SEVENTH FRAMEWORK PROGRAMME

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

TACTICS

Tactical Approach to Counter Terrorists in Cities

Deliverable details	
Deliverable number	D9.4
Title	Workshops and closing conference
Author(s)	Morpho, TNO
Due date	31-08-2015
Delivered date	15-09-2015
Dissemination level	Public
Contact person EC	PO

Cooperative Partners	
1.	TNO
2.	RAND
3.	KLPD
4.	PRIO
5	ITTI
6	TCD
7	ISCA
8	UPV
9	Fraunhofer
10	KMAR
11	MPH

Table of Contents

1 Executive summary

As described in TACTICS deliverable D9.2 Dissemination Plan the TACTICS consortium has organised four workshops and a final event to disseminate the project:

- Four workshop meetings to enable cross-exchanges between the counterterrorist units and police authorities.
- A final conference was organized for all contributors, target groups of end users, scientists and other interested parties to mark the end of the programme. An overview of the key results have been given and a panel discussion was be held on what recommendations can be made for the future.

1.1 Events

The consortium organized the following events:

1.1.1 The four workshops

1. International bias mitigation workshop with end users.
2. The need for a TACTICS-like system, during the CCR summit with end users, policy makers and industry.
3. The video workshop with end users from UK, France, Netherlands, Germany and Spain.
4. The deployment workshop with NATO and European parliament members.

1.1.2 The Final Exercise

The final exercise worked out as a dissemination event, Spanish, Dutch and French end users attended the exercise and gave positive feedback on TACTICS , therefore the final exercise is also reported in this document.

1.1.3 An additional workshop on Pre Commercial Procurement for TACTICS

Following the end users and TACTICS reviewers feedback, a workshop focused on a possible Pre-Commercial Procurement (PCP) project to expand TACTICS concept to market maturity was organized.

1.1.4 The Final event

The final event was held at the IFSec London exhibition in June 2015, to benefit from the large audience brought by the exhibition.

1.2 Conclusions

This deliverable describes the four workshops, the additional workshop (focused on PCP), the final exercise and the final conference that constitutes the major dissemination events from TACTICS.

1.2.1 Dissemination channels

In terms of dissemination channels TACTICS used both :

- large exhibition events to benefit from the audience (end users, policy makers and industry) derived from the exhibition, like
    - the CCR summit (450+ Public Safety & Security experts: Directors, Decision-makers, Executives, Procurement Officers, ICT Managers, Project Managers from: Fire & Rescue Services, Health Services, Defence, Intelligence Services, Local & National Government

Bodies, Police (Law Enforcement, Intelligence, Command & Control, Crowd & Riot Control), Public Safety & Security Related Industry.

- o and IFSEC (40,000 security managers, loss prevention managers, facilities managers, installers, integrators, electricians, consultants, architects and specifiers to network, source solutions and discover what the future holds from our leading suppliers.)

- as well as more focused private meeting based on specific topics with the end users like the deployment and video workshop.

1.2.2 End user appreciation

In terms of end users feedback, most end users were interested in TACTICS concepts at a subsystems or component levels. Several end users stated that they would like to use a TACTICS like system today. One of the consortium end users asked for the Capability Manager part to be built for their system. End users said they would like to use TACTICS as a training system. They pointed out that TACTICS needs to be integrated with existing infrastructure in order to be operational.

Appreciation at the CCR Summit 2014:

At the CCR Summit in 2014 the audience was interested in a system like TACTICS. It took a moment to grasp the ideas behind TACTICS, then the audience asked several questions. For example about the innovation that TACTICS brings. They saw the added value to a security control room to see all data in on common operational picture.

Appreciation from the video workshops

During the video workshops the audience gave the following feedback: TACTICS holds its objectives in its concept, the concept has raised interest of the present agencies that have found it very capable. Nonetheless, they have précised that it feasibility and pertinence can't be assessed if not in the concrete field, to test on their different realities they have to face:

- -heterogeneity of their systems and of the quality of those systems
- -heterogeneity of the end-customers

The concept has to be thought in an incremental way to build different layers step by step, while having field's assessment and on-the-go upgrades. It has to be decomposed for each end-user.

Agencies are confronted to a diversity of field realities…that lead them to various requirements.

Appreciation from the Final Exercise

The Final Exercise successfully illustrated TACTICS capabilities, including some of its signature features such as behavioural analysis, face recognition and counter-bias. The feedback from the audience was positive and validated not only the system as a whole, but also its operating concept.

The comments suggested that, if properly integrated and connected with existing systems, a system like TACTICS could improve situational awareness, decision-making and preparedness of security forces, in addition to allowing for a better management of capabilities.

In addition, the audience suggested that TACTICS could also be further developed and used as a powerful training tool for officers and/or entire teams who would be exposed to many of the aspects of real life operations and events in a close-to-reality environment.

Appreciation at the Final Event IFSec 2015

During IFSec 2015 some vendors were interested in the behavior detection part of TACTICS. Also a panel discussion was held. Topics were privacy, trust, deployment of TACTICS and usefulness in an operational environment. Highlights were:

-TACTICS is especially necessary since the latest way of working of terrorists is to have several smaller attacks carried out by small groups of persons. The attacks are mobile and multi target. Therefor there is a chase involved. Furthermore 85% of the camera's is in private hands. In order to successfully mitigate threats it is important to use these private CCTVs.

-The terrorist don't warn anymore in advantage, compared for example with the IRA. They used to warn the authorities before the attack. We can't stay at high alert all the time, therefor our response to threats must innovate. TACTICS can assist with this, I see it as a useful platform to manage resources quicker.

-The public will want a system like TACTICS. Trust is essential. Trust is related to transparency and therefor the authorities have to communicate emotionally about a system like this. For example about where the data is stored, who can access it. So a key question is: How do we communicate Privacy by Design. All of what is sketched today will be there in the future. If the EU and research consortia like TACTICS won't do it, the private sector will push it. Keeping humans in the loop is essential to trust.

Appreciation at the Pre Commercial Procurement Workshop

End users, Europol etc. were interested in the possibility of a PCP. It is investigated if a PCP workshop can be held during the CCR-Summit 2015.

2 Workshop 1: International Bias Mitigation Workshop

The workshop on Bias Mitigation was held 18 February 2014

The following topics were discussed:

Integration of Morphological Analyses and Global Terrorism database?

Morphological Analyses (MA) was presented in the starting screen of TDT together with the Global Terrorism Database, users can choose between these tools by pressing a button. This introduces the first problem: how to choose? Colours? This introduces a bias.

