SIAM

Security Impact Assessment Measures

Work package 10: Cultural Differences

Deliverable 10.2 - Media analysis of discourse about

future security technologies

SEVENTH FRAMEWORK PROGRAMME

Massimo Migliorini

Roberta Sabbatelli

Sabrina Ricauda

Enrico Fiore

Faheem Ijaz

Work package 10

Deliverable 10.2

Project number

Call (part) identifier

Funding scheme

Table of Content

INTRODUCTION & EXECUTIVE SUMMARY

Acceptance of security measures is a crucial aspect for decision makers: a failure in taking different groups of scrutinized people into account may pose serious problems in the implementation and use of a security measure. While some feel that physical intrusiveness is the strongest form of infringement, others are much more aware of their data being dispersed globally – depending on cultural practices and technological developments. Last but not least, the SMTs might not be perceived equally for all groups. Gender, age, and status are important categories to be included in the analysis.

The following document describes the results of the work done by SITI within SIAM Project Work Package 10. The purpose of WP10 is to reveal all critical factors (including cultural differences) that may lead to different attitudes and different levels of acceptance toward different types of SMTs.

The document is focused on "**Future SMTs**" that is, according to SIAM project classification (see WP 2 and WP 5), **"security technologies that have not still achieved a mature stadium in terms of applicability and/or diffusion".**

The document is structured in 5 sections:

1. **Objectives:** the section states the objectives of the report.

2. **Methods**: the section describes the methods used for data collecting and reporting.

3. **Trust Drivers**: on the basis of the main findings of WP 10 work, the section describes the generalized Drivers that rule people acceptance of SMTs. It is worth to highlight that these Drivers represent an important basis of knowledge that will allow SIAM Partners to define new Assessment Criteria and Attributes for SIAM Assessment Support Systems, with specific focus on the subject *of Trust*.

4. **Future SMTs Analysis:** the section contains a detailed analysis of several SMTs, identifying acceptance issues and connecting them to Trust Drivers and related Mitigation Technologies (MTs).

5. **Conclusions:** the section provides conclusions based on the research findings.

1. OBJECTIVES

Deliverable 10.2 is strictly related to Deliverable 10.1, since both documents aim at capturing potential acceptance issues related to SMTs, as well as at analysing the sensitivity level of different people groups (on the basis of gender, age, job, religion, health problems and, where possible, cultural differences). The crucial objective of WP 10 is to reveal critical factors leading to different attitudes and different levels of acceptance toward different types of SMTs, and to relate these factors to the Data Model developed in SIAM project, in particular considering: SMT Typologies, Freedom infringement dimensions, Type of Scrutinized, Counter-infringement Technologies (or more generally Mitigation Measures).

2. METHODS

WP 10 work is built on the information gathered from three different sources:

a) **Produced documents and research**: all data collected in previous SIAM work packages, in particular in WP 4 and WP 8, were used to derive potential acceptance issues. Data collected were analysed, aiming at defining the interrelations between spotted acceptance issues and the sensitivity level of different people groups.

b) **Surveys with Advocacy Groups**: a series of interviews with different categories of people were held. Data collected during the interviews were analysed, aiming at spotting further acceptance issues and at understanding their interrelations with SMTs Typologies and people Groups.

Interviews were performed with people belonging to different fields:

- social assistance/support for protected categories;
- social assistance/support for criminals and prisoners;
- psychology;
- psychotherapy;
- human rights and discrimination against violence;
- civil codes and regulations;
- foreign people rights;
- mass transport systems daily users and users representative associations;

c) **Media Coverage:** freedom infringements as well as security benefits from security technologies are discussed in print media, online, and on TV. Scandals, technology renaming ("body scanner") and lawsuits obviously point to strong attitudes against a measure. A data mining on Mass Media communication materials (articles, videos, websites, etc.) was performed, to provide a rough overview of the attitudes commonly expressed.

D 10.2 information was mainly collected through **Media Coverage (source C)** and **Produced documents and research (source A).**

Gathered information were elaborated and divided into 9 Technologies Typologies, according to the classification developed in SIAM project:

Threat Detection

- *Object and Material Assessment SMTs* (also: *Screening SMTs*) are used within security measures to search and assess people, luggage, cargo and airport deliveries to identify possible dangerous or illegal substances and objects e.g. weapons, drugs, or explosive residues.
- *Event Assessment SMTs* attempt to identify an unfolding crime by, for example, using CCTV to detect *suspicious behaviour* or to spot *abandoned luggage*.
- *People Assessment SMTs* are used in measures designed to identify potential malefactors. This includes questioning strategies, profiling methodologies such as passengers' background checks, or asymmetric screening based on demographics.

Access Control

- *Identification SMTs* are used to identify people as part of security measures designed to establish access rights.
- *Physical Access SMTs* relate to the broad category of physical barriers and access technologies such as turnstiles, perimeter fencing, and automated car park barriers.

Support

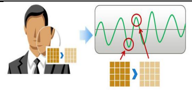
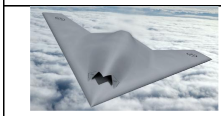
- *Process Control SMTs* capture a range of technologies that configure security process, including control of passenger flow, and randomised or intentional selection of security measures applied to individual passengers.
- *Information and Communication SMTs* capture the computing and communication technologies used for a variety of different security measures within any security regime, such as those which can be found in devices and algorithms for information processing, as well as data transfer and storage.

Policing

- *Situation Awareness SMTs* includes the use of CCTV (increasingly employing PTZ cameras) to monitor an environment and to liaise with staff on the ground, and the use of asset management solutions such as RFID tags and readers to track baggage and passenger movements or ANPR technology to identify vehicles.
- *Enforcement SMTs* are technologies used in security measures that respond to some process deviations or detected threats, such as those ensuring that each piece of hand luggage is screened or those dealing with weapons detection.

The list of "Future SMTs" that have been considered during WP 10 analysis is reported in the following table. A further detailed description is contained in Paragraph 4 ("Future Technologies

Analysis”).

