, in other words, function in a way that the police generally may freely search in *the* VIS; search is both purpose and necessity limited, and is performed via other centralised authorities that, in the case of hits, deliver the requested data material to the requesting police.

[45] The applicable crimes are those listed in the European Arrest Warrant (OJ L [2002] 190/1) and the Council FD on combating terrorism (OJ L [2002] 164/3), *if* they also are punishable in national law with maximum three years imprisonment or more, cf. Art.2(1)j; k. The authorities with exclusive responsibility for "intelligence relating to national security" shall not have access (Art.5[1]). The law enforcement competences are also divided into the *designated (law enforcement) authorities* and *verifying* authorities. These act independently, without instruction possibilities from the former to the latter (Art.6[1]). It may be within the same unit, but act independently (Art.6[1]). The arrangement is, in other words, like with the VIS access; there is a strict divide into a two-instance access system, implying an extra 'barrier' between the administrative and the policing 'tracks' of search.

[46] The Prüm search may be avoided if there are "reasonable grounds to believe" that such a search would not lead to an identity establishment (Art.20[1]).

[47] Europol's access conditions to Eurodac are set out in Art.21. They are only slightly different from those of the member states in arts.19-20. New access from 2015 (OJ L [2013] 180/1). See for details e.g. Ugelvik, S *op.cit.* 2014 chapter 10.3.2.2.

5.3.3.3 Objections to the interoperability

The preamble to the regulation emphasises that the purpose of Eurodac is changed in manner that "interferes with the fundamental right to respect for the private life of individuals whose personal data are processed in Eurodac." The standard requirement in EU documents is that the measures should be in accordance with laws that are sufficiently clear and with foreseeable outcomes, alongside the requirement that any interference has to be "necessary in a democratic society to protect a legitimate and proportionate interest and proportionate to the legitimate objective it aims to achieve."[48] The seriousness of such crimes satisfies the requirement of proportionality (Eurodac 2013 preamble [10]). It is specifically emphasised in the preamble that since this search by law enforcement authorities is happening in registers containing information about people with a clean criminal record (13) and on persons who are not presumed to have committed a terrorist offence or other serious criminal offence (15), the safeguards are particularly important. Another personal data-related safeguard is in Art. 22(1-2); specifying that all communication shall be secure and electronic (e.g. phone contact is not permitted), securing the processing track-record for control purposes.[49] All these safeguards must naturally be linked to the capability in the CM process, if the TM is to gain access to the datbases and use the information.

Traditionally, the police access to administrative databases such as immigration registers has been very restricted, and the two types of databases have been clearly separated. One of the reasons for the separation is the principle of purpose limitation, implying that information given or taken only shall be used for the purpose of which it was gathered. A primary concern is, according to e.g. Mitsilegas, that this 'blurring of boundaries' between databases containing information collected concerning 'innocent' and suspected/convicted people may decrease the scrutiny and democratic control of the use and application of the data (Mitislegas 2009 p. 246. See also the EDPS Opinion 29.04.13, with reference to previous Opinions with similar concern of 2005; 2006; 2009 (fn.27)). In other words: When a person gives information to an administrative body, e.g. the Immigration authorities, the person shall, to a far-reaching extent, be able to trust that this information is only used with the purpose he was informed of, within the purpose of the receiving entity (e.g. an asylum decision).

The information databases accounted for, VIS and Eurodac, both have a strict division between the 'local' and 'central' levels. All searches must go through a national control entity. The CM assessment of these capabilities will depend on whether there is a police human resource that may have (facilitated) access or not. In general, it must be noted that police access is subject to strict requirements of necessity and specific purposes of serious crime control, in contrast to the case with SIS access, where more ordinary police tasks (public order, etc.) are sufficient.

In the final part of this report, the ethical issues of TACTICS CMT are discussed.

---

[48] Peers criticises the Eurodac for already being in breach with the purpose limitation principle of data protection law (i.e. giving access to the data only for the purposes it was originally collected for) because of too lengthy retention of the data (2011 p. 366).

[49] There are specific data processing and protecting measures in ch.VII of the Regulation. For detailed discussion on Eurodac with particular focus on data protection and human rights, see e.g. Karanja 2008:265-279.