This is not preferable and makes it more complicated. These two should be integrated.

The two scenarios:

1. There will be an attack in a stadium using chlorine.
2. There will be an attack in a conference center using a Vehicle Borne Improvised Explosive Device (VBIED).

The Global terrorism database seems not very flexible to use when searching. You want to be able to search based on the information you have. The tool has to be flexible.
Also a user wants fast feedback when working under time pressure.

Global terrorism data base is highly structured. Morphological analysis is a relational database.

Value of TACTICS

End user: We want an advisory tool, we already have an information system on threats and capabilities. Does TACTICS give advice? An advisory tool would be new to what already exists. TACTICS is a quick way to do this. Also: TACTICS is a big red button: this threat is bigger or different than what we have seen before. For example an incident with chlorine - TDT- a support what will be the effect depending on the amount and the link with capabilities. TACTICS could make explicit that you need other capabilities.
Support during a large crisis – fast picture of what you need.

At what level do we use TACTICS?
Who is end user? National? Local? Political organization?

Conditions - TACTICS

What conditions are important for a successful implementation?

Make explicit what system provides to the user
Make sure you don't inhibit the process too much
Don't block the system
Must take into account time pressure that people have.
Must make people aware of biases, must be smart so that people really see it.

Existing tool that might be useful: Risk analysis tool (as used by Transport Police, UK)

Attention

Examples of how these biases are of influence in practice:

Preconception: preconceived ideas of who might be responsible based on what you know and think you know. Preconceptions based on experience, previous incidents. These preconceptions influence perception.

Madrid: bombings on rail and underground (ETA); they had an incident a year before by ETA. It might have affected wider response (ETA does not leave country, so they probably did not think of closing the borders; they started looking at ETA community; intelligence focuses on wrong group, different support bases, different tactics). Oklahoma: Clinton mentioned Middle-East (even Sikhs were killed). You need to falsify information. Rabin assassination: focusing on wrong group (Muslims, but it was right-wing), secret service worked together with wrong intelligence. Everybody who talked to him framed him as part of their group (chauffeur, Jew, undercover agent).

(existing) solutions:

Use mechanisms of auto-critique (question yourself; out of the circle of influence; real-life training. Ask yourself: what if I am completely wrong?)
Like having a parrot on your shoulder.

Secondary to commander in control has role to ask question (KMAR) and to construct evidence that this is true or this is true (falsify). This is done in training and during operational scene.

Get information from technical experts (e.g. handprint how a bomb is made), this expert information can be useful. Using experts can also be dangerous, because often they are really sure. Therefore use different types of knowledge: acquired knowledge (science) and experience knowledge (experts).

Ego, somebody with high position might be difficult to overrule. An open atmosphere and no hierarchy are important.

Build cross checks

Bring in people with different experience and expertise, bring in external eye.
Have two teams, have crazy teams. Check blind spot; are you blind right now?

At certain stages build into system: bring in fresh eyes: here is everything, see what you make of it.

Check questions:

- Who authorized this?
- What other options are there?
- What other explanations are there?
- Is information missing? Is it reliable?

Important to validate information

Rephrase hypothesis: prove that x, y did it, prove that x,y didn't do it

Intelligence cycle – re-task for gathering info

The difficulty is that you don't know that you are biased.

Use out of the box thinking, make information explicit

Use part of the team – send people home, later use them, fresh view

Keep telling 'you are only human'

Use a second group as a back office

Categorizes people, e.g. stereotyping

Not relevant in TACTICS, in the sense that it is very micro. You do not know enough to tell people what they are looking for, so you want them to keep an open mind, so do not tell them about the group that might be responsible. This is very risky, because there might be a societal response to going after all persons of a specified group.

Is more relevant on operational level (if you look at camera), might lead to false judgments

Information

If you have a pre-conceived idea, you think it supports your hypothesis.

'If I had never believed, I would never had seen it.'

Human-machine

You have to update your system, to avoid relying on the wrong information. Anyway, overly relying on the provided information is not a good idea. Example of over-reliance: if license plate system indicates there is no specific information, people assume the car is ok (might be a false license plate). It gives wrong assumptions.

Risk of glorification of technology.

Build procedures and protocols to bridge the technology and human action.

How is this dealt with in practice: you could rotate people; introduce deliberate false positives (to test the system), red teaming.
Train operator – how to use system, use right procedures.

Pop up: I am only a machine.

Pop up: question X is not yet answered, let the system highlight factors that are unanswered; function that reminds you that something has not been done yet (also addresses cognitive lock-up)

System produces a periodic report, this can be given to the devil's advocate team. Also useful in case of rotation.

Advice taking: you cannot hide behind a system; TACTICS is framed as a decision making tool, but the individual needs to make the ultimate decision, TACTICS advices.

Interaction team

Communication, coordination is also important between units and within team (e.g. friendly fires).

Is relevant for TACTICS: within tool, within TACTICS, outside TACTICS.

Groupthink/ or one dominant person who influences opinion/decisions: not always easy to circumvent hierarchy. Mirror team (realistic mirror performance).

John Harvey Jones: I don't want yes-men, I want constructive no-men.

Should the second man be the one who uses TACTICS? No, should be the first, but there might be an option that produces a challenge for the first (second).

TACTICS should deal with the problem that there is one person responsible and lower ranks will not contradict.

Accordion of stress: you do not know in what stage you are, always changing energies

General:
We need something in TACTICS that raises the issue of bias, at least marking within the system that this is an issue (but not always in the same way).

Must make people aware of biases, must be smart so that people really see it.

Must take into account time pressure that people have.

If you build something into the system, be careful, you don't want to annoy users. Training would be good: how to operate the system, and then: what biases are common and how to deal with it?

Experiment

ISCA wants to make a computer-based training with a demo (training mode and operational mode. Training mode can build trust in the system).

RAND: Libyan embassy in 1984: tunnel vision

In the introduction of the CBT: have something about biases (using examples by RAND).

3 Workshop 2: The need for a TACTICS like system

The CCR Summit (see http://www.ccrsummit.com/) is an annual International Summit that successfully addresses synergies between stakeholders, policymakers versus operations and multi-agency collaboration.

In a 2-day program with 6 parallel streams of interactive Summit Break-Out Sessions, Master classes & Workshops challenges are assessed, discussed and addressed using (inter)national showcases.