	**Heart-rate Detection** (Category: *People Assessment*)
	Terahertz cameras (Category: *Object and Material Assessment*)
	**Unmanned Aerial Vehicles (UAV)** (Category: *Event Assessment/Situation Awareness*)
	Unmanned Ground Vehicles (UGV) (Category: *Event Assessment/Situation Awareness*)
	Biometrics combined with ID cards and DNA analysis (Category: *Identification*)
	Automated profiling systems (Category: *Identification/People Assessment*)
	Cyber security systems (Category: *Information and Communication*)
	Energy harvesting systems (Category: *Process Control*)
	Electromagnetic pulse (EMP) (Category: *Process Control*)
	Directed-energy weapons (Category: *Process Control*)

3. TRUST Drivers

A “**Trust Driver**” is herewith intended as <u>a logical criterion that can drive people to effectively trust or not to trust an SMT</u>. Trust Drivers, detailed and discussed here below, have been derived from the analysis of different SMT’s acceptance issues, and represent one of the most important results of both D 10.2 and D 10.1. It is worth to highlight that most of these drivers will be used in Task 10.4 to integrate the list of Assessment Criteria and Attributes produced for SIAM Assessment Support Systems, with specific reference to *Trust* subject.
As a result of both D10.1 and D10.2 analysis, this paragraph is reported in both deliverables.

A cluster of Trust Drivers were identified during WP 10 analysis:

- **a) Reliability**
- **b) Health hazards**
- **c) Experience**
- **d) Communication**

e) Human interaction
f) Diffusion
g) Appearance
h) Privacy
i) Cultural/Historical/Religious Background
j) Regulations Gaps

a) **Reliability**

The frequency of false positives or negatives puts a question mark on the effectiveness of most modern technologies. E.g. false positive may be generated while using heart rate monitoring of aged people, or people with heart diseases or even of nervous travellers (for example in case one is late, or afraid of flying). False negatives can occur when an attacker uses soothing substances to hinder the real heart rate detection. When people perceive a significant number of these events, their trust in the concerned SMT consistently decreases.

b) **Health hazards**

The fear of health hazard is one of the most important and well-known driver of people trust in a SMT. Security scanners for example are an effective method for passengers screening and have been deployed worldwide. However, these scanners are based on X-ray technology and people normally consider it as a danger for their own health. The same happens in case of electromagnetic pulse technology, in particular for people wearing electronic medical devices (such as pacemakers).

c) **Experience**

When a user enters in contact with a new technology, his attitude is typically based on his previous *experiences*, that is:

1) Past situations in which he physically interacted with the SMT;
2) Other contexts he is aware of in which the SMT has successfully been integrated;
3) Other contexts that he knows where “similar” SMTs do actually work.

d) **Communication**

Modern Mass Medias have a great power in influencing people trust towards SMTs. The more a negative opinion is remarked and diffused, the more it grows up in relevance. Common sense of Trust can also be influenced in a negative way, that is by not diffusing any information at all. Usually people do not have positive attitudes towards something they do not know anything about.

e) **Human Interaction**

The presence of a human operator near an SMT can influence people trust in a double way: in some cases it can increase positive attitudes like in the case of detection dogs, where a human operator can “inspire” a sense of security and full control of perceived potential dangers (e.g. traveler aggression by dogs). In other cases it can decrease positive attitudes: this is the case of body scanner, where people feel particularly exposed and the presence of a human operator increases their sense of vulnerability.

f) **Diffusion**

The more an SMT is used in other contexts/by other people/for other purposes, the more people are accustomed to it, the more they have positive attitudes towards it.

g) **Appearance**

One factor, whose influence on people trust is often under-evaluated, is physical appearance. The presence of high noise, strong lights, bad smell usually drive people to have a negative attitude towards an SMT. In particular cases even the external design can play a relevant role: it is enough to think about UAVs and UGVs, where an excessively aggressive external design can make people feel in a “military” environment, generating negative feelings and consequently decreasing their trust.

h) **Privacy**

When people perceive that an SMT can infringe their privacy, their attitude typically turns to highly negative. This aspect includes informational/data privacy, bodily integrity and personal privacy. Data privacy involves theft or sharing of personal information, without the owner consent or approval, which may have been stored at a system or organization. Bodily integrity concerns technologies that have the capability (or are perceived to have it) of exposing people to harms or even injuries/mutilation. One example of this is given by the use of needles for DNA analysis. Personal privacy can be infringed by exposing people individual traits, uses or traditions to security operators, thus violating personal privacy.

i) **Cultural/Historical/Religious Background**

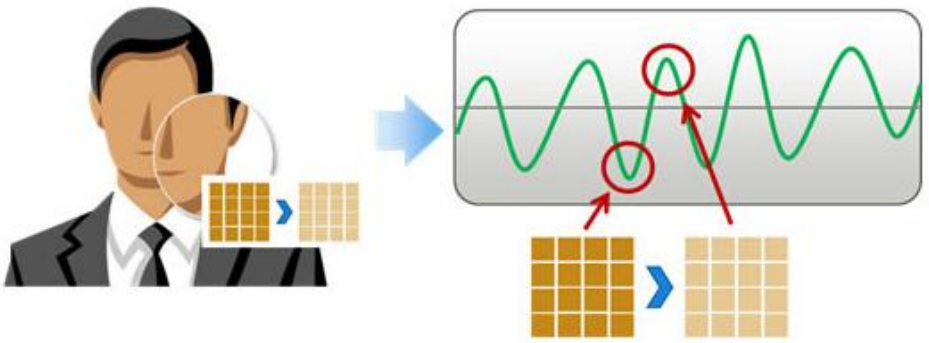
People cultural/historical background can play a role in fostering or reducing the acceptance level for an SMT. Cultures in which people are not allowed to exposing any parts of their bodies (including arms, legs and face) clearly have a more negative attitude towards detection technologies. People tied to essentiality in their traditions or life-style, normally are more suspicious towards sophisticate hi-tech SMTs.

j) **Regulations Gaps**

The presence of Rules and Regulation in matter of SMTs use is a great driver for people trust. Regulations give people a sense of “stability”, allowing them to feel more secure about their individual rights not being infringed. This issue concerns in particular SMTs which do not have a standard regulation framework over the world, but which deal with regulation changes from Country to Country.