6 Ethical issues of TACTICS CMT

Technology is never inherently good or bad; its impact depends upon the uses to which it is put as it is assimilated into society (DuGay *et al.* 1997). The word “ethical” means relating to or being in accord with approved moral behaviours (Chambers 1991). The word approved places this definition firmly in a social context. Behavior can be considered ethical relative to a particular social group if that group would approve of it (Thelwall and Stuart 2006). When developing a system such as TACTICS, that may be implemented in various jurisdictions and developed differently after this research project ends, it is difficult and maybe even unwanted to try to establish a general notion of which use of the system is unethical. The cultural, social and legal context may vary to the extent that a common notion is impossible. Still, the system is developed within the EU framework, and thus requires at least the research project to take as point of departure a high ethical standard related to commonly approved within the EU Member States.

6.1 General ethical awareness

It is an open question whether the CMT via the CM itself should apply a general ethical awareness in chosing the capabilities to present to the TM. (See for details on the process in D5.2 p.7 ff.) In the CM process, security capabilities are systematically collected (step 1) and described (step 2). It follows that the capabilities presented to the TM should be characterised both by its technical, financial, geo-spatial and quality-of-service *and* ethical attributes, as well as “attributes related to the appropriateness of the capability for detecting currently known signs” (*ibid*). The output of the two steps is a prioritised list of capabilities configurations matching the scenarios.

The CM provides the capabilities and resources to be proposed to the TM, while the TM decides whether and how the proposed capabilities and resources may actually be used. As seen above, there are many legal thresholds and requirements related to the various resources, capabilities and coupling of capabilities. A central characteristic of most of them is that the assessment of whether the use of them meets these thresholds and requirements is a complicated one. It is impossible to automatically assess whether employing three CCTV cameras, one police officer and a police dog does or does not constitute an unproportional infringement into a person’s privacy. The question is thus whether the CMT opens up for too open a choice for the TM without the sufficient alert to the legal and ethical limitations of the choices. In addition, once the capability is collected and presented to the TM, it may be practically highly improbable that the TM would *not* employ this in a situation where a terrorist attack is under way. As such, one could envisage that the CM process was differentiated between the applicable situations. In the situations where there a terrorist attack is in process of happening, the thresholds for state interference in the individuals’ rights is far lower than in other situations. In situations where the attack has not yet happened, or during the investigative stage *after* a terrorist attack, the threshold will generally be higher. The question is whether these thresholds are sufficiently implemented in the CMT particularly and TACTICS in general.

The CM is a human professional who is in control of and responsible for matching capabilities and resources with the needs expressed from the TM. The CM thus also needs to make a choice between a large number of capabilities to provide to the TM. Section 2 in D5.2 analyses the rationalities of decision making. Here, it suffices to point at the possibilities of the CM’s potential wish to over-achieve towards the TM, since the matters at stake (anti-terrorism) have great potential negative effects. This may affect the ethical assessment, or at least imply that the CM rather has the TM making the choice on whether an accessible capability which may have seriously privacy infringing or unethical consequences, but at the same time *could* prove valuable in the threat mitigation. In the current status of the development of TACTICS, there does not seem to be any absolutely clear solution to this challenge. The conclusion must be that the decision-making on both the CM and TM level is as informed as possible, based on a set of information concerning the capabilities and resources which includes a strong emphasis on a consideration involving the permissible limitation test as well as the particular legal requirements following the measure.

In an extensive analysis, RAND Corporation suggests six main types of tools or methods that may support ethical decision-making in counter-terrorism activities (Reding *et al.* 2014):

1. Mitigation methods to reduce the likelihood of certain ethical problems arising and/or of certain situations leading to unethical decision-making.
2. Professional development methods to cultivate individuals’ capacity to identify, reflect on and respond to ethical problems.

3. Guidance methods to provide professionals with an easily accessible reminder of the law, policies and norms of their institution.
4. Leadership methods to reinforce ethical practice in the organisation, including leadership by example and direction from superiors.
5. Advice methods to ensure that there is an independent check on the ethicality of decisions in place.