Each year 450+ Public Safety & Security experts join this inspiring Summit to meet up with fellow professionals & selected industry exploring ways to maximize the results of collaborative efforts between different entities. Under the attendants you can find:

Directors, Decision-makers, Executives, Procurement Officers, ICT Managers, Project Managers from: Fire & Rescue Services, Health Services, Defence, Intelligence Services, Local & National Government Bodies, Police (Law Enforcement, Intelligence, Command & Control, Crowd & Riot Control), Public Safety & Security Related Industry.

The TACTICS project hired a room to present the TACTICS results and ask for input from the audience. The public version of the presentation can be found on the TACTICS website http://www.fp7-tactics.eu via News (http://www.fp7-tactics.eu/files/documents/TACTICS%20CCR%20Summit%202014%20public.pdf).

The audience were interested in a system like TACTICS. It took a moment to grasp the ideas behind TACTICS, then the audience asked several questions. For example about the innovation that TACTICS brings. They saw the added value to a security control room to see all data in on common operational picture.

The audience at TACTICS workshop during the CCR summit in Kerkrade The Netherlands.

4 Workshop 3: Video workshop with end users

4.1 Introduction

In recent years, the threat of terrorism has become an important issue, emphasized by several successfully carried out terrorist attacks in urban areas (New York, Madrid, London…). Characterized by high population density and vast metropolitan features, cities are very “attractive” to terrorists since attacking these locations has a strong impact in terms of number of victims, of emotions and sometimes in terms of cultural values.

In that perspective, the TACTICS European project offers to help security forces by developing three tools: The Threat Decomposition Tool (TDT) which provides knowledge about modus operandi, The Capability Management Tool (CMT) which provides knowledge about the resources security forces have at their disposal, The Threat Management Tool (TMT), which automatically uses both of the previous functions to allocate in real time resources to manage threats. TACTICS also offers a facilitation approach developed on three levels: Tactical (implementation manual), Operational (deployment strategy) and Strategic (policy recommendations).

In this context, CCTV brings high value as an observation device and is a primary focus in TACTICS priorities. Video monitoring assists the implemented tools in the study of the threat decomposition, and is a device easily usable by security forces.

The goal of this workshop was be to understand the usage of video analysis in the decomposition of terrorists’ modus operandi and the identification of the suspects. The objective was also to assess the current and expected benefits of the technologies to address future needs of Police forces.

4.2 NETHERLANDS: Focus on showing evidence

The Netherlands Forensic Institute (NFI) is funded by the Netherlands Ministry of Justice but is a real independent services provider. Police and Public prosecution are free to choose any provider. The service focuses on criminalistics and applies to post-event situations, to demonstrate associations between people, places and things and to analyse evidence.

The evidence from video images are unconditioned, they can be from:

-Surveillance video with problems of few images, poor quality and time-lapse

-Handy cam, webcam, telephone recordings with problems of moving camera, in- and –out zooming, broken/deleted video/photo

-Photo-material (police photos, ID-documents)

-Crime scene-registration (overview photos, trace photos, 3D lasers scan)

The specific video issues are:

-poor quality players (not all frames are shown)

-limited expert options

-Image degradation due to “grabbing”

-video recording from screens

-a video file can be unplayable

In general, initial analysis (material inspection, questions asked and investigational possibilities) lasts 12 hours, but Full investigation of the material, including reporting, can easily rise to 56 hours.

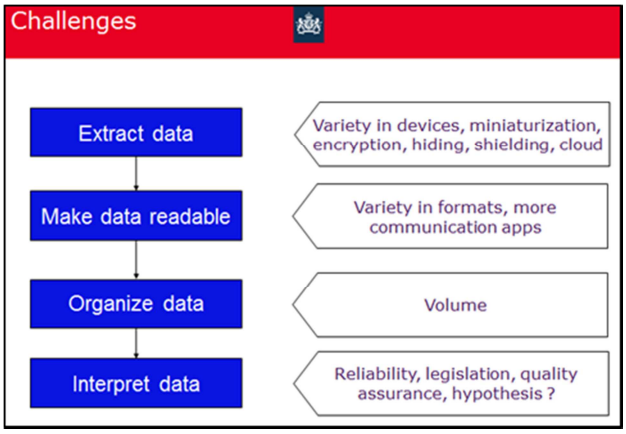
So the needs is of a software that does:

-3D model, photogrammetry (body height measurement and speed determination) and determining the time the recording was made

-Defraser to find and repair broken video files

-Comparison through PRNU pattern (Photo Response Non-Uniformity) which is the camera fingerprint, unique for every digital camera (also in webcams, phones and videos)

-NFI video player to view without installing and frame stepping



4.3 GERMANY: Focus on extraction of faces

RPKA's main task is to collect information on several monitored areas and to analyse all data. It is a huge amount of workload so they are searching for software that will take only movements for example. Except for crowds where the use case is to be able to detect if a wanted person appears in the march (hooligans for instance).

RPKA has islamists on a watch list in their zone and more over whole Germany: they need technology, they don't have enough resources to watch them 24/24, 7/7 and all-year long. Indeed, they would like to be able to do a motion picture with all the apparitions on a wanted person to detect the weak signals that could betray a suspicion of an attack coming soon. For instance, the Kouachi brothers in France were well-known and watched, but they haven't been able to detect the imminence of their attack besides the recurrence of their face apparition in watch groups. There is a problem of human resources and time.

They would like to extract automatically the data from a VMS to analyse it and save it once sorted out… but only the important part of it because:

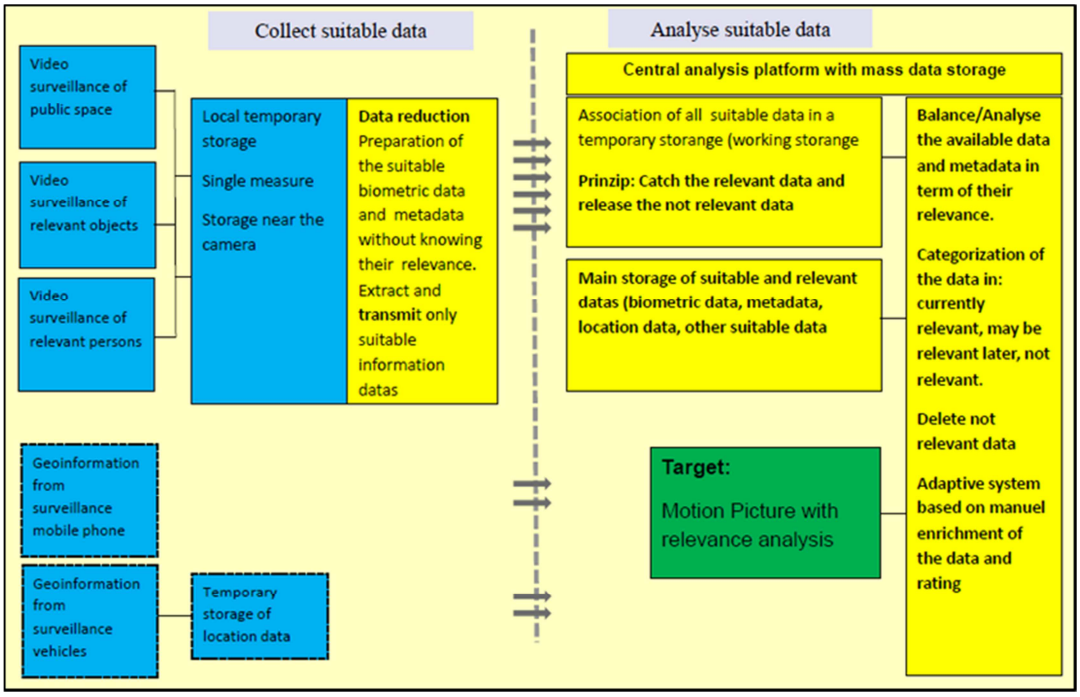
-they won't have time to analyse everything anyway

-in some cases they have to act really fast because the data could be erased after 24h (like in Mc Donald's)

-legally, policemen can only save images with people interesting for the investigation. Privacy and Ethics are issues too.

Of course, a solution installed in the VMS (and so the Police connect them on the VMS to withdraw in few minutes the results of queries) raises the problem of communication.

Exigencies of a solution:



4.4 UK: Focus on the different formats

The use cases of a London law enforcement agency are several but very different from the use cases of an Intelligence agency:

-Assisting DNA recovery from the video of a 7/7 Bomber handling a rail inside Tube carriage. To collect the images of a subway wagon, we have to go in it; there is no direct transfer to their VMS.

-Vehicle Identification from poor quality CCTV using unique features: they have to take a reference picture that can identify it in another way than just the license plate (how many stickers on the windscreen for instance)

-Bus CCTV used to confirm vehicle registration or mobile phone cell analysis used to locate occupants vehicle

-Suspect tracking using various CCTV sources (not unique VMS source: DAB, train, financial transaction in a supermarket…)

-etc.

For the 2004 London bombing attacks, a whole warehouse had been requisitioned to store all the CCTV exhibits recovered (80,000) but **less than 10% of each evidence collected were analysed and less than 1% were finally used**. And the storage cost a lot. But it was the only solution to be sure to have all the videos that “could” be useful were in our possession before their erasure.

Every day they are dealing with almost 200 video evidences of Counter terrorism; they have 21 people Full time just for this anti-terrorism matter, and the tasks load is increasing.

Cameras with more frames are amazing (like the 2012 Olympics HD CCTV) to be able to use the « zoom » and they hope all cameras will correspond to that quality in the future. Cameras’ quality is improving (multiplied by 3 for half the price) but remain low in municipalities ‘old installations. But currently, different formats are the main challenge.

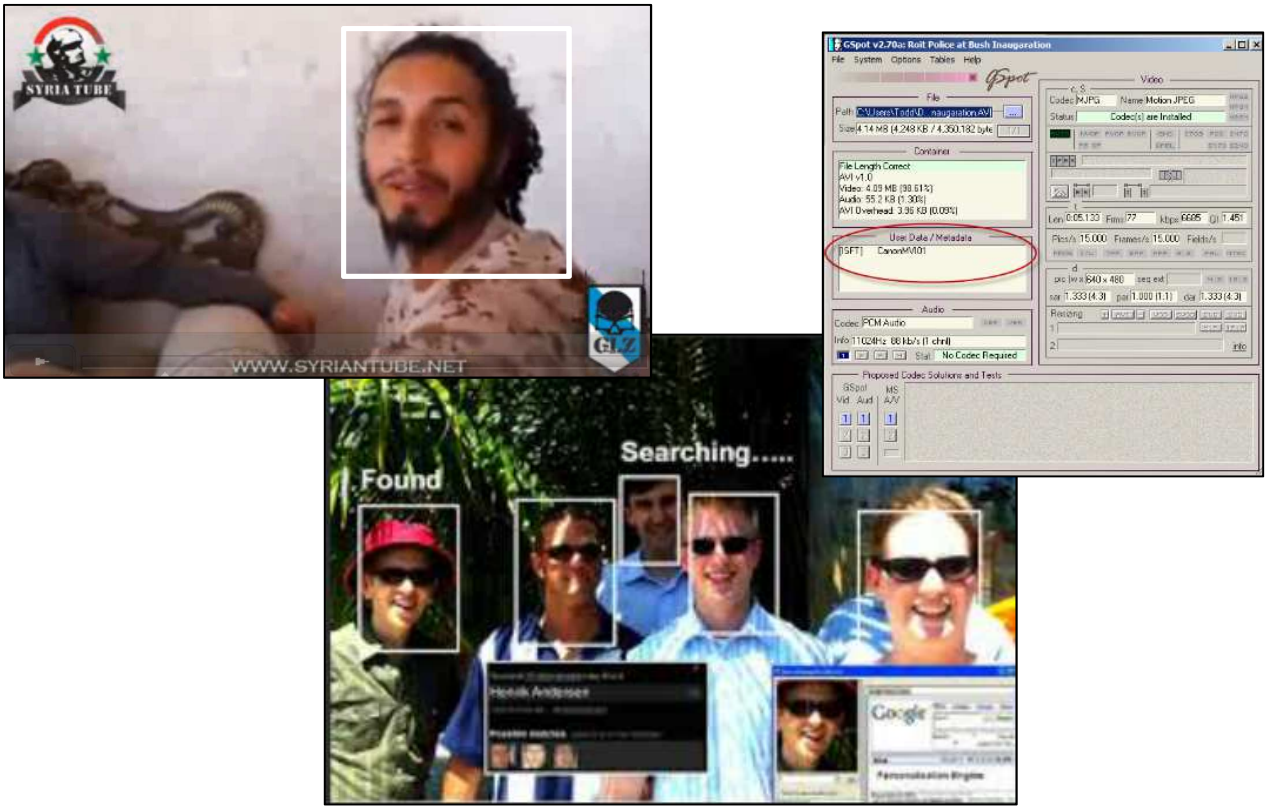
They dream of one software that transcodes all formats in almost real time. For closed systems, analytics can be performing, but as soon as it is in police real field, they face the problem of formats, and they don’t have time to wait for the transcode before being able to use analytics.

