ICT Trends in European Policing

COMPOSITE

Draft of Deliverable D4.1

COMPOSITE
COMPARATIVE POLICE STUDIES IN THE EU

Photo: David Adams

Authors: Sebastian Denef[5], Nico Kaptein[8], Petra S. Bayerl[1], Kamal Birdi[7], Fabio Bisogni[12], Damien Cassan[9], Jochen Christe-Zeyse[4], Pietro Costanzo[12], Mila Gascó[13], Kate Horton[1], Gabriele Jacobs[1], Theo Jochoms[3], Katerina Krstevska[15], Stojanka Mirceva[15], Ad van den Oord[10], Catalina Oțoiu[11], Rade Rajkovchevski[15], Zdenko Reguli[14], Trpe Stojanovski[15], Gabriel Vonas[11]

This research is partially funded by the European Commission as part of FP7 in the context of the COMPOSITE project (contract no. 241918). This report is the draft of a public deliverable to the European Commission (D4.1 Analysis of technology trends for policing)

More Information:
www.composite-project.eu

1-15 See affiliations on page 7.

Summary:

ICT Trends in European Policing

In this report we present the results from interviews and document analyses of current and planned information and communication technology (ICT) projects with police forces from 10 European countries and from interviews with technology vendors in the field of ICT for policing. Based on a cross-country, cross-organisational analysis, we present the following themes that describe major trends in ICT for European policing:

» the integration of intelligence data systems
» the adoption of mobile computing
» the use of video surveillance technologies
» the application of digital biometrics
» the crosscutting issue of user acceptance
» the emerging challenge of social media applications

We discuss how these issues are relevant and thereby point to open issues for future research.

Contents

Introduction:

Studying ICT Changes in European Policing

Recently, rapid developments in the field of ICT have had a major influence upon police work. Technological innovations turn out to change the organisational environment in significant ways. For police, ICT plays a twofold role: New technologies can support police work but also provide new opportunities for offenders to commit crimes.

Within the COMPOSITE project, a European-wide research project aimed at investigating change within police forces, a dedicated work package ‘Technology Adaptation’ specifically focuses on change processes relating to ICT.

As a first step, the trend analysis presented in this report scans for current ICT developments and thereby provides pointers for future research.

Researching Changes in European Policing: The COMPOSITE Project

The COMPOSITE project performs comparative police studies in the European Union. The project brings together researchers and police forces from Belgium, the Czech Republic, France, Germany, Italy, Macedonia, the Netherlands, Romania, Spain and the United Kingdom (Figure 1) to investigate organisational change processes in police forces.

Security issues consistently rank among the most pressing concerns of citizens in virtually all European countries. Terrorism, organised crime, drugs, and violence have an impact upon citizens' perception of their immediate surroundings and also shape their attitudes towards the state and its representatives.

Open borders, the free flow of people, goods, information, and capital also facilitate the planning and committing of crimes. Politicians and police forces alike are faced with the pressure to address these problems in ways that should alleviate citizens' fears on the one hand, but will not infringe upon civil liberties and human rights, on the other.

For European police forces, these major societal changes have triggered ambitious change programmes aiming at modernising and rationalising the way police work is conducted. The face of the police slowly changes in a fundamental manner.[1] Consequently, it is important to understand the impact of the specific cultural and social contexts of policing and to consider the sometimes dramatic differences in which current challenges, on the one hand, and modern policing concepts and instruments, on the other, are interpreted and implemented in different European countries.

Central to the research in the COMPOSITE project is therefore to study and compare these change initiatives and to determine important factors that trigger change processes, impact the implementation and determine the chance of success.

The results from the COMPOSITE project should not only bring about new insights for scientific discussion, but also reveal best practices and bring about practical improvements in the conception, planning, organisation and implementation of change processes in European police forces.

Therefore, dedicated work packages are responsible for academic coordination, the dissemination of the results to relevant police communities and the general public, as well as for the implementation of a consulting and training program.

Additionally, the project will set up a European Police Monitor that aims to systematically collect information on change processes within European police organisations and to share the results in a user-friendly way.

[1] Jacobs, G., Christe-Zeyse, J., Keegan, A., & Pólos, L. (2008). Reactions to organizational identity threats in times of change: illustrations from the German police. Corporate Reputation Review, 11: 245-261.

Fulfilling the demands of this European approach, researchers of 15 organisations from 10 European countries work in COMPOSITE, as the map on page 7 shows. The project consortium additionally receives advice from its end-user board with experts from police forces and other police related organisations.