Each of these categories may be applied using a range of tools. Advice methods may include tools such as ethics consultants, legal advisors, peer support and ethics committees. These ethics tools may seem less relevant during an ongoing terrorist attack. It is, however, vital that both 'background' or underlying ethics methods *and* 'emergency' or imminent ethics tools are part of the TACTICS and CM. Without the background training of the users of TACTICS, they may not be able to identify, reflect on and respond in an ethically appropriate way when assessing the capabilities, their matching and furthering of information 'in the heat of the moment'. As is also pointed out in the RAND analysis, the tools used by professionals to address ethical problems vary greatly between sectors and countries. This serves to emphasise that the ethical guidelines set out in the TACTICS project only may be just that, overall guidelines. These must be taken into account but also elaborated and advanced within the national contexts upon implementation of the system-of-systems.[50]

6.2 The broader picture of security policies in a societal perspective

The urban characteristics and issues related to terrorism in urban environments are accounted for and discussed in in D4.3. There are, however, some particular features also related to the CMT that concerns the urban characteristics, and that should be discussed in an ethical assessment. Ethics are integral to the field of balancing privacy, liberty, security and general human rights when making decisions in counter-terrorism acitivites.The professionals involved in the capability and threat management processes must be proficient in making decisions that are both accurate, efficient and ethical. In TACTICS, it is part of the capability management to characterise the capablities' ethical attributes, e.g. level of privacy, when establishing the appropriateness of the capability in the situation in question (see D5.2).

The German Constitutional Court noted in a 1983 judgment that "a person who wonders whether unusual behaviour is noted each time, and thereafter always kept on record, used or disseminated, will try not to come to attention in this way ... This would ... limit the ... common good, because self-determination is an essential prerequisite for a free and democratic society that is based on the capacity and solidarity of its citizens." The idea of "panopticism" is that surveillance "fosters well-adapted, peaceful, disciplined behaviour" and ultimately deters demonstrations and other disorderly behaviour (Ullrich and Wollinger 2011)

In response to security fears, rich-world governments are analysing and exchanging ever-greater quantities of information on their citizens, using data mining tools to identify individuals "of interest". In the near future, it will be so easy to put everyone under digital surveillance that it could easily become the default position. This includes international cooperation between public authorities aimed at identifying suspected football hooligans, illegal or trafficked migrants, political activists, terrorists and paedophiles. Being given any of these labels by any authority, in any country, can quickly lead to such a stigma becoming all-pervasive, without it being possible to challenge the body that initially made the mark.

6.2.1 Future consequence: Re-defining of resources

The capabilities management tool presupposes the categorisation of various clusters or combination of resources. The TACTICS system is only to be set in motion with the purpose of mitigating serious terrorist activities. With the purpose limitation related to terrorist threats, a potential consequence of the TACTICS system and CMT in particular, is that far more 'ordinary' resources may be reframed as counter-terrorist measures. One could for example imagine that the CCTV cameras in general grocery stores or even connected to private homes are labelled as counter-terrorist resources, in order to generate them into the CMT. While it is not in itself problematic that the police get access to such kinds of measures in order to mitigate a terrorist attack, the reframing and matching of all possible resources may lead to a far higher general level of surveillance with a potentially too swift stroke of a pen. It is impossible at the present stage to pre-consider the impact of connecting absolutely all kinds of potential resources in society.

[50] Reding *et al.* find for example that so-called moral-case deliberation is well-established in the Netherlands, but hardly known in the United Kingdom. Also the level of ethics training among professionals varies greatly between countries – whether it is formal, practical or at the heart of the curriculum (2014 p.xvi).

6.3 Extension of the system

It follows in D5.2 that the TACTICS CMT tool may be considered extended in various directions. The end-users envisage for example incorporating crowd-based or social networks as sources of information and as means of steering behaviour. The suggested extension of the system may serve to symbolise two transversal issues that are ethically challenging for the TACTICS system.

One concerns the future implementation of TACTICS. The current TACTICS design targets terrorist situations alone. However, as the end-users suggest, the system is already before ready researched envisaged with greater possibilities for the security personnel. An important aspect to point at in this stage of the system development is therefore that there may be ethical consequences of the system that are not yet visible. TACTICS may easily be redesigned to target for example property crime, or loitering or similar lower-scale crimes or disorder problems. This is of course a development that will have to be dealt with in due time by the national authorities respectively, since it proably would raise additional questions related to implementation of legislative regulations and thresholds. The possibility for establishing a system that easily may be redesigned for other purposes is, however, a challenge that should be discussed already at the initial research stage. Both the possible change in purpose and the effect of TACTICS as 'a system of systems' need evaluation.