4.5 SPAIN: Focus on the huge amount of videos to analyse

Guardia civil, mainly the Intelligence Headquarter, has to face a huge amount of videos from different sources (CCTV, YouTube, social Media…) to be analysed. The analysts waste a lot of time trying to figure out which of them are interesting for the investigation, and which not (language is also a big problem in this task). Every month they have to extract hundreds and hundreds of faces from jihadist videos that they stock in servers for future comparison. And this is just for faces; they also need to extract pertinent logos, leads etc. or just mentions of “Al-Andalus”, which refers to Spain that Jihadist want to attack to “take back”. Once the interest determined, they need to extract metadata of the source (computer’s name, what camera used…).

Oppositely to the UK testimony, each video is visualized by several persons in Guardia Civil, to be sure not to miss something. All data might be important. They mainly focus on people and cars. The quality of cameras in Madrid is quite good. If they know who committed the act, they analyse days or even weeks before the act, in order to detect them doing a prior study. It is crucial to detect who accompanied them or which vehicle they used. They often share information with other countries through Europol or secured channels.

They would like a software that could allow to store all information, find relationship between people, organization, timeline… The solution could have false positive, but not false negative.


SYRIA TUBE
WWW.SYRIANTUBE.NET
GSpot v2.70a: Riot Police at Bush Inauguration
Found
Searching.....

4.6 FRANCE: Focus on the relative good quality of their video sources

Major events that have highlighted the new needs:

London riot 2011(UK): 150,000 hours of CCTV

Stanley Cup riot (CAN): 5,000 hours

Boston marathon (US): 6,000 hours

“We will go through every frame of every video to determine who exactly was in the area” internet vigilants speculate at Boston (extracted from an article of The Independent).

The French DGSI (Direction Générale des Services Intérieurs) has the same problem as their European colleagues about the volume of data to analyse every day and about the poor quality of some YouTube videos downloaded from Syria or IS. But all the resources from their stakeouts are of very good quality because of the cameras they use (with even larger amount of data to analyse).

Their main need would be to be able to identify one person appearing in a video from YouTube or from their stakeouts. They also need to extract all the faces from a video, all the faces good enough to be automatically identified with a comparison 1 against n.

Use case: one jihadist came back from Syria: they need to know if they already have him in their databases and add this picture to all the data they have about him.

*

Question of format:

Industries cannot be forced to adapt a unique format so there is a need to find a universal reader and to analyse terabits of videos. They are always searching for new software that could help them. A standard couldn’t be possible for intelligence services because they also rely on video data from citizens, mobile phones etc… Therefor a solution reading only few formats could be interesting on some important CCTV (casinos, hotels chains …) but not for private ones. Even the Intelligence services choose specific cameras for specific purposes. For example surveillance mission during nights have special cameras.

Nonetheless, it worth trying to impose a format to let the majority of evidences in the same format, and have a small part in other formats. ISO 22311 is a first step to try imposing a standard for videos of video surveillance. Of course cheap Chinese material would be bought by people but even if only 10% of all the material were on this same standard, it could be a huge benefice step.

4.7 Presentation of TACTICS project: modus operandi and pattern realized by taking post-event investigation results into account

4.7.1 Trends in biometrics searching for new modalities

ITTI is both an independent consulting firm in the area of telecommunication, IT and business; and applied research institute in Information and communication Technologies. Its expertise related to video processing gathers: video coding and compression; image analysis, processing and pattern recognition; biometrics; telemedicine; CBIR systems and machine vision and robotics.

To ward off the disadvantages of the traditional methods in human identification, ITTI presented the trends based on image analysis, with the emphasis on perspective biometrics. Biometrics show characteristics valuable in identification like universality, robustness, measurability, performance, acceptability, circumvention or uniqueness.

Nowadays, mobility, multi-modality, user acceptance, contactless and liveliness detection are the factors driving research. In the future, research tends to enhance biometrics in the head and face vibration during speaking, the electrical and magnetic field analysis, and acoustical holography.

4.7.2 The TACTICS' Threat Management Tool

UPV, Universidad Politècnica de València, has been working on the TACTICS project from the modus operandi side.

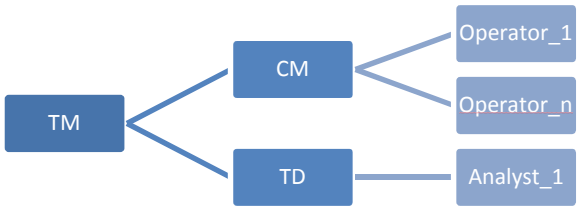
UPV innovation provides sensor integration such as public traffic camera or video integration from mounted cameras on FR or vehicles. It analyses information about past events to establish a modus operandi and define the likeliness to happen of an event. Its objective is to eliminate bias thanks to the studies led by TNO.

It can show where units are located and many other data. Videos can be sent directly to the Central and they are geographically marked. The commander can then chose, according to what he sees, how to react and to organize his capabilities. He can set up alarms for defined threats.

4.7.3 A Comprehensive Approach to Capability Management

Fraunhofer is Germany's leading organization for applied research and technology transfer. In TACTICS, they lead the development of the Capability Management Tool (CM). In a context of time pressure as during a terrorist attack, Human decision-making processes rely almost entirely on feelings, experience and informed decision. The results are that some potential solutions are missing, and decisions are biased.

To avoid wrong decisions, the CM provides knowledge on the current capabilities that security forces have at their disposal at the threat locations. The tool implies key actions: apply systematic portfolio management, keep track of your knowledge and new developments, think beyond traditional borders and teach the staff to develop their capabilities.



TACTICS' communication triangle

Workflow:

1. Specification of resources capabilities
2. Acquisition of resources
3. Matching: request from the TM
4. Deployment: connect everything
5. Information from the CM to the TM

Yet, this tool still faces challenging issues: insufficient human resources to maintain such a system, experts need to be in the field instead of the office, it is another system with screens, and there is limited time to train people. Moreover, the emphasis is made on the issue of privacy and ethics. Does 100% surveillance lead to 100% public security?