Focusing on ICT: Work Package Technology Adaptation

In the frame of the COMPOSITE project, the work package 'Technology Adaptation' focuses on change processes related to digital information and communication systems (ICT) that have a noticeable effect on policing, investigating the adaption of these ICT systems by European police forces.

Policing is a highly complex, information-led activity that requires the integration of multiple data sources, often in short time frames. The sensitive nature of most information and the severe consequences of possible errors further increase the relevance of adequate design and use of ICT.

ICT systems present an opportunity for police forces to increase their capabilities. ICT concepts, architecture and design have matured significantly and are subject to continuous innovation. Relevant ICT may range from systems installed in public environments over PC-based systems in offices, to systems installed in cars and mobile systems used on-site. In addition to systems that are specifically designed for the police, ICT in use by the general public may offer the police new means of dealing with their tasks.

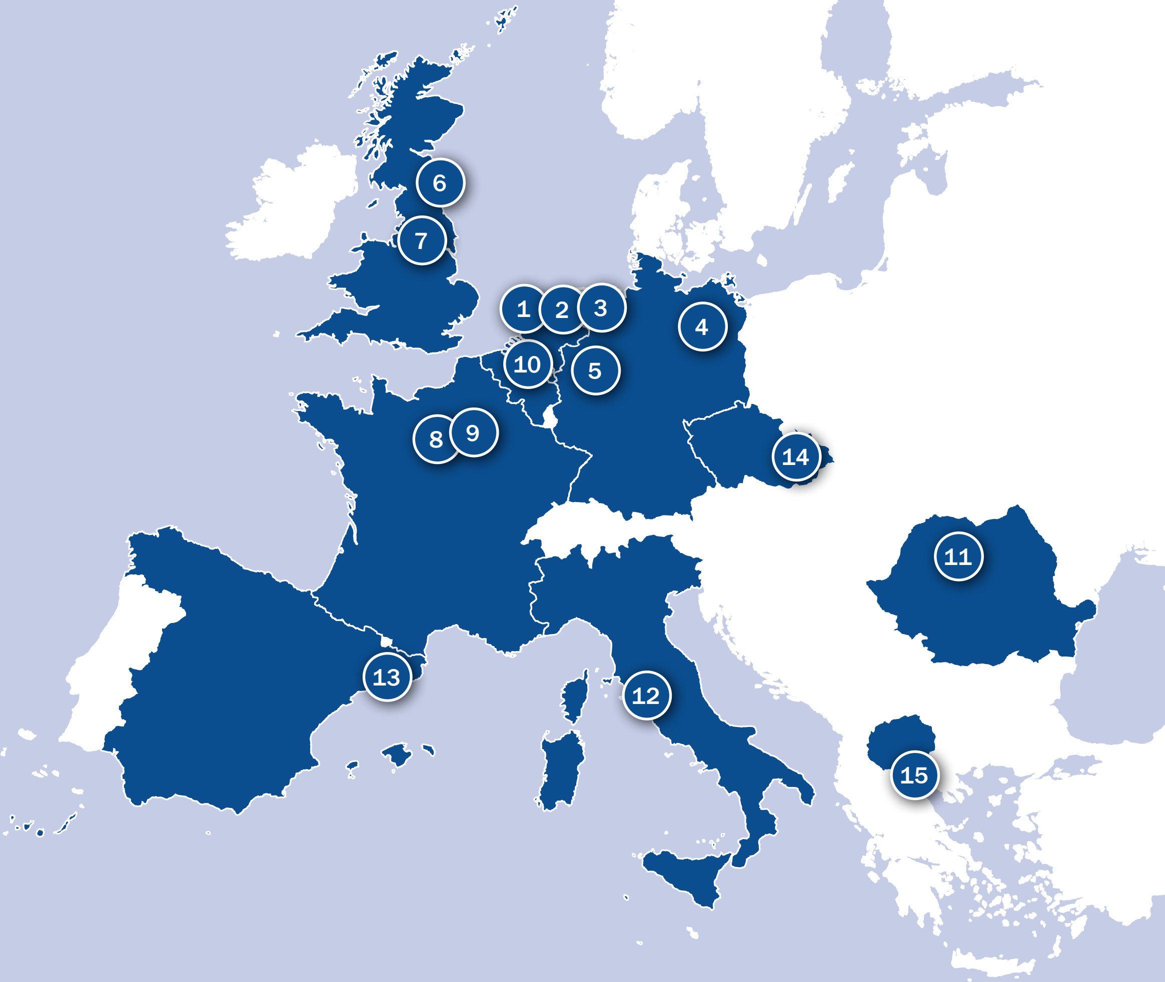
Emerging ICT and their appropriation by society may also constitute a threat that demands new competencies and practices to be developed and integrated in existing police work. Offenders could use systems directly against the police or against the general public.