4. Future SMTs Analysis

HEART-RATE DETECTION



Functionalities	Monitoring of individual heart-rates from a distance to detect if a person is agitated or nervous; persons with atypical heart-rates are singled out for questioning / inspection or put under surveillance Criteria to assess technology performance can be: immunity to interference (noise)
Threats	Terrorist attacks
Processes	Security checks, monitoring of crowds / individuals
Security Sensitive Areas	Airport terminals, train stations
Users	Security personnel, police
Potential Freedom Infringements	Human dignity, general right of privacy

This SMT involves innovative applications for cameras that allow monitoring heart-rate with a high-distance scanning device focusing on people faces. It works analysing face blood volume, which increases every time heart beats. The process isn't visible to the naked eye, but digital cameras can detect it. Hearth-rate detection can be quickly and efficiently performed with low cost webcams and even from mobile phones.

Which acceptance issues might arise?

False positives are very frequent, for example if travellers are anxious, late, scared to fly or have heart dysfunctions. Furthermore, a criminal could make use of soothing substances able to hinder the real heart rate detection, thus creating false negatives. This security system is also discriminant for cultures in which people are not allowed to show their face (ex. women with burqas). Also, the use of this technology without a proper communication to travellers may cause anxiety, resulting in false positives.

Furthermore, the low cost and the capability to be plugged into mobile phones commonly used allows indiscriminate uses of this SMT, with relevant consequences on people privacy infringement.

Which Trust Drivers are involved?

Reliability is one of the most critical drivers involved for the mentioned issues concerning this SMT. Privacy and Cultural/Historical/Religious Backgrounds are involved as well, together with Communication (even if it plays a less relevant role).

How might these problems be solved? Do you know any existing Mitigation Measure (MM)?

People privacy can be preserved limiting the range of cameras and informing people they are being monitored. False alarms can be mitigated using multiple technologies with different operating methods and data crossing. Instead, discrimination problems can be solved improving the system with the capability to derive heart-rate from other parts of the body, e.g. hands. Trained personnel from both sexes might be involved as well, to further reduce discrimination based on people cultural traditions (where women faces can be seen only by other women).

Which are, in your opinion, the most sensitive people to this SMT issues, depending on cultural background, gender, age, job, health problems?

People belonging to more rigid cultures are more exposed to discrimination and privacy issues. Relating to false positives, anxious people or people with health problems can generate false alarm more frequently.

RESUMING TABLE

ACCEPTANCE ISSUES	TRUST DRIVER	MMs	Most Sensitive People Groups
High possibility of indiscriminate uses	Privacy Communication	Action range limitation People information	All
High rate of false positives	Reliability	Multiple technologies data crossing	Anxious people People with hearth illnesses
Easiness to force false negatives	Reliability	Multiple technologies data crossing	All
Face exposure	Cultural/Historical/Religious Background	Hand Analysis Software and devices	People belonging to more rigid cultures

TERAHERTZ CAMERAS

Functionalities	Spot hazardous objects and materials hidden on a person`s body. Criteria to assess technology performance can be: quality of detection Driver, image resolution, ability to differentiate between hazardous and non-hazardous objects, ability to penetrate clothing, false alarm rate, no health hazard from radiation
Threats	Smuggle of hazardous objects and materials into airplanes / security-relevant areas, terrorist attacks
Processes	Security checks, crowd monitoring
Security Sensitive Areas	Airports, train stations
Users	Security personnel, police
Potential Freedom Infringements	Human dignity, general right of privacy, freedom of worship (religious dress codes), right to physical integrity

An American Company has recently developed a programmable picosecond laser, using far-infrared radiation in the terahertz band, which is capable of spotting in real-time traces of a variety of substances (explosives, chemical agents, hazardous biological substances, etc.) at a distance of up to 50 meters [3]. The beam used by the spectrometer is capable of penetrating most materials including wood, leather, cloth, ceramics, plastic, and paper, so it can essentially pass through opaque materials such as clothing, packaging and even certain building materials [4].

Which acceptance issues might arise?

This system may generate false positives in case of substances traces resulting from particular jobs or activities (such as: gunpowder residue from hunting, smoke particles, nitrate fertilizer, etc.). Other false positives could be generated by interferences with other systems because of the spectrometer long action range. Privacy issues can be raised because of its capability of penetrating through some building materials, invading citizens' private life. Other issues can be generated by its capability to showing bodies through clothes, hence invading human dignity. Finally, the general lack of information concerning system functioning could instil people to think that radiation can be unhealthy.

Which Trust Drivers are involved?

In case of false positives travellers can doubt the Reliability of the system, while the capability to see through different materials can generate a common sense of Privacy infringement. Health Hazards risks can also be perceived because of the low “common knowledge” and diffusion level of this SMT.

How might these problems be solved? Do you know any existing Mitigation Measure (MM)?

Specific filters to limit the action range would be useful to reduce false alarms. Furthermore, software able to show only an anonymous human picture and not a naked profile could mitigate privacy issues and consequently trust problems. Finally, mass media communication or local info-points could be good means to inform people on the system functionalities and turning them to more positive attitudes.

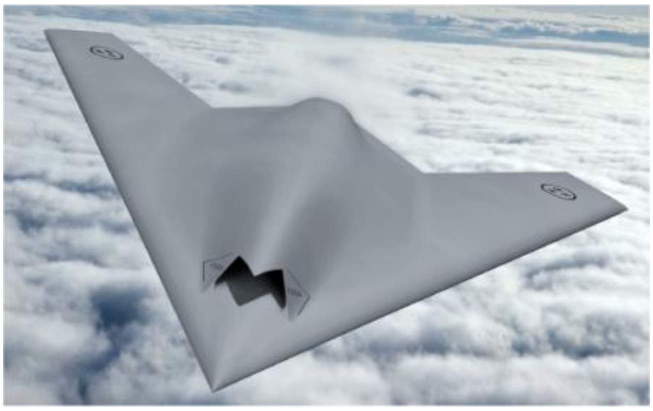
Which are, in your opinion, the most sensitive people to this SMT issues, depending on cultural background, gender, age, job, health problems?

