TACTICS
TACTICAL APPROACH TO COUNTER TERRORISTS IN CITIES

NEWSLETTER
ISSUE 02 - MAY 2015

TACTICS CAPABILITY MANAGEMENT TOOL

The purpose of TACTICS' Capability Management (CM) is to improve the knowledge on the available capabilities at security forces' disposal. Indicators of a potential threat, provided by the Threat Manager (TM) are matched to available capabilities, i.e., detecting a certain behaviour (indicator) might be matched to security staff, camera surveillance. The matching yields a dynamic overview of most appropriate and available capabilities, aiming at improved detection circumstances. In addition, CM supports the management of capabilities.

In contrast to existing resource management systems, TACTICS' CM starts with TM's information needs instead of resource availability. So, instead of requesting a CCTV camera, the manager would request a location to be put under observation. This could be implemented with a camera, but also with other means. This is a lighter version of the strategic variant of capability management, which is in a defense context used to manage change, procurement and innovation on an organizational level. In TACTICS, capability management is applied on specific threats.

It is obvious that not every urban environment has all the capabilities that would be needed to detect specific signs and behaviours as required instantly up and running. Nor do the counter terrorism forces have the knowledge of all potential local capabilities that could be used in case of a threat. For example, most European shopping malls are not equipped with any means for detecting weapons but do have a variety of public and private cameras and security staff. The question is how counter terrorism forces get an overview of what capabilities are (potentially) available at a specific location, and which means would be best suited to detect the specific signs and behaviours in the given situation.

Each capability has its strengths and weaknesses that need to be known to allow for their management by combining them to create optimal detection circumstances. Some coherent, yet non-exclusive examples are given below:

- Intelligent cameras are better at detecting deviances across large spaces and times compared to what security officers can see. However, they currently have problems detecting detailed behaviours.

- Camera operators have the advantage of being able to see more detailed deviances in large spaces. However, a disadvantage is that they are not good at detecting deviances over long periods of time because they have limited attention spans and work in shifts.

- Floor security has the advantage of being able to see very detailed deviances from a very small distance. Also, the people who actually walk around the location are the only sources that are capable of acting directly after they see something deviant. However, humans are susceptible to biases such as prejudice or stereotyping.

- Databases may have large amounts of information in a way that is easy to process, but they are historical data, and only give a prediction instead of a description of the present, as a sensor would give.

The CM, as any other information management system has to be integrated into the overall workflows of respective forces.

TACTICS CM goes beyond the state of the art by supporting security forces (1) to systematically create an overview of the current capabilities available at urban locations and the capabilities that would be needed, (2) to prevent or deal with an attack, and (3) to create optimal detection circumstances, taking into account each capabilities' strengths and weaknesses.

FACE RECOGNITION

Identifying dangerous people is key to prevent incidents in public places. By setting up surveillance cameras at strategic points equipped with face recognition software, known individuals can be recognised and identified by the system in real time. In the same way, CCTV recordings of incidents can be submitted to a face recognition system. Comparisons may then lead to the identification of suspects or at least provide investigators with information to track them. Detecting abnormal behaviors can also be performed thanks to this technology: a person detected several times in front of a camera which is installed near a sensitive building can be considered as suspicious.

Recognizing faces is the most natural thing to do for the human brain. Besides, capturing portraits digitally is easy: contactless, with no need for specific equipment now that cameras are everywhere, in the streets, in computers, even integrated in the smartphone in your pocket. But when it comes to identifying someone from his or her face, it is not because it is natural that it is simple. The face is a three dimensional ever changing object always in motion. For an efficient identification system, face recognition technology starts well before image comparison.

DETECTION

The first step is to detect the face in the images collected from the source. It can be easy in static images such as identity documents with standardized pose, lighting and plain background. It can be a huge challenge in video streams with multiple persons in movement and a busy background. The goal is then to detect faces successfully, which means maintaining a low rate of false face detection. This stage is performed with a classifier that indicates whether an image of fixed size represents a face. The classifier learns from a database of faces and non faces.