The extended use of ICT turns out to be much more than just a technical innovation to make police work easier and more efficient. Technological innovations change the organisation and its environment in various ways. ICT in the police is closely regulated by laws, yet may go way beyond what is allowed for the 'normal citizen'. ICT use and design thus become delicate issues.

The research on ICT in COMPOSITE is guided by the understanding that "computer technologies are not neutral—they are laden with human, cultural and social values"[1] and is focused on socio-technical issues that arise from ICT within the context of police work. Thus, we focus on issues that arise in the interaction between technology, on the one hand, and police organisations, individual actors, private companies and the general public, on the other.

[1] Harper, R., Rodden, T., Rogers, Y., and Sellen, A., eds. Being Human: Human-Computer Interaction in the year 2020. 2008, Microsoft Research: Cambridge.

Figure 1: COMPOSITE Project Consortium



Project Consortium

1 Erasmus-University Rotterdam, Netherlands (Coordinator)

2 University Utrecht, Netherlands

3 Police Academy of the Netherlands

4 Fachhochschule der Polizei des Landes Brandenburg, Oranienburg, Germany

5 Fraunhofer-Institut für Angewandte Informationstechnik FIT, Sankt Augustin, Germany

6 University of Durham, United Kingdom

7 Sheffield University, United Kingdom

8 Capgemini Telecom Media Defense, France

9 Centre National de la Recherche Scientifique, Paris, France

10 University Antwerpen, Belgium

11 Babeş-Bolyai University, Cluj, Romania

12 Fondazione per la Ricerca sulla Migrazione e sulla Integrazione delle Tecnologie, FORMIT, Rome, Italy

13 ESADE Business School, Barcelona, Spain

14 Masaryk University, Brno, Czech Republic

15 University St. Kliment Ohridski, Skopje / Bitola, Macedonia

Methods:
Mapping Trends

Our first objective in the work package ‘Technology Adaptation’ is to map the current, most relevant ICT developments, opportunities and related practices in the domain of policing and to look for commonalities and differences across Europe.

To learn about current ICT trends, we approached the field by studying current and planned ICT projects at different police forces and by studying new technological developments coming from the industry of ICT solutions for police contexts.

By comparing all the data collected through interviews, surveys and document analyses, we identify a number of themes that describe current trends and issues for ICT at European police forces.

Studying Police and Industry Perspectives

As ICT emerges in the interaction between market demands and technological innovations, our analysis takes into account current demands and initiatives by police forces as well as current and envisioned systems offered by vendors.

On the police side, we conducted interviews with ICT experts at police forces in all 10 European countries. Local teams performed semi-structured interviews with a total of 52 police officers from a variety of police forces (see list on page 11). To cover a wide range, we aimed at talking to different police forces in each country at local and federal levels with different tasks such as border police or municipal police forces.

Interviewees were officers with responsibilities related to ICT, whose tasks ranged from specifying user requirements for a particular project to deciding on national ICT strategies. Each interview lasted between one and two hours. Based on semi-structured guidelines, we identified current and planned ICT projects. For each project, information about its scope, the motivation and triggering needs, the technology itself and its impact on the practice and problems, were gathered. We asked questions such as: What systems are currently being envisioned, designed or introduced for police work? What police processes do these systems support? What needs do they address? How are systems designed, specified and introduced? What are the problems during design and introduction? Which ICT constitutes a threat to police work? How are those threats handled?

We further collected public or police-internal documents for additional information about the projects identified in the interviews. The interviews were recorded if possible and, in combination with the data from the documents, used to produce a record for each project as part of a cross-national database.

On the vendor side, a cross-national market study on available ICT in the field of first response was performed to identify important trend-setting vendors and designers having a strong impact in this sector. Our approach combined a detailed product enquiry, surveys and semi-structured interviews with selected key vendors. We selected vendors that currently deliver technology to police forces or aim to do so in the future. We looked for companies that attend international police conferences and added them to a list, which we screened for their relevance in providing ICT for the police.

We invited companies to participate in telephone interviews; 20 were willing and able to participate in an interview (see the list on page 11). The companies interviewed included both large, multinational companies and small, local niche players. We focused on European companies, but also included a few vendors that have their current business mainly outside Europe. Each interview lasted around 45 minutes. Based on semi-structured guidelines, we identified current and foreseen ICT applications for police. The vendors were asked to explain their technology and to explain who would work with the technology and how it would affect police work. We also asked for best practices and challenges around the introduction of this technology. To conclude each interview, we collected vendors' views on the relevance of different technologies now and in the coming years. The interviews were recorded and summarised in a standardised format that followed the interview guidelines.