Even if this concerns all people, women belonging to more rigid religious traditions are more reluctant to accept an SMT showing their bodies through their clothes. Furthermore, elderly and pregnant women are more sensitive to health risk. People working with particular substances (e.g. gunpowder) could be more frequently involved in false positive.

RESUMING TABLE

ACCEPTANCE ISSUES	**TRUST DRIVER**	**MMs**	**Most Sensitive People Groups**
False positives	Reliability	Filters	People working with particular substances (e.g. gunpowder)
Building materials penetration	Privacy	Filters	All
Clothes penetration	Privacy	Filters	Women People belonging to more rigid cultures
General lack of information	Experience Dissemination Level Communication Health Hazards	Local info-points	Elderly and pregnant women

UNMANNED AERIAL VEHICLES



Functionalities	Patrol / surveillance, reconnaissance, other functionalities depending on the type of sensors that are built into the vehicle Criteria to assess technology performance can be: ability to transfer collected data to a control station via live feed, operation time, capable of autonomous orientation
Threats	Dependent on area of use and built-in sensors: theft, espionage, terrorist attacks, unauthorized intrusion, vandalism
Processes	Surveillance of large areas from the sky
Security Sensitive Areas	Possibly airport perimeter if no interference with flight traffic is guaranteed
Users	Security personnel, police, military
Potential Freedom Infringements	General right of privacy, right to physical integrity (if equipped with means to harm humans)

Which acceptance issues might arise?

There are many notices about incidents [5][6] that involve UAVs and civilians (injured or killed) in military operations. The main danger seems to be posed by mid-air and ground crashes. Furthermore, the aggressive military appearance of UAVs inspires anxiety in people, giving them the feeling to be in a "constant war" environment. Optical systems in use today require good weather and are susceptible to obscurant agents, such as smog and smoke. Poor reliability of UAV systems is frequently mentioned as a principal inhibitor to the integration and wide-spread acceptance of this SMT. Studies confirms that UAVs have a high accident rate when compared to manned aircraft. According to a recent Defense Science Board review [8], approximately 85 per cent of all UAV accidents are a result of equipment failure.

Which Trust Drivers are involved?

Communication and Experience drivers are involved, due to the common sense that this technology is linked to military operations. Reliability is involved as well, because of the high rate of accidents that involve civilians in military operations.

How might these problems be solved? Do you know any existing Mitigation Measures (MMs)?

There are different kinds of technologies/measures that can be used to mitigate UAVs issues:

- Developing standards and recommended practices to organize the UAV use in civil areas.
- Improving UAVs sensing systems by diminishing size and power requirements and increasing capability and affordability.
- Developing cooperative surveillance systems that cross information provided by UAVs with local telemetry systems, with the purpose to reduce UAVs use.
- Informing people about UAVs presence, purposes, and benefits for their security.
- Providing effective measures to divide UAVs from Aircrafts Flight space.
- Differencing the design and the appearance of UAVs used for military and civilian purposes.
- Improving Aircraft sensing systems to detect UAVs and prevent crash risks.

Which are, in your opinion, the most sensitive people to this SMT issues, depending on cultural background, gender, age, job, health problems?

If Aircrafts are not adequately equipped, pilots might be exposed to a greater stress (also in terms of further training) to ensure crashes with UAVs are avoided. Anxious/phobic people might be more sensible to UAVs psychological pressure.

RESUMING TABLE

ACCEPTANCE ISSUES	**TRUST DRIVER**	**MMs**	**Most Sensitive People Groups**
Ground Crashes	Experience Health Hazards Communication	Developing Standards and Recommended practices. Improving UAVs sensors performances.	Anxious/phobic people
Mid-air crashes with aircrafts	Experience Health Hazards Communication	Developing standards and recommended practices. Improving UAVs sensors performances. Providing effective measures to divide UAVs from Aircrafts Flight space. Improving Aircraft sensing systems to detect UAVs and prevent crash.	Aircraft pilots Anxious/phobic people
Poor reliability	Reliability	Improving the integrity of components	All
Military appearance	Appearance Communication	Informing people about UAVs presence, purposes, and benefits for people security.	Anxious/phobic people

UNMANNED GROUND VEHICLES

Functionalities	Patrol / surveillance, reconnaissance, other functionalities depending on the type of sensors that are equipped on the vehicle Criteria to assess technology performance can be: manoeuvrability, ability to operate / navigate in street traffic, ability to transfer collected data to a control station via live feed, operation time
Threats	Dependent on area of use and built-in sensors: theft, espionage, terrorist attacks, unauthorized intrusion, vandalism
Processes	Surveillance of remote areas
Security Sensitive Areas	Airport perimeter
Users	Security personnel, police, military
Potential Freedom Infringements	General right of privacy, right to physical integrity (if equipped with means to harm humans)

Which acceptance issues might arise?

People often associate these vehicles with military operations; therefore they feel unsafe, imagining also that these vehicles can be armed. Their menacing appearance can instil in people the idea that the technology is dangerous, also because the vehicle is without operator, which make people think that it is out of control. Another negative aspect that can reduce people trust can be represented by the fact that the technology used in these vehicles is very expensive, since it has to be the best existing one. In fact each unmanned vehicle requires its own specific programming, which means that many technology engineers spend countless hours on testing and designing these vehicles. If a technological error occurs, these vehicles become useless, and may be even dangerous for people or things.

Which Trust Drivers are involved?