The description of the Threat Management and Threat Management Tool in WP6 shows that the overall function of the system is 'on the move' towards greater system of systems functionality. Section 3 in D6.5 shows the interoperability between the functions of TACTICS (TMT, TDT and CMT).

The *other* transversial issue concerns the pre-prototype phase of the ethical assessment of the system. TACTICS is in a pre-prototype phase. The system as a whole requires customisation into the national jurisdiction it may be implemented in. This means for any phase of the system development, new legal and ethical issues will arise. It is thus important to emphasise that the ethical and legal assessments made in the current research project may not be considered *final* such assessments. The implications of a finalised TACTICS system implemented in national jurisdictions are impossible to pinpoint at the present stage.

7 Conclusions

In this report, we have described the most relevant challenges related to the TACTICS CMT concerning legal conditions, ethics, human rights and privacy (LEHP).

The relevant international legal instruments that need to be taken into account when using the CMT were accounted for in the first part of this report, and specifically the legal thresholds that are applicable for all the resources and capabilities dealt with in TACTICS. Related to the overarching data protection principles, the report suggests implementing the permissible limitations test into the CM process (section 4.3.2). This test requires all collection and transfer of personal data in TACTICS to take place according to a set of general pdata protection and privacy principles. The suggestions for future, factual TACTICS systems-of-systems follow immediately below, but first, a brief sum-up of the general requirements that was underlined in this report. Personal data must be fairly and lawfully processed, following a clear legal basis; collected for specific, explicitly defined and legitimate purposes; and not further processed in a way incompatible with those purposes; retained only as long as is necessary to fulfill that purpose. The CM must assure that the data is is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed, and must regularly check if the data are up-to-date and accurate. The data should be anonymized in the extent necessary, or be subject to consent from the data subject. For the general use of the system, regular checks should be performed to ensure that the CM processes follow these requirements. It is vital that the system warrants notoriety and traceability of all data collection and processing, so that such checks may be performed. The collected data into temporary TACTICS databases must be securily stored, meaning that its processing will be done in a confidential and secure manner. There should be strict access thresholds, in that only designated security personnel should have access to the data, with heightened level of access control depending on the type and extent of data. Transfer to foreign jurisdictions must not take place without proper ensurance of adequate local levels of data protection. National data supervisory authorities must be notified before carrying out any wholly or partly automatic processing operation.

The challenge of invasiveness following the combining of multiple interfering capabilities/measures was also discussed. Making use of several kinds of information about a person may induce another level of invasiveness than when used isolated. The discussion of this effect was intended to assure that privacy, ethical, democratic and legal aspects are embedded into the CMT when it will be implemented in national jurisdictions.

The report's section four was dedicated to analyzing the LEHP aspects of the most central specific capabilities that the CMT may collect and provide to the TM.

The final part of the report, section 6, has analysed the ethical issues related to the CMT. The primary ethical concerns relate to the general ethical awareness of the usage of the TACTICS CMT, and of the future extension of TACTICS as a system to other areas of society than that of counter-terrorism. This is a clear wish of the end-users (see e.g. D5.2 p. 30). While this is not possible to assess at the present time, a particular concern of the future use of TACTICS CMT is that all ordinary resources in society will be redefined as counter-terrorism resources to be able to be applied in greater system-of-systems. Such potential redefining of all resources and capabilities may lead to connections and have impacts on the general level of surveillance and total potential police control in the society that are impossible to pre-consider.

Of the most important guidelines for the TACTICS system as a whole, the most relevant for the CMT are listed in the following, to conclude the report.[51] More detailed legal requirements must be implemented particular to the country in question upon final implementation of the TACTICS system in national jurisdictions. These legal requirements must build on and take into account the international standards on human rights, including those presented in this report. This report should be seen as a building block in developing a tool where these requirements are implemented. In the following bullet-points, the most relevant requirements and thresholds are expressed:

- Rules must be established that permit and govern the use of a TACTICS-like system in law, using the most appropriate instruments and providing all the adequate safeguards. Judicial and administrative overview and redress should be ensured.