4.7.4 Multi-camera person tracking and behaviour recognition

TNO was founded by law in 1932 to enable business and government to apply knowledge. As an organization regulated by public law, they are independent. They create innovations that boost the sustainable competitive strength of industry and well-being of society. In TACTICS, they worked on automated processing of camera images that can help operators to follow persons, or to find where a person was before. Recognizing actions such as loitering or running may help finding suspect behaviour. TNO innovation uses track information, similarity and motion to find relevant cases.

Operators can be helped by

-assisting in finding people by appearance (past or present, running in a field-lab in a shopping mall)

-being alerted to specified behaviour (planned for June 2015 at Schiphol for a few cameras)

Then real-time processing is becoming possible. False alarms are still occurring but few enough for an operator to handle. They use weak signals:

-a similar person may not be the suspect

-a certain behaviour may not be 100% correlated to a threat

-Combination may be enough to find a suspect.

4.7.5 Integrated solution for post-event video analysis

After a long process of comprehension of the needs of Public security agencies in the video field, Morpho has developed a multi-modal solution to help the investigators analysing an increasing volume of video data.

The solution aimed at helping the investigators to go FIRSTLY to the most important chapters and to dedicate someone on it for example. The idea is to have a pre-selection to earn time and generate leads as fast as possible. Is it not only to reduce workload, but improves it, provides leads to resolve more cases, and to permit the work of several shifts or teams on a case, without losing data and time. Analytics are not all the solution, they are part of, and it permits to sort out videos. In the current architecture, there is a specific module to host detectors. This module has been built to be agnostic to the type of object detected. Today it already detects faces, fingers, iris and people. Moving forward, this module shall be able to host any favourite detector. In the meantime, Morpho will be able to integrate it – if the provider agrees. The system doesn't include a possibility to resynchronize in date and time the different videos (with a sound that could be recorded with different image flows) so far but we plan to offer a manual re-synchronization.

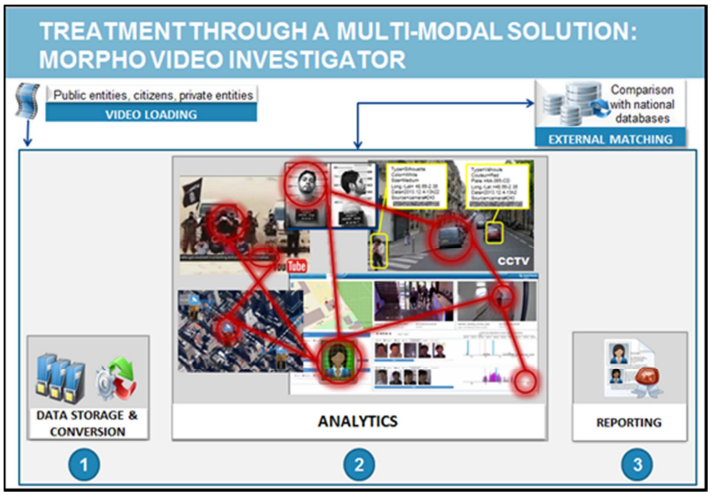
Currently we first need to import and index videos (50h in 10h). In another step we would like to have the analytics closer to the VMS to use the analytics close to real time.

The solution is based on 3 main steps:

1: Importation of video data from public entities, citizens or private entities, data storage, conversion into a same format (we don't have a universal reader but we convert as many format as possible) and indexation

2: Use of analytics through a flexible interface. Analytics are add-on , can be changed, upgraded etc. For instance: gender, movement, age, persons, vehicles, faces, licence plates… A link with national databases can be done.

3: The semi-automatic building of a report thanks to image bookmarks realized during the investigation through the analytics interface.



4.7.6 Conclusion

Tactics holds its objectives in its concept, that has raised interest of the present agencies that have found it very capable. Nonetheless, they have précised that its feasibility and pertinence can't be assessed if not in the concrete field, to test on their different realities they have to face:

- heterogeneity of their systems and of the quality of those systems

- heterogeneity of the end-customers

The concept has to be thought in an incremental way to build different layers step by step, while having field's assessment and on-the-go upgrades. It has to be decomposed for each end-user.

Agencies are confronted to a diversity of field realities…that lead them to various requirements.

5 Workshop 4: Deployment strategy workshop

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

Agenda

15.30 Welcome by Dr - (RAND Europe)

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

15.40 Presentation of findings from TACTICS

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

16.30 Facilitated discussion on the policy implications (RAND)

17.00 Reception hosted by RAND Europe

Consortium attendees:

Title	Name	Organisation
Ms		RAND
Dr		RAND
Dr		RAND
Mrs		RAND
Dr		RAND
Dr		PRIO
Ms		PRIO
Dr		TNO

Participants:

Title	Name	Organisation
Mr		NATO
Dr		NATO
Ms		Cypriot PermRep to the EU
Ms		EPP Group in European Parliament

Mr		Knowledge, Risks and Urban Environment Unit, Environment DG, European Commission
Mr		DG HOME, European Commission
Mr		DG HOME, European Commission
Mr		Belgian Federal Force, Direction Special Units (DSU)
Dr		AIRBUS Defence and Space
Ms		NATO

Three additional participants had signed up but didn't attend

Summary of discussion and questions

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

6 Final exercise

6.1 Introduction

The final exercise for TACTICS was organised at UPV's premises in Valencia (26-28 May) with an audience of nine interested stakeholders from the end-users community and policy makers.

Below several pictures to give an impression of the setting of the Final Exercise.

Figure 6.1 The people operating the TDT, TMT and CMT.

Figure 6.2 Interaction with the audience.

Figure 6.3 Discussion to obtain feedback from the audience.

The goal of this event was not to validate the system itself (already validated during the first and second FEX), but to showcase TACTICS' maximum (current) potential in assisting the management of a terrorist threat.

The one-day event included three sessions. The first session was dedicated to a set of briefings conducted by consortium members to present the TACTICS system, its tools and signature features. The goal of these short briefings was to allow the audience to acquire a basic understanding of how the system works before the demonstration started.

The second session was the demonstration itself which was then followed by the third and final session during which the audience had the opportunity to comment and ask questions.

6.2 The demonstration

As stated in the introduction, the goal of the final exercise was to illustrate what TACTICS is capable of at its current readiness level (TRL-5) and solicit feedback from the external audience.

To achieve this goal the scenario was slightly modified to maximise the use of certain capabilities and the roles of the three managers were played by internal consortium members who were familiar with TACTICS tools. The scenario feeds and the related follow up actions undertaken by the managers were scripted and agreed among all participants.