Combining Data and Deriving Themes

To combine the results, we coded the data according to themes in the use of technologies, motivations and problems, looking for overlapping patterns in the data.

With the project records, we performed two steps of analysis. First, local teams looked for patterns and special issues within their respective country and added issues not covered in the project records in a summary report. Second, we performed a comparative analysis of all projects identifying cross-national trends. In this second step, we coded the data with keywords for the types of technologies used, motivations and arising issues, in order to extract patterns from the records. In a database including all projects and codes, we categorised the data accordingly and checked whether or not issues occurred in multiple countries. The categorization led to common themes and special ICT topics currently relevant to European police.

Based on the feedback from the vendors, we refined these categories, so that police and vendor inputs jointly build a set of themes that reflect the current trends.

To validate the results and combine the police and industry perspectives, we presented early results of the analyses to the end-user board (see list on page 11). During the workshops, we discussed the themes and asked the officers to rank the identified topics according to current relevance in their country and police force and according to their estimated relevance for the next 2–4 years. While priorities differed across countries, all themes were considered relevant and no additional themes were added.

Presenting Six Themes

The six themes we present in the following text stem from a bottom-up categorization of the data.

The following themes are not necessarily exclusive, indeed we often found technologies or initiatives that touch multiple themes. Nevertheless, the themes represent visible patterns and trends in our data mirroring common issues of ICT in European police forces from different perspectives.

While some of the themes are technologically driven and directly point to a certain class of devices, others stem from a common motivation or need, or address a common problem.

We have ordered the first four themes by their respective presence in the data and their occurrence in different countries. The fifth theme 'User Acceptance' presents a common issue across different projects, the final theme points to a trend that does not have a large presence in all countries but is expected to gain increasing relevance.

Involved Police Forces

- **Belgium**: Local[1,2] and Federal Police[1,2] (Police Zone Vlas[1], DIRCO Eupen Federal Police[1], General Directorate of Support and Management[1] and the Permanent Committee of the Local Police[1])
- **Czech Republic**: Czech Federal Police[1] and Municipal Police of Adamov[1], Kyjov[1] and Letovice[1]
- **France**: Police Nationale[1], Gendarmerie Nationale[1,2] and Ecole Nationale Supérieure de la Police[2]
- **Germany**: Federal Police[1], State Police of Berlin[2], State Police of Brandenburg[1], State Police of Rheinland-Pfalz[1,2]
- **Italy**: Arma dei Carabinieri[1,2] and Corpo Forestale dello Stato[1]
- **Macedonia**: Macedonian Police[1] (Criminal Intelligence Section in Organised Crime Department[1], Department of Forensic Science[1] and Department of Informatics and Telecommunications[1])
- **Netherlands**: Police forces Rotterdam-Rijnmond[1], Amsterdam-Amstelland[1], Gelderland-Zuid[1,2] and Limburg-Zuid[2], Politieacademie[2], Voorziening tot Samenwerking Politie Nederland (vtsPN)[1,2]
- **Romania**: Border Police[1,2], Municipal Police of Cluj[1]
- **Spain**: Mossos d'Esquadra[1,2], Madrid Municipal Police[2]
- **United Kingdom**: South Yorkshire Police[1], North Yorkshire Police[1,2] and Greater Manchester Police[2]

[1] On-Site Interviews

[2] End-User Board

Interviewed ICT Vendors

- Axis Communications GmbH
- BeInformed Nederland B.V.
- Cognitec systems GmbH
- Esri Nederland B.V.
- Exalead (Dassault systèmes)
- HONAC Nederland B.V.
- HSB identification B.V.
- I2 Group Ltd
- IBM Nederland B.V.
- Memex Technology Ltd
- Mendix Technology B.V.
- ORACLE Corporation UK Ltd
- Palantir Technologies
- Panasonic Europe GmbH
- Research In Motion (UK) Ltd
- Ripples HLS Group
- Rola Security solutions GmbH
- SAP AG
- Thales Nederland B.V.
- Verint Systems Ltd

Theme 1:

Integrating Systems

The first theme was the increased connection of various systems and data sources in order to enhance intelligence and increase efficiency. Standards and new interfaces between systems are being developed so that previously unrelated information can be combined and used to support information-led policing.