[51] As follows also from D 2.1 pp.18-19. Some of these requirements will be followed up on in D6.2.

- There should be explicit limitations as to the scope of the TACTICS system in terms of aims (counter-terrorism only), geographic reach (urban area as reduced as possible), use (*ad hoc* activation for a specific amount of time, no standby or continuous running), access (restricted and monitored access to the information system). This may ensure that the CM process does not involve capabilities that do not meet the applicable requirements.
- CMT process-wise, a 'variable geometry' system should be implemented in the tool, with an explicit threshold to its full use and intermediary steps where the most intrusive functionalities are un-locked only if strictly needed and under stricter conditions. Progressively restrict access to the most sensitive functionalities to mitigate the risk of abuse or data breaches.
- Upon national implementation, there should be established a clear chain of supervision and responsibilities of the CMT process. The decision of deploying and activating the system, both ordinarily and in the field, should be taken under strict criteria, and accountability of this decision should be ensured, alongside possible judicial review.
- Transparency and checks of the process should be guaranteed by ensuring that records are kept of all the different steps of deployment and of the information justifying further use. Traces of logging should be kept and regularly checked. Abuse should be punished.
- Next to a formalized procedure of external review (preferably after each use of the system), and internal auditing system should be considered. In this sense, the appointment of a data protection officer could ensure a more tailored use of the system without hampering law enforcement needs and specific practices.
- Avoid the establishment of new *lasting* databases. Ensure that the collected and processed data are stored in a secure environment, and foresee a very short period of data retention. After each use of the system, ensure that all data that are not needed in judicial procedure are erased as soon as possible and, in any case, within explicit time-limits. The principle of data minimization at both the level of data collection and data processing. The need to retain any data should be properly justified and all the necessary steps to anonymize them should be taken.
- Depending on national regulations, the CMT may access different types of sensitive data . Prior to implementation, there should be a precise clarification of which personal data that may be processed in the CMT. Enhanced technical, organizational and legal safeguards should be provided. Introduce state of the art systems to avoid collecting these data, or filter them if collection is not avoidable because of structural constraints. Explicitly prohibit the use of ethnic profiling and clearly describe the core operations of behavioural profiling.
- Identify clearly what the system sources are and the quality and reliability of the related data. Access to each data source should be properly justified and its (expected) added value should be stated and, later, assessed.
- Given the likely exceptional use of the system (rare but particularly intrusive), it is advisable to schedule a comprehensive review after each use of the system. This kind of assessment could increase the quality of the system both in terms of respect of fundamental rights and efficiency and effectiveness. Furthermore, the trust of the public in the proper use of the system and in the behaviour of law enforcement authorities could be further strengthened by such reviews.

8 List of acronyms

CMT	Capability Management Tool
GTD	Global Terrorism Database
CM	Capability Manager
TM	Threat Manager
TDM	Threat Decomposition Manager
MA	Morphological analysis
ECHR	European Convention of Human Rights
ECtHR	Court of the European Convention of Human Rights
CFREU	Charter of Fundamental Rights in the EU
CJEU	Court of Justice of the EU
DPD	Data Protection Directive
Convention 108	Council of Europe Convention no.108
ICCPR	International Convenant on Civil and Political Rights
LEHP	Legal, ethical, human rights and privacy
UN	United Nations
TACTICS	Tactical Approach to Counter Terrorists in Cities (FP7 project)
TDT	Threat Decomposition Tool
TMT	Threat Management Tool

9 Bibliography

Amicelle A and Favarel-Garrigues G (2009): La lutte contre l'argent sale au prisme des libertés fondamentales: Quelles mobilisations? *Cultures et Conflits* 76(3): 15–42

Andenæs, J (1998): *Statsforfatningen i Norge.* Oslo: Tano Aschehoug

Aruna Kumari, D, Rajasekhara Rao, K, and Suman, M: "Privacy Preserving Data Mining", In: *Advances in Intelligent Systems and Computing* Volume 249, 2014, pp. 517-524.

Bellanova, R (2014): *The politics of data protection: What does data protection do? A study of the interaction between data protection and passenger name records*. Université Saint-Louis – Bruxelles and Vrije Universiteit Brussel.