The driver of **Appearance** is involved since people can be impressed about this SMT aggressive aspect. Also, since it is linked to military operations, **Communication** and **Experience** drivers are included, as well as **Reliability** driver, because of the accidents happened in the military field that involved civilians. The **Diffusion** can be very low at the moment since the poor technology reliability doesn't permit the application of this device in all conditions, and also the high technology costs can act as deterrent for its utilization.

How might these problems be solved? Do you know any existing Mitigation Measure (MM)?

Informing people that in the area there are these kinds of vehicle and explaining the behaviour they should adopt with them can be a way to improve the technology acceptance. Also, people have to be informed about the devices used in the vehicle and which tasks the vehicle has to perform. From the technology point of view, improving sensors enable a self-localization, hazard avoidance and automation.

Which are, in your opinion, the most sensitive people to this SMT issues, depending on cultural background, gender, age, job, health problems?

The annoying feeling is perceived by everyone, but people that don't trust technology when it is not driven by an operator are more worried than others.

Moreover, parents can be afraid for children, because children can confuse this kind of vehicle to a game.

RESUMING TABLE

ACCEPTANCE ISSUES	TRUST DRIVER	MMs	Most Sensitive People Groups
Idea that the technology is dangerous due to its aspect	Appearance Communication	Informing people about vehicles tasks;	All
This technology is linked to military operations	Appearance Communication Experience	Informing people about vehicles tasks; Informing people about the behaviour to adopt with vehicles	All
No operator near the device	Reliability Appearance	Informing people about vehicles tasks; Informing people about behaviour to adopt with vehicles	People that don't trust technology
Technology errors	Reliability	Improving sensors enable a self-localization, hazard avoidance and automation	People that don't trust technology
Expensive costs compared with benefits	Diffusion	Evaluating tasks that the vehicle has to perform.	All

<table>
<tr><th colspan="2">BIOMETRICS COMBINED WITH ID CARDS AND DNA ANALYSIS
 </th></tr>
<tr><td>Functionalities</td><td>Access control, identification / verification; any measurable/collectable, unique, universal and permanent feature can be used
Criteria to assess technology performance can be: minimization of false negatives / positives, throughput rate, social acceptance, possible combination with other identification methods (e.g. ID cards)</td></tr>
<tr><td>Threats</td><td>Persons gaining access to restricted areas without permission, unauthorized intrusion</td></tr>
<tr><td>Processes</td><td>Security checks, any point of entrance to a restricted area</td></tr>
<tr><td>Security Sensitive Areas</td><td>Airports, customs, immigration</td></tr>
<tr><td>Users</td><td>Security personnel, police</td></tr>
<tr><td>Potential Freedom Infringements</td><td>General right of privacy, freedom of worship (religious dress codes)</td></tr>
</table>

Which acceptance issues might arise?

The modality in which personal data are stored and according to which people can access at the database where detailed personal data are, can transmit to people a sensation that their data are not stored safely. Other problems are related to time, money and technology that have to be employed. In fact the system would be hugely expensive to set up and administer. Furthermore the security of biometrics is questionable; there are doubts about the accuracy of equipment and the margins of error for validating a person's identity from biometrics. There is even the possibility to get mistakes in the automatic fingerprinting recognition and false matches (that is, incorrectly matching a subject with someone else's reference sample) and false non-matches (failing to match a subject with his/her own reference sample). From the health point of view, there is the idea that the technology may cause damages to the user (there is a common thought that retina or iris recognition can be dangerous to the eyes and DNA analysis needles can hurt people). Also, if it is required to touch the device, it can be felt as a disease vector.

There is the belief that biometric data do not get useful information to prevent terroristic attack or improve safety, since identification alone doesn’t reveal anything about whether a person is a terrorist. People trust can be reduced by the feeling that this SMT can discriminate people by their appearance.

Which Trust Drivers are involved?

Privacy is one of the main trust drivers for this technology. In fact something that worries people is how their data are handled and stored. Therefore **Communication** is a consequence since people have to be informed about the uses and limitations of this SMT. Moreover the biometrics is very expensive but not really accurate. Consequently, it is important to evaluate if **Reliability** is worth the money and time spent for it.

Health hazard has also to be taken into account since it is not clear if the technology may cause damages to the user.

How might these problems be solved? Do you know any existing Mitigation Measure (MM)?

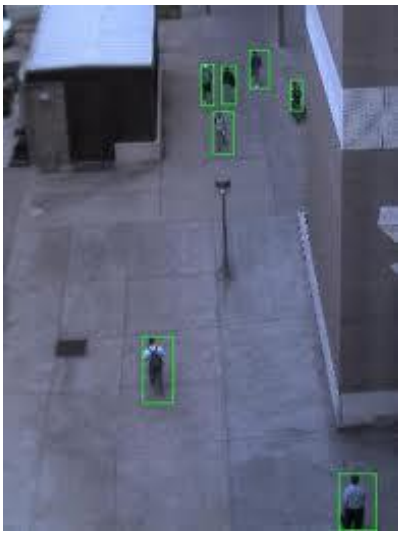
Security standards and procedures have to be implemented in order to protect biometric data and to regulate databases access. From the health point of view, people have to be informed about the consequences of long-term effects of repetitive exposure to device.

Which are, in your opinion, the most sensitive people to this SMT issues, depending on cultural background, gender, age, job, health problems?

Many people have fingers that simply do not "print well." Even if people with "bad prints" represent only 1% of the population, this means inconvenience and suspicion for that minority. Also, this technology may lead to minority ethnic groups' discrimination. Not to forget that it can cause uneasiness to people with physical problems or deficiencies.