Linking systems helps the police to increase overall efficiency and to minimize the need to enter data more than once. It also helps police forces to overcome organisational boundaries between states and countries, as well as separated responsibilities for types of crimes; boundaries that do not exist for offenders. Additionally, combining data and intelligence across organisational boundaries may dramatically enhance investigative capabilities and provide support in real-time.

The combination of intelligence requires different police forces or departments to share sensitive data. Beyond a search for design methods that fit these challenges, future research could provide answers to the challenge of how to balance disparate organisational goals such as catching-up with criminals and how to sustain the trust of the general public.

Building Interfaces

This effort ranges from digitising criminal records that were previously stored in paper form to developing message formats that allow sharing information across European police organisations.

In **Belgium**, a current reform integrates police forces that were previously separated. As a consequence, police forces also work on developing an integrated information system that replaces two existing systems and manages all police-related information regarding people, vehicles, goods and locations to create an integrated system of police records and to generate police statistics.

In another initiative, Belgian police forces work on establishing a web-based toolset that allows them to share information from different sources across the organisation. Tools support briefings and de-briefings, disclose operational information relevant to the daily work of the police, enable searching and accessing relevant documentation, and allow the planning, coordination, monitoring, and management of police patrols. Officers can be assigned tasks using the system and have the ability to report on their work. Officers who are overtaking tasks have access to this information, and can add to it, which allows the creation of complete event histories of certain patrol tasks.

In the **Czech Republic**, systems are set up to make wider use of the central registry of drivers for the municipal police. At the time of writing, this solution is being tested in three big cities—Brno, Pardubice and Prague.

In **Germany**, given the diversified IT structure of the 16 state police forces and two federal police forces, there is the need to integrate and standardise existing systems. A common information model should allow for the integration of existing systems at different police forces. Current projects across states combine intelligence of certain crime types or offender groups.

Integration of IT systems also takes place within individual forces. The federal police currently introduce central server infrastructures to unify the systems so that the individual PC at a police office becomes a terminal and logs on to the central terminal server that holds all the applications. Other integration efforts should allow for the creation of search warrants for people and goods in the national police system, directly in the system of the federal police. In another initiative, integration should allow for periodic security checks against existing databases on people's background to support authorities in providing residence permits but also in cases when people take jobs in safety-critical infrastructures.

The federal police also runs a project to digitize and improve criminal record databases that store information about the behaviour of an offender before and after the act of crime and other patterns in the behaviour and personal characteristics that might help to draw conclusions in cases when an offender commits a second crime. Here, previously analogue information becomes part of the overall system.

In **Italy**, the Carabinieri implement a system to support their nationwide asset management. The system integrates various data sources for decision support and monitoring regarding police equipment such as vehicles, furniture, weapons or communication devices, from their acquisition to the dismantlement, thus providing a real-time overview of all the national resources, trends and needs.

In another project to support investigators in criminal profiling, the Carabinieri combine operators' inputs with other data sources taking into account, for example, visibility, weather, or audible conditions at the crime scene. The system, thereby, creates criminal and forensic profiles of offenders and reconstructs the crime scene. The analysis will help investigators to define the perimeter for their operations.

In **Macedonia**, police forces will establish a national coordinating centre for intelligence analysis. By standardising the collection of criminal data, police and other state institutions could become more efficient in their work. The centralised, unified, and unique database system should contribute to strengthening the fight against organised crime. In future, the intelligence data can be exchanged between different law enforcement agencies. As all data is collected in one place, police forces avoid entering the same data twice. A central system also allows for a unified level of system security and centralised updates.

In the **Netherlands**, efforts are undertaken to automate the integration of information from disparate sources. For instance, a software has been developed that automatically searches in newspapers, internet, transcripts of television or radio broadcasts for clues on known or suspected criminals. At the federal level, a new Central Intelligence Officer (CIO) has just been appointed.

In **Romania**, the border police introduces a national alert information system that allows national authorities through an automatic search procedure in the system, to have access to search warrants of people and goods. The systems helps to fulfil the Schengen Aquis and supports customs control, the issuance of visas and stay permits as well as other control activities carried out by police forces or other authorities.

In **Spain**, an overall information system integrates core data via web services. Vertically, within Spain, the systems integrate the databases of open calls and warnings regarding people and antecedents and histories of people. Horizontally, within all units in Catalonia, the system integrates a variety of 31 databases.

In line with the breadth of the examples above, the vast majority of technology **vendors** suggest that the improvement of infrastructure in collaboration and data exchange, on the one hand, and projects that make use of such infrastructure to share data