Boehm, Franziska (2012): "Information sharing and data protection in the Area of Freedom, Security and Justice". In: Gutwirth, S *et al*. (eds): *European data protection: In good health?* Dordrecht: Springer

Bygrave, L (2014): *Core Principles of Data Privacy Law.* New York and Croydon: Oxford University press

Chambers (1991): *Chambers concise dictionary*. Edinburgh: W & R, Chambers Ltd

De Hert, P (2005): Balancing Security and Liberty within the European Human Rights Framework. A Critical Reading of the Court's Case Law in the Light of Surveillance and Criminal Law Enforcement Strategies after 9/11. *Utrecht Law Review* 1 (1): 68-96

De Hert, P, Papakonstantinou, V, and Riehle, C (2008): "Data protection in the third pillar: cautious pessimism". Maik, M (ed.): *Crime, rights and the EU: the future of police and judicial cooperation.* Justice: 2008

DeRosa, M (2004): *Data Mining and Data Analysis for Counterterrorism*, CSIS Press (https://cdt.org/files/security/usapatriot/20040300csis.pdf [20.11.14])

DuGay, P., Hall, S., Janes, L., Mackay, H., & Negus, K. (1997). *Doing cultural studies: The story of the Sony Walkman.* London: Sage

Eckhoff, T and Smith, E (2006): *Forvaltningsrett.* Oslo: Universitetsforlaget.

European Digital Rights papers (2013): *An Introduction to Data Protection* (EDRi report)

Fetzer, P.L. (2003), "Nothing to Hide, Nothing to Fear", in *Moebius Journal 1 7*

Financial Action Task Force (FATF) (2007): *Guidance on the risk-based approach to combating money laundering and terrorist financing: High level principles and procedures*. Paris: FATF

González, M.C., C.A. Hidalgo and A.-L. Barabási (2008): "Understanding individual human mobility patterns", *Nature,* 453, 479-482

Harris *et al* (2009): *Law of the European Convention on Human Rights*, Oxford: Oxford University Press

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

Hoffman, B (2002): "Rethinking Terrorism and Counter-Terrorism since 9/11". In: *Studies in Conflict and Terrorism,* 25, pp. 303-316

Reding, A, *et al.* (2014), *Handling ethical problems in counterterrorism: An inventory of methods to support ethical decisionmaking*, Cambridge and Brussels: RAND Europe, p.xvi.

Rosenfeld, M (2008): "Judicial Balancing in Times of Stress". Bianchi, A and Keller A. (eds): *Counterterrorism: Democracy's Challenge*. Oxford: Hart

Joseph, S, Schultz, J and Castan, M (2004): *The International Covenant on Civil and Political Rights: Cases, Materials, and Commentary*, 2nd edn. New York: Oxford Univ. Press

Lock, T (2012), "End of an Epic? The Draft Agreement on the EU's Accession to the ECHR", *Yearbook of European Law*, (http://ssrn.com/abstract=2103514 [17.11.14]

Lund, Ketil (1996): *Rapport til Stortinget fra kommisjonen som ble nedsatt av Stortinget for å granske påstander om ulovlig overvåking av norske borgere (Lund- rapporten)*. Oslo: Stortinget

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

McBride, P (2009): "Beyond Orwell: the application of unmanned aircraft systems in domestic surveillance operations". In: Journal of Air Law and Commerce 2009, 74 (3), pp.627-62

Mitsilegas, Valsamis (2009): *EU criminal law.* Oxford: Hart

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

Myhrer, Tor- Geir (2001): "Etterforskningsbegrepet". *Tidsskrift for Strafferett.* 1 (1), 6- 30

O'Neill, M (2012): *The Evolving EU Counter-Terrorism Legal Framework.* London and New York: Routledge

Peers, Steve (2011): *EU justice and home affairs law.* Oxford: Oxford University Press.