IMAGE ENHANCEMENT

Once the faces have been found and adjusted to the same scale and position, they need to be enhanced. This involves minimizing the effects of compression, correcting inconsistent lighting or detecting and excluding unusable zones (masked by clothes for example).

Figure 1: Face detection on a given frame

FEATURE EXTRACTION

The image is processed to extract information and convert it into a digital description for computer-based comparison. Every face has numerous, distinguishable traits, such as the distance between the eyes, the width of the nose or the shape of the cheekbones. Face recognition algorithms rely on those feature points but also on mathematical information not identifiable by the human eye.

Figure 2: Feature extraction: Hierarchical graph matching

COMPARISON

Once the face features are extracted, they can be compared to the ones in the database or a watchlist and identify whether the person is already in it or at least get a list of potential candidates who look like him/her. The comparison, or matching, is achieved through a succession of algorithms in a multi-stage architecture: the first ones are conservative and fast, the last ones are slower but very selective. Each matching step provides a candidate list of which only the top is used for the next step. This approach narrows down the list to be able to use more demanding algorithms efficiently on a smaller amount of data. This process ensures both high accuracy and fast matching. The outcome of the comparison is a matching score per candidate measuring the similarity between two sets of face features and reflecting the confidence level that they are coming from the same person. The final step involves score normalization, in order to guarantee the matching score remains stable.

DECISION

In law enforcement scenarios, a human reviewer is usually employed to systematically review the candidates returned from an identification search. Usually, the reviewer inspects the suggested candidates ordered in descending matching score, stopping when he is able to positively confirm a mate. The length of the candidate list may be fixed or variable by applying a threshold. In this case, he only reviews the candidates with a matching score above the threshold. Thanks to accurate face recognition algorithms, with images

of reasonably good quality (such as mugshot), the use of such a threshold allows for a dramatical reduction of the reviewer workload. Indeed, the reviewer will only receive a small number of images that stand a high chance of matching the wanted person, thus preserving his time and attention to process more cases or spend more time on critical cases. In blacklist management cases, the information will be generated only if the matching score of at least one candidate image is above the threshold. In this case, only the image of the first candidate will be sent to the operator, who will verify the detected person and his corresponding match are the same person.

FUTURE

During the last decade, face recognition research methodology has matured, sizable training databases have been collected, and the feedback from practical deployments has been incorporated, which has led to a dramatic jump in accuracy. The last NIST benchmark's conclusions are clear: face recognition technology is mature enough for operational use in identification systems with frontal images in a controlled environment. Efforts do not stop here. Research is moving forward on accurately processing more difficult images and video sequences, with lower resolution and a less controlled environment. Some of the challenges include external factors (such as lighting) or subject cooperation (for instance facial expression or occlusions). Addressing those challenges will lead to an increased performance and an extended range of applications for face recognition.

FACE RECOGNITION

Legend- Netur ad qui omnistor aboressequi si delecto ene volo maio mint arcid quidessunt as volorroltatiae exceraturi andi temquae nimodiame prest moditatur autet, con comnitibus modit, ventios dolupta tistrumet utemquiat.

The purpose of the TACTICS validation exercise is to authenticate the functionality of the TACTICS system and to showcase its developments beyond the state of the art. We do this by bringing together all of the elements of TACTICS—both as a project and as a system— to address a simulated scenario in which there is a known specific threat to public safety and/or an actual terrorist attack.

We used the scenarios developed in TACTICS Work Package 2 as a starting point for the validation scenario (FEX Scenario), and have dedicated considerable effort toward formatting the FEX Scenario in such a way that it is at once operationally realistic and a suitable platform by which to display the added value of the TACTICS developments and capabilities. Throughout the course of the validation process, from FEX scenario development to participation in the exercises, we have exploited the advantage of having end users within our consortium. The input and contribution of consortium members Dutch National Police and the Dutch National Marechaussee are of great importance in ensuring relevance and innovation.