The demonstration lasted just under one hour and was able to successfully illustrate TACTICS capabilities.

6.3 Feedback from the audience

After the demonstration, a Q&A session was conducted with the stakeholders present in the room. A list of questions and related answers can be read in Annex B. Particularly relevant were the comments made with regard to the possible future deployment of TACTICS and the criticality of its integration with current systems. In addition, it was noted that TACTICS could also be further developed into a powerful tool for the training of emergency managers (e.g. computer-assisted exercises).

In addition, the participants were also asked to complete an evaluation questionnaire following the TACTICS demonstration. Six participants (4 end-users, 1 liaison officer, and 1 private company observer) completed evaluation questionnaires (Questionnaire template available in Annex C).

Overall, all participants who completed the questionnaire indicated that they liked the TACTICS system that they observed on the day. Also, all six participants agreed that the TACTICS system enhances the situational awareness in a crisis management situation. In addition, the six participants all agreed or strongly agreed that TACTICS enables better decision-making in managing a terrorist crisis incident.

With regards to the extent to which TACTICS helps mitigate potential bias in decision-making, one participant disagreed with the statement, whereas the remainder of the participants either agreed or strongly agreed.

Half of the participants indicated an interest in the system as a whole, whereas the other three were split between not indicating particular interest (1), mostly interested in TDT (1), mostly interested in TDT and TMT (1).

Three participants indicated an interest in investing in a TACTICS-like system. The other three didn't answer this question. Those who indicated an interest, didn't currently have a system like TACTICS in place, and considered the system to be able to improve situational awareness, decision making and preparedness of security forces, in addition to managing their capabilities better.

6.4 Summary of main findings from the final exercise

The demonstration exercise successfully illustrated TACTICS capabilities, including some of its signature features such as behavioural analysis, face recognition and counter-bias. The feedback from the audience was positive and validated not only the system as a whole, but also its operating concept.

The comments suggested that, if properly integrated and connected with existing systems, a system like TACTICS could improve situational awareness, decision-making and preparedness of security forces, in addition to allowing for a better management of capabilities.

In addition, the audience suggested that TACTICS could also be further developed and used as a powerful training tool for officers and/or entire teams who would be exposed to many of the aspects of real life operations and events in a close-to-reality environment.

7 TACTICS Pre Commercial Procurement and Follow-up strategy workshop

Subject	***TACTICS Pre Commercial Procurement and Follow-up strategy workshop***		
Location	**TNO** **Meeting room 07.010** **Anna van Buerenplein 1** **Den Haag**		
Date	Thursday 13 August 2015		
Invitees			
	Europol		
	RB&W		
	V&J	Ministry of Defence	
	KMAR		
	KMAR		
	KMAR		
	ENLETS	European Network of Law Enforcement. Technology Services	
	NP/KLPD		
	NP/KLPD		
	ISCA		
	TNO		
	TNO		
	TNO		
	TNO		
	TNO		

Objectives :The goal of this meeting is to investigate how we can extend the TACTICS concepts beyond the end of the TACTICS project.

For example via a Pre Commercial Procurement (PCP), which was recommended by the reviewers . TACTICS is on TRL level 5/6 , a PCP would allow to reach higher levels TRL 9, using financing tools like the EU – Pre Commercial Procurement.

Agenda:

Welcome (TACTICS Consortium Manager TNO)

TACTICS system & concept and Privacy by Design presentation (Technical Project Manager TNO)

Fusion Unit and Face Recognition presentation (TNO)

Appreciation of TACTICS results (Advisory Board member)

We start with an update for people who were not able to join IFSec or the Advisory Board meeting of 7 July:

Notes:

The TACTICS team asked the Advisory Board on their ideas about a PCP Pre-Commercial Procurement project as a follow up on TACTICS in the meeting of 7 July.

-A problem with procurement is that centralized purchasing (inkoop in Dutch) organisations tend to buy the most economic product with only 80% of the end users (e.g. police) wishes. Therefor it is important to connect the purchasers/acquirers (inkopers/verwervers in Dutch) to innovative/new tools.

-Europol is interested in a follow up of TACTICS, involvement of national police is conditional.

During this meeting the attendants added to that:

-The Dutch police has had a meeting with one of the consortium members (Fraunhofer) about a proof of concept follow up system for capability management. So they are interested in parts of TACTICS.

- The process of PCP can go via the ministry of Economic Affairs. They have much knowledge about this.

During the TACTICS (dissemination) meetings we noticed that about 3 European countries have interest in (parts of) TACTICS.

The Dutch police (KLPD) doesn't have interest in a TACTICS PCP at this moment, they have other priorities and are not interested to commit to long term projects now. There is a general interest in a PCP, depending on subject and timing.

KMAR has staffing issues, but sees opportunities for an TACTICS PCP.

KMAR has to be able to combine this with their strategic roadmap.

UK/AUS/USA are innovative countries and good to cooperate with.

Next steps:

- KMAR and RW&B will investigate if it is possible to organise a meeting on the CCR summit.
- CCR summit is attended by many people and decision makers in the TACTICS target groups.
- This will allow to check, if a sufficient number of end users are interested to start a PCP.

8 Final event

TACTICS was presented successfully during IFSec 2014 in an open theatre (as shown below).

The consortium decided to make use of the large audience to organise the final event during IFSec 2015. The audience consists of more than 40.000 global security professionals: security managers, loss prevention managers, facilities managers, installers, integrators, electricians, consultants, architects and specifiers to network, source solutions and discover what the future holds from our leading suppliers.

This time we hired a closed room to allow more private interaction with the audience.

Three complementary ways were used to draw the attention towards the TACTICS project and her results. The project used a part of the booth of the project partner Morpho, flyers were presented with an attractive text and an interview was given and shown on the big screens in the IFSec hall where hundreds of people walked during the day.

1. Booth:
2. A TV interview
3. TACTICS panel discussion

8.1 TACTICS Booth

The Morpho booth with the TACTICS corner on the right site, before the start of the conference.

A TACTICS consortium member in discussion with a visitor of the Morpho booth.

TACTICS at the booth with visitors.

8.2 TACTICS Interview

The interview about TACTICS at the TACTICS booth.

The interview was shown in the hall of the IFSec conference where thousands of people walked through.

8.3 TACTICS Panel Discussion Flyer

A flyer was used to attract people to join the panel discussion: The flyer was distributed to promote the panel discussion in the private room and is shown below.