Reid, K (2007): *A Practitioner's Guide to the European Convention on Human Rights*, 3rd edn. London: Sweet & Maxwell

Sambei, A, Polaine M, Du Plessis, A (2009): *Counter-Terrorism Law and Practice: An International Handbook.* Oxford University Press

Schmid, A (2011): "The Problem of Defining Terrorism". Schmid, A (ed.): *The Routledge Handbook of Terrorism Research*. Abingdon: Routledge

Taipale, S (2003): "Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data," *Columbia Science and Technology Law Review* 5 (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=546782 [20.11.14]

Thelwall, M and Stuart, D (2006), "Web Crawling Ethics Revisited: Cost, Privacy, and Denial of Service", In: *Journal of the American Society for Information Science and Technology,* Volume 57, Issue 13, pp.1771-9

Tranberg, Charlotte Bagger (2011): "Proportionality and data protection in the case law of the European Court of Justice". In: *International Data Privacy Law*, Vol. 1, No. 4, 2011, p. 239-248

Troncoso Reigada, A, (2012) "The Principle of Proportionality and the Fundamental Right to Personal Data Protection: The Biometric Data Processing." In: *Lex Electronica* 17 (2): 1-44

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

Ullrich, P. and Wollinger, G.R. (2011) A surveillance studies perspective on protest policing: the case of video surveillance of demonstrations in Germany. Interface, 3(1), 12–38

UN Human Rights Committee (2003): "General Comment 16", *Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies (*Twenty-third session, 1988), U.N. Doc. HRI/GEN/1/Rev.6 at 142 (2003).

Vermeulen, M and Bellanova, R (2012): "European 'smart' surveillance: What's at stake for data protection, privacy and non-discrimination?" In: *Security and Human Rights*, Vol. 23, No. 4, 2012, pp. 298-311

Wright *et al* (2010): "Sorting out Smart Surveillance". In: *Computer Law & Security Review*, 2010, vol. 26, no.4

Zedner, L (2007): "Pre-Crime and Post-Criminology?" 2007, 11 Theoretical Criminology

Conventions, treaties, directives, opinions, etc.

COM (2014) 207 final: *A new era for aviation, Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner.*

Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders. OJ L 239.

The Hague programme : strengthening freedom, security and justice in the European Union (16054/04), Brussels, 13 December 2004

OJ [2012] C 326/391 Charter of Fundamental Rights of the European Union (2012/C 326/02, CFREU)

COM (2005) 597 final Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs (Brussels, 24 November 2005).

Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950.

Convention for the Protection of Individuals with regard to Automatic Prosessing of Personal Data (ETS No.108), Strasbourg 28 January 1981

OJ [2009] L 325/14 Council Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules for Europol analysis work files

OJ [2009] L 121/37 Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA).

OJ [2008] L 210/12, (Prüm) Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross- border cooperation, particularly in combating terrorism and cross- border crime.

OJ [2005] L 68/44, Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including the fight against terrorism.

OJ [2002] L 164/3 Council Framework Decision on combating terrorism

OJ [1995] C 316/1, Council Act of 26 July 1995 drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention).

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data.

OJ [2005] L 309, Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

OJ [2013] L 180/60 Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (recast) [Dublin II, in force 1 January 2014].

Opinion of the European Data Protection Supervisor (EDPS) on the Communication from the Commission to the European Parliament and the Council on “A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner”, Brussels, 26 November 2014.

OJ [2002] L 190/1 European Arrest Warrant

Joint Supervisory Board’s 11-05 Opinion Article 45 2nd March 2011 on the Systematic verification in the National Schengen Information Systems (SIS) of guests staying in Schengen State hotels: compliance with the Schengen Convention (http://schengen.consilium.europa.eu/media/201436/11-05%20opinion%20art.%2045.en11.pdf [14.01.15].

OJ [2008] L 218/60 Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short- stay visas (VIS Regulation).

Ot. prp. nr. 36 (2008- 2009) *Om lov om endringer i utlendingsloven 1988 og utlendingsloven 2008 (gjennomføring av forordning nr. 767/2008 og rådsbeslutning nr. 633/2008 vedrørende visuminformasjons systemet VIS) mv.*

Regulation (EC) No 216/2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/E, 20/02/2008

RA 98 Directive of 22 December 1999 (RA 99/238): Del II no. 3 Etterforsking (Norwegian Director of Public Prosecutions)

European Union (2008) Revised strategy on terrorist financing. Note from Counter-Terrorism Coordinator to COREPER/Council p.2 (http://register.consilium.europa.eu/pdf/en/08/st11/st11778-re01.en08.pdf [14.01.15]

UN High Commissioner for Human Rights, Fact Sheet no.32 (http://www.ohchr.org/Documents/Publications/Factsheet32EN.pdf [18.11.14].