RESUMING TABLE

ACCEPTANCE ISSUES	TRUST DRIVER	MMs	Most Sensitive People Groups
Data security	Privacy Communication	Standard or procedures that regulate database access. Informing people about the uses of these data	All
Dangerous or unhealthy	Health Hazards Communication	Informing people about the long-term effects	People with physical problems or diseases
The system would be expensive to be set up and administered	Reliability	Evaluating if it is worth the money and time spent.	All
Identification of problems about the accuracy of equipment	Reliability	Implementing secondary procedures	People with physical problems or deficiencies
Efficiency in preventing terroristic attacks	Reliability	Discrimination	Minority ethnic groups discrimination

AUTOMATED PROFILING SYSTEMS 	
Functionalities	These systems are similar to currently existing profiling systems in terms of purposes, aiming at profiling people, categorizing people into risk categories, singling out passengers for more rigorous checks. They differ from current systems in being less tied to human operators, allowing people to be directly identified/checked by technical devices (ex. CCTV) connected to a remote database and supported by advanced software for the recognition of individuals' somatic traits and/or the spotting of suspicious behaviour. Criteria to assess technology performance can be: access to background information, accuracy of background information.
Threats	Terrorist attacks, illegal migration, human trafficking
Processes	Security checks, monitoring of crowds / individuals, patrols
Security Sensitive Areas	Airports, train stations, bus terminals
Users	Security personnel, police
Potential Freedom Infringements	Human dignity, general right of privacy, right to equality and non-discrimination

Which acceptance issues might arise?

The main issue that creates doubts about this technology resides at the basis of it, that is how to decide criminal profiles, without discriminating ethnic and religious minorities.

In addition, there is a privacy issue. In fact the collected data identifying suspected profiles may be broad and they can include personal information, pictures or biometric identifiers, address, flying patterns with a particular airline, bill paying at a particular address, criminal records, and other information.

Which Trust Drivers are involved?

How profiles are created may discriminate a certain type of people. **Privacy** is involved since a lot of information about people has to be investigated to create profiles. This information database needs a safety solution to store all the information that can be used to create archives containing private information: movements, behaviour, etc.

How might these problems be solved? Do you know any existing Mitigation Measure (MM)?

Behaviour science studies have to be improved, since patterns of behaviour considered anomalous in one culture are normal in others; better understanding cultural effects could lead to more effective and, possibly, less discriminatory use of profiles. Factors to be considered as elements of the profile should be based on measurable, verifiable data indicating that the factors chosen are reasonably predictors of risk, not stereotypes or generalizations.

Another proposal could be to establish databases of past incidents and known terrorists in order to help developing profiles, and to introduce an efficient screening technology.

Which are, in your opinion, the most sensitive people to this SMT issues, depending on cultural background, gender, age, job, health problems?

Since at the moment this technology has discriminatory aspects, the most affected categories are people from ethnic or religious minorities, as well as young and black people, mainly males.

RESUMING TABLE

ACCEPTANCE ISSUES	**TRUST DRIVER**	**MMs**	**Most Sensitive People Groups**
Determination of the profiles	Cultural/Historical/Religious Background	Improving behaviour science studies Selecting appropriate factors to create profiles	Ethnic groups Religious groups Young and black people, as well as males
Collected data	Privacy	Selecting appropriate factors to create profile	All

CYBER SECURITY SYSTEMS

Functionalities	Securing computer systems and data / communication channels Criteria to assess technology performance can be: scope of protection, keeping security up to date
Threats	Hacking, data tampering / manipulation, digital intrusion, other digital attacks (e.g. denial-of-service, session hijacking, network eavesdropping, etc.), phishing, malware
Processes	Any computerized system that can be accessed remotely
Security Sensitive Areas	Any computerized system that can be accessed remotely
Users	IT-specialists, Global business and trade, Security agencies, Military, general online user
Potential Freedom Infringements	Privacy, information sharing transparency, sharing of unnecessary personal information.

Which acceptance issues might arise?

Cyber security involves information sharing to enhance security of critical infrastructures, business etc. It involves information sharing between government and private sector and among private sectors themselves. This information sharing raises many privacy and antitrust concerns. Online networks and systems are prone to cyber-attacks and lack of legislation regarding international cyber-crimes pose a challenge to users trust on online systems. Lack of global laws to prosecute cyber-crimes, laws concerning scope of information sharing and transparency and accountability issues arising in case of misuse of private information are major concerns in cyber security. Databases create for cyber security may be vulnerable to hacker attacks and a solution need to be found.

Furthermore, international cybercrimes challenge the effectiveness of law enforcement. Since there are ‘no cyber borders between countries' and because existing laws in many countries are not tailored to deal with cybercrime, criminals increasingly conduct crimes on the Internet in order to take advantages of the less severe punishments or difficulties of being traced. Even though some countries are cooperating in this regard, efforts of establishing global standards of legislation and law enforcement both on a regional and on an international scale are still needed. This clearly has an effect on the acceptance level for cyber-security devices.

Which Trust Drivers are involved?

Privacy and **Regulation Gaps** are the main Trust Drivers involved in this technology, which seems to need a coherent global standardizations.

Communication on information sharing should be received. Human failing in handling information and software vulnerabilities can be improved to effectively improve trust in systems **Reliability.**

How might these problems be solved? Do you know any existing Mitigation Measure (MM)?

Database should be managed locally and secure operating systems and coding to be employed in order to stand any hacking/malware attack on system. Legislation needs to be done for global cyber-crime laws. Lines need to be drawn on cyber security threat information and non-cyber security threat information and users should be informed for any information sharing.

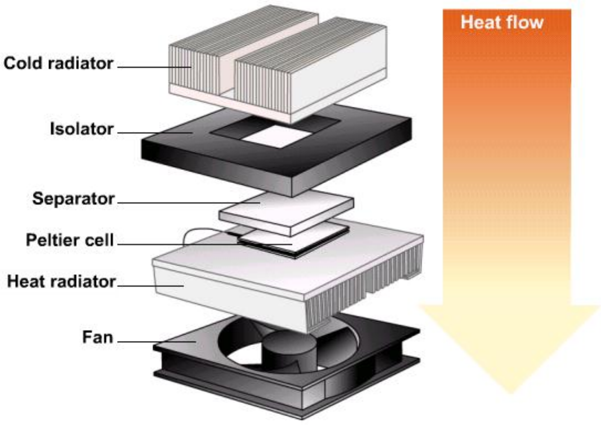
Which are, in your opinion, the most sensitive people to this SMT issues, depending on cultural background, gender, age, job, health problems?