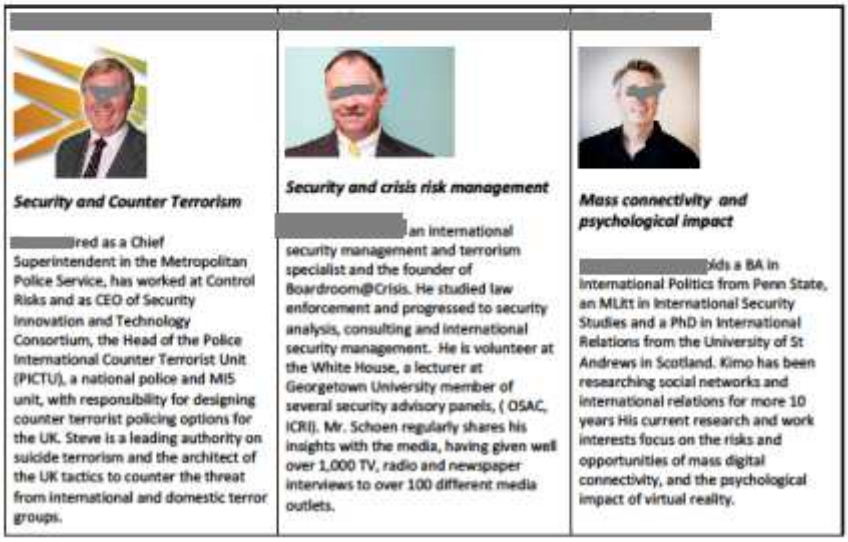
Join the TACTICS Panel discussion!

Recent terrorist attacks in European cities as in Paris and Kopenhagen show that the need for a fast well organised response is actual. The results of the European research project TACTICS supports security forces in creating a fast coordination and overview to accurately respond to threats.

Join the panel discussion and see how:
-your products can be connected
-your expertise can be assisted
Towards a safer world!

Please help us with your input:
improve TACTICS and bring it to daily practise.

We are proud to present our inspiring panel members:



Security and Counter Terrorism

[redacted]red as a Chief Superintendent in the Metropolitan Police Service, has worked at Control Risks and as CEO of Security Innovation and Technology Consortium, the Head of the Police International Counter Terrorist Unit (PICTU), a national police and MI5 unit, with responsibility for designing counter terrorist policing options for the UK. Steve is a leading authority on suicide terrorism and the architect of the UK tactics to counter the threat from international and domestic terror groups.

Security and crisis risk management

[redacted] an International security management and terrorism specialist and the founder of Boardroom@Crisis. He studied law enforcement and progressed to security analysis, consulting and international security management. He is volunteer at the White House, a lecturer at Georgetown University member of several security advisory panels, (OSAC, ICRI). Mr. Schoen regularly shares his insights with the media, having given well over 1,000 TV, radio and newspaper interviews to over 100 different media outlets.

Mass connectivity and psychological impact

[redacted]ids a BA in International Politics from Penn State, an MLitt in International Security Studies and a PhD in International Relations from the University of St Andrews in Scotland. Kimo has been researching social networks and international relations for more 10 years His current research and work interests focus on the risks and opportunities of mass digital connectivity, and the psychological impact of virtual reality.

The flyer at the entrance of the hired private room is shown below:

8.4 Highlights in the panel discussion

After the explanation of what TACTICS is by the technical project manager as shown in the picture below, the panel members shared their opening statements and visions.

The panel members started with the following opening statements:

1. TACTICS is especially necessary since the latest way of working of terrorists is to have several smaller attacks carried out by small groups of persons. The attacks are mobile and multi target. Therefor there is a chase involved. Furthermore 85% of the camera's is in private hands. In order to successfully mitigate threats it is important to use these private CCTVs.
2. Also the terrorist don't warn anymore in advantage, compared for example with the IRA. They used to warn the authorities before the attack. We can't stay at high alert all the time, therefor our response to threats must innovate. TACTICS can assist with this, I see it as a useful platform to manage resources quicker.
3. The public will want a system like TACTICS. Trust is essential. Trust is related to transparency and therefor the authorities have to communicate emotionally about a system like this. For example about where the data is stored, who can access it. So a key question is: How do we communicate Privacy by Design. All of what is sketched today will be there in the future. If the EU and research consortia like TACTICS won't do it, the private sector will push it. Keeping humans in the loop is essential to trust.

Then questions were asked resulting in the following highlights:

Former Scotland Yard member: in the UK there are 6,5 million camera's, giving hours and hours of footage that nobody can watch all. Therefor the automated selection of relevant footage is an advantage.

Privacy and trust panel member: if we look back into history we see that when a catastrophe happened, there were many small series of discussions, but in the end somebody has to say no. To use a system like TACTICS for forensics is okay, but predictive is not all right. The vision on what is allowed changes in society, this is in relation with democracy. For example in recent history we have seen that a rebel can be democratically chosen as a new political leader.

Question of police officer in the audience: How can we get the public to support us?

Privacy and trust panel member: we are often to rational in our communication, we should use emotional communication to be more effective.

We discuss Charlie Hebdo as an example how TACTICS could have been used.

Former Scotland Yard member: TACTICS can support with detecting the reconnaissance of attackers and spotting anomalies. It is hard to tell when TACTICS can be switched off again, some threats take 3 minutes others, like Mumbai, 3 days. Also it could broadcast a message to the first responders, for example move the VIP away, lock a building, stop buses and get people out. Everything you can do to make the situation different from what the attacker expects, disrupts them.

Privacy and trust panel member: there is a 25% cut in budget and 85% cut in security personnel, but the public expects the same service level. Therefor there is a strong need for a system like TACTICS.

Privacy and trust panel member and End user: The TACTICS concept should not be used for terrorist crises only. We must think about how to make it a tool for daily use, with (privacy) levels. Parts that can be used in case of a robbery and parts that can only be used for terrorist threat.

Security- risk manager and deployment member: ask google or twitter to the table. How hard would it be for you to make a TACTICS-like system? What challenges do they see? Also the fact that an attack is world news within half an hour is an extra reason to structure. This helps forces to give a public response.

Former Scotland Yard member and member of the audience: TACTICS cannot be switched on and off in 1 location because the attackers move to several places nowadays.

9 References

TACTICS Consortium. (2014). *D9.2 Dissemination plan.*

http://www.ifsec.co.uk/

http://www.ccrsummit.com/