UN International Covenant on Civil and Political Rights (ICCPR), New York, 16 December 1966

UN Convention on the Offences and Certain Other Acts Committed on board Aircrafts (1963), Tokyo 14 September 1963, ICAO Doc. 8364/704

UN Convention for the Suppression of Unlawful Seizure of Aircraft (1970), Hague, 16 December 1970, *United Nations, Treaty Series*, vol. 860, No. 12325

UN Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971), Montreal, 23 September 1971,

UN Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, Including Diplomatic Agents (1973), General Assembly, 14 December 1973, *United Nations, Treaty Series,* vol. 1035, p. 167

UN International Convention Against the Taking of Hostages (1979), General Assembly, 17 December 1970, *United Nations, Treaty Series*, vol. 1316, No. 21931

UN Protocol for the Suppression of Unlawful Acts of Violence at Airports Severing International Civil Aviation (1988) Supplementary to the Convention for the Suppression of Unlwaful Acts against the Safety of Civil Aviation, Montreal, 24 February 1988,

UN Convention for the Suppression of Unlawful Acts against Safety of Fixed Platforms Located on the Continental Shelf (1988), Rome 10 March 1988, IMO Doc. SUA/CONF/16/Rev.2

UN Convention on the Marking of Plastic Explosives for the Purpose of Identification 1991), Monteral 1 March 1991, U.N. doc. S/22393

UN International Convention for the Suppression of Terrorist Bombings (1997), New York, 15 December 1997, U.N. doc. A/52/653

UN International Convention for the Suppression of the Financing of Terrorism (1999), General Assembly of the United Nations, 9 December 1999, U.N. Doc. A/RES/54/109

UN International Convention for the Suppression of Acts of Nuclear Terrorism (2005), New York, 13 April 2005, UN Doc A/RES/59/290 (2005)

UN Amendment to the Convention on the Physical Protection of Nuclear Material (2005)

UN Protocol of 2005 to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigations, Vienna, 1 November 2005

UN Protocol of 2005 to the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf of 1988

EU Research Research Project Reports

DETECTER (Detection Technologies, Terrorism, Ethics and Human Rights) research project (2011): “Recommendations of improved monitoring mechanisms of secret counter-terrorism activities” (WP 8, *D16.3*), EU FP7

Transnational Terrorism, Security, and the Rule of Law research project (2008): “Defining Terrorism”. *Deliverable 4,* WP 3 (http://www.transnationalterrorism.eu//tekst/publications/WP3%20Del%204.pdf [18.11.14]), EU FP6

TACTICS (Tactical Approach to Counter Terrorists in Cities) research project (2013). “Conceptual Solution Description”, *D3.1,* WP 3, publicly available online at: http://www.fp7-tactics.eu/files/documents/D3.1_Conceptual%20Solution%20Description.pdf [20.01.15], EU FP7

TACTICS (Tactical Approach to Counter Terrorists in Cities) research project (2013). “System architecture”, *D3.2,* WP 3, publicly available online at: http://www.fp7-tactics.eu/files/documents/D3.2_System%20Architecture.pdf [20.01.15], EU FP7

ECtHR cases

Bykov v. Russia, App. No. 4378/02 (2009)

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others, oined Cases C-293/12 and C-594/122014 (2014)

Google Spain SL, Google Inc.v Agencia Española de Protección de Datos (AEPD), Case C-131/12, 2014.

Von Hannover v. Germany (No. 2), Applications nos. 40660/08 and 60641/08 (2012)

Huber C-524/06 ECR I-9705 (2008)

Huvig v. France, App. No. 11105/84 (1990)

Kiliç v.Turkey, Application no. 22492/93 (2000)

Klass and Others v. Germany, Appl.no. 5029/71 (1978)

Kruslin v. France, App. No. 11801/85 (1990)

Malone v. the United Kingdom, App. No. 8691/79 (1984)

Murray v. UK, App. 18731/91 (1996)

Niemietz v. Germany, App. No. 13710/88 (1992)

P.G. & J.H. v. the United Kingdom, App. No. 44787/98 (2001)

Uzun v Germany, Application no. 35623/05 (2010)

Weber & Saravia v. Germany, App. No. 54934/00 (2006)