All people are subjected to this SMT issues. No discrimination issues based on cultural background are involved in case of cyber security.

RESUMING TABLE

ACCEPTANCE ISSUES	TRUST DRIVER	MMs	Most Sensitive People Groups
Privacy and antitrust	Privacy	Database should be managed locally	All
Hacking / phishing/ malware attacks	Reliability	Database should be managed locally	All
Transparency, accountability, information regulation	Privacy Regulation Gaps	Users should be informed for any information sharing	All

ENERGY HARVESTING SYSTEMS



Functionalities	Able to harvest energy from surrounding environment, exploiting for example local temperature gradients (Peltier Cells) vibrations, electromagnetic waves, etc. The energy collected is used to supply sensors or similar device. Criteria to assess technology performance can be: energy production rate, size, absence of hysteresis, reliability
Threats	Sabotage
Processes	Energy supply for sensors
Security Sensitive Areas	Airports, train stations
Users	Security personnel
Potential Freedom Infringements	-

Which acceptance issues might arise?

No acceptance issues have been identified for this technology.

Which Trust Drivers are involved?

No trust Drivers have been involved for this technology.

How might these problems be solved? Do you know any existing Mitigation Measure (MM)?

-

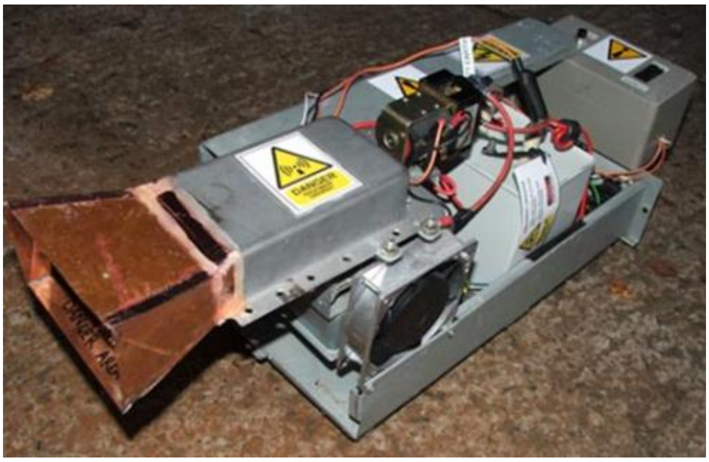
Which are, in your opinion, the most sensitive people to this SMT issues, depending on cultural background, gender, age, job, health problems?

-

<u>RESUMING TABLE</u>

ACCEPTANCE ISSUES	TRUST DRIVER	MMs	Most Sensitive People Groups
-	-	-	-

ELECTROMAGNETIC PULSE



Functionalities	Disabling electronic devices through overvoltage, stopping incoming vehicles without using force, omnidirectional Criteria to assess technology performance can be: radius of operation, no health hazard
Threats	Terrorist assault; use only as a last resort due to the significant collateral damage after every use
Processes	Defence against imminent or on-going attacks
Security Sensitive Areas	Airports as a whole
Users	Security personnel, police, military
Potential Freedom Infringements	Human dignity, right to physical integrity

Which acceptance issues might arise?

The EMP can destroy electrical components used in everyday items, such as computers and communications equipment, as well as large infrastructure equipment and transformers used in our electric grid with disastrous consequences for the affected area. It can, for example, overload the entire airport, aircrafts in flight and travellers' electronic devices causing many economical and psychological damages. The system can also generate serious damages to medical devices (e.g. pacemakers). This reflects in a common negative feeling for this SMT.

Which Trust Drivers are involved?

Communication is the driver involved to fill in the lack of knowledge about the technology mechanism. This gap leads to a lack of confidence in the **Reliability** of EMP systems and to fear that the system can have **Health** consequences.

How might these problems be solved? Do you know any existing Mitigation Measure (MM)?

The knowledge can be enhanced through the development/increasing of adequate information and communication procedures, while the fear for health hazards can be reduced by decreasing the intensity standards of the electromagnetic pulse.

Which are, in your opinion, the most sensitive people to this SMT issues, depending on cultural background, gender, age, job, health problems?

All the people with electronic devices and electronic medical equipment could be affected by this technologies issues, with high impact on their trust level.

<u>RESUMING TABLE</u>

ACCEPTANCE ISSUES	**TRUST DRIVER**	**MMs**	**Most Sensitive People Groups**
Destroy electrical equipment	Reliability Communication	Spreading information and decreasing intensity of the system	Owners of electronic devices
Interference with medical devices	Health	Decreasing intensity of the system	People with electronic medical equipment

DIRECTED-ENERGY WEAPONS

Functionalities	It can be used against terrorists armed with weapons, against objects, or to disable electronic devices through overvoltage. Criteria to assess technology performance can be: range of action, hazards for people health
Threats	Terrorist gunmen, terrorist assault
Processes	Defense against imminent or on-going attacks, crowd control
Security Sensitive Areas	Airport terminals, train stations, bus terminals
Users	Security personnel, police, military
Potential Freedom Infringements	Human dignity, right to physical integrity

Which acceptance issues might arise?

This kind of weapon is not so precise, and it acts in an impact area. Considering these assumptions, during its utilization it can happen that innocent people are involved and may be injured. In addition, these technologies have a high energy need, which reduces their portability. Furthermore, it is likely that some directed-energy weapon may interfere with medical devices e.g. pacemakers.

To end up, some weapons can hit people without leaving damages, which can make people think that they can be used in hidden mode. All this issues have a strong impact on people trust toward this SMT.

Which Trust Drivers are involved?

This kind of weapon is poorly known as well as its radius of action, which can involve common people directly or indirectly. This involves **Communication**, so that people are aware of its use, and **Health Hazards** since we don't know yet the damages that it may cause. **Regulation Gap** plays also a relevant role in decreasing common acceptance level for this SMT.