We decided to carry out the TACTICS validation in four phases in order to allow us to continually improve the tools, the scenario and the execution of the exercise in parallel. Separating the validation into phases ensures that we will arrive at the best method of showcasing TACTICS to the stakeholders and provides us with the opportunity to tailor the tools to the end users' needs. With the TACTICS validation process we strive to show TACTICS as a user-friendly system of tools that offer end users significantly improved work processes and results, and to exhibit some of the specific unique attributes of TACTICS such as its use of morphological

analysis, face recognition, privacy by design, counter-bias mechanism and deviant behavior detection.

We have currently completed two of the four phases of validation. End user feedback at this point has been generally positive. As we are approximately half way through the validation process, final conclusions cannot yet be drawn. From the end user perspective, the main added value of TACTICS at this point is speed as it relates to improved decision making. With TACTICS, end users could make decisions earlier and take actions faster, which presents the possible advantage of preventing damage and saving lives, all of which stem from the main added value of speed. The phased approach to validation provides us with the opportunity to incorporate end user feedback and suggestions to maximize the added value of TACTICS.

TACTICS Validation Phase 1 took place in Hoofddorp, the Netherlands in May 2014. The goal of the first phase of validation was testing the implemented requirements of each of the TACTICS tools, further development of the FEX Scenario and preparation for TACTICS Validation Phase 2. After this phase of validation we were able to detail the implemented requirements for each tool and confirm that they were all up to standard.

TACTICS Validation Phase 2 took place in Delft, the Netherlands in September 2014. The goal of the second phase of validation was to get feedback from end users on the tools and the FEX scenario. To do this, we organized a classroom exercise by which end users used the tools with the FEX Scenario that we developed. After the exercise we had an immediate debrief with the end users and the consortium members, during which we noted positive feedback and improvements to be made for TACTICS Validation Phase 3.

TACTICS Validation Phase 3 will take place Thursday 28 May 2015 in Valencia, Spain. The goal of the third phase of validation will be to expose TACTICS to a broader end user participant audience and therefore garner more opinions and feedback from the end user community. The goal of the Final TACTICS Validation Exercise will be to hold a larger-scale exercise with an enhanced version of the TACTICS system and FEX Scenario. We will film the final exercise and will be able to use this video for dissemination purposes.

Following the validation exercises there will be a data analysis of the preliminary implementations of TACTICS, which will contribute to the TACTICS Instruction Manual explaining how to apply the TACTICS system in any urban environment. In addition to technical instruction, this manual will also address change management, including how to easily facilitate a transition to more effective public security on a tactical level. In light of the expanded communication network of relevant entities involved in threat and/or crisis management that TACTICS brings, this manual will be published in two levels of security classification in order to protect the security and privacy of the public.

The TACTICS validation brings all aspects of the project together, showing our research, development and innovation coming to fruition in our trial exercises. Through the TACTICS validation process, especially the more advanced phases, we are able to showcase the beyond the state of the art capabilities of TACTICS to stakeholders and end users. It is furthermore a platform for us to exemplify how TACTICS addresses present-day challenges, specifically that of an impending or actual terrorist attack in an urban environment.

PRE ANNOUNCEMENT – TACTICS – END EVENTS – Save the dates!

The TACTICS project will end this year. To get a better grasp on TACTICS and what it can do for your organisation you are invited to attend the following TACTICS events:

- **The final exercise** will be presented **Thursday 28 May 2015** in Valencia, Spain

- **The results of TACTIC** will be shown, during the well-known IFSEC International 2015 Conference, **Wednesday 17 June 2015** in the South Gallery 8.

During this conference, the results of the project will be presented and leading experts in the field will discuss the findings. During the event, participants are invited to participate in discussion sessions addressing different security topics.

The IFSEC takes place from 16-18 June 2015 in London. Registration is free. For more information see www.ifsec.co.uk

YOUR CONTACT

For more information on TACTICS, please contact:
info@fp7-tactics.eu

VISIT TACTICS WEBSITE

http://www.fp7-tactics.eu/project.html