How might these problems be solved? Do you know any existing Mitigation Measure (MM)?

The only way to solve these issues is to improve the technologies itself.

Which are, in your opinion, the most sensitive people to this SMT issues, depending on cultural background, gender, age, job, health problems?

People having heart problems or other electronic medical devices are more concerned about the short and long term effects of this technology.

RESUMING TABLE

ACCEPTANCE ISSUES	**TRUST DRIVER**	**MMs**	**Most Sensitive People Groups**
Innocent people can be involved and injured	Health Hazards Reliability	Improving the technology	All
Interferences with medical devices	Health Hazards Reliability		People with diseases
High power requests	Reliability	Improving energy storage, Improving energy efficiency	All
Used in hidden mode	Communication	Informing	All

5. Conclusions

In general, the acceptance of a technology depends very much on how this is proposed. This does not affect already known technologies, such as cameras, they are so widespread that people have become accustomed, but plays a crucial role in technologies that are still to be diffused.

People have always to be informed about the use of a SMT and its contraindications if any. Staff working with a technology must be trained to correctly deal with people. They must receive psychological training since any operator must be able to communicate with the customers. In fact, one very important aspect about the use and implementation of new security technologies at critical places and buildings is the acceptance of these technologies by the general public. These technologies may involve use of X-rays and terahertz radiations. They can cause problems on health or violate human dignity, just to mention two issues which put serious question marks on technology acceptance.

As already said before, a major concern which is common with the use of most of security technologies is privacy violation. Privacy issue includes personal, physical and data privacy. Personal and physical privacy can be considered violated when scanners are used, giving the possibility of seeing through clothing and walls. That's why it would be useful to find a way where the technology itself processes directly the image, so that the human eye should not intervene. Data privacy issue arises with personal data sharing for cyber security purposes without the user consent. It is imperative to avoid the indiscriminate use of information sharing, and also it depends on how and who uses them.

Some technologies like unmanned aerial and ground vehicles are very expensive and have reliability issues. Also, their appearance gives a notion of some military use like spying or being armed with weapons. They can be seen as an excessive security measure. We have to see statistically how real the risk is.

Therefore, in order for a technology to be widely accepted, people should be informed and educated about its purpose and use, its importance and usefulness and about all the associated risks and contraindications. This is because most of the time newer technologies make people reluctant and create a sense of anxiety and fear, which can be avoided by experts debates and by spreading information through media.

Also, an in depth study on health effects of some technologies need to be done extensively.

The impact of technologies like electromagnetic pulse and energy directed weapons is wide in terms of collateral damages to electronic equipment, so their use needs to be precisely defined.

One clear thing is that there cannot be any SMT that can have 100% of acceptance. So instead of having a single technology for a specific security measure, there should be multiple technologies that can serve for the same purpose. Some of these technologies must be used only in specific areas or times, since they may cause economic and psychological damages. Therefore they should be used with caution, only in extreme situations and not abusing.

6. Bibliography

[1] T. Pursche et al., *Video-based Heart Rate Measurement From Human Faces*, 2012 IEEE International Conference on Consumer Electronics (ICCE)

[2] www.positivefuturist.com/archive/367.html

[3] www.extremetech.com/extreme/132620-how-terahertz-laser-scanners-will-spy-on-you-in-airports

[4] http://www.wi-ltd.com/security/Scanning_and_Screening/X_Ray_and_Screening_Systems/People_Scanners/WG_Body_Passive_Terahertz_Scanner

[5] DeGamo M.T. (2004). Issues Concerning Integration of Unmanned Aerial Vehicles in Civil Airspace. MITRE.

[6] http://edition.cnn.com/2013/03/15/world/asia/u-n-drone-objections

[7] https://sites.google.com/a/cortland.edu/unmannedmilitarygroundvehicles/home

[8] S. J. Anderson, S.C. Peters, K. Iagnemma. Semi-autonomous stability control and hazard avoidance for manned and unmanned ground vehicles. MI 48397 1.

[9] http://www.citizenshipfoundation.org.uk/main/page.php?217#arguments_public_opinion

[10] http://www.time.com/time/nation/article/0,8599,1974927,00.html

[11] Stelvio Cimato, Marco Gamassi, Vincenzo Piuri, Roberto Sassi (2006). Privacy Issues in Biometric Identification. INFORMATION SECURITY.

[12] National Science & Tecnology Council (NSTC) Subcommittee on Biometrics (2006). Frequently Asked Questions about biometric. http://biometrics.gov/Documents/FAQ.pdf

[13] ICAO Secretariat (2003). Effectiveness of security inspections depends on human proficiency. ICAO Journal.

[14] http://www.notbored.org/maomagazine.html

[15] U.S. Congress (1992). Office of Technology Assessment, Technology Against Terrorism: Structuring Security, OTA-ISC-511. http://www.skyjack.co.il/pdf/Humans-factors-in-Aviation-Security.pdf

[16] http://epic.org/privacy/faa/airline_security_letter.html

[17] https://www.eff.org/deeplinks/2013/02/cispa-privacy-invading-cybersecurity-spying-bill-back-congress

[18] http://www.cov.com/files/Publication/9eddbda3-770d-4388-881d-24f0f88f8b20/Presentation/PublicationAttachment/f42eb03e-12cd-4a1e-8abc-2b8e07aee13d/Reflections_on_Legal_and_Policy_Developments_in_Cybersecurity.pdf

[19] American Foreign Policy Council, *Defence Dossier*, February 2012, Issue 2

[20] Foster J. S. et al., *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP)* Attack, Volume 1: Executive Report 2004

[21] http://www.cbsnews.com/stories/2008/02/29/60minutes/main3891865.shtml

[22] http://en.wikipedia.org/wiki/Directed-energy_weapon

[23] http://www.wired.com/dangerroom/2013/04/air-force-directed-energy/

[24] http://www.examiner.com/topic/directed-energy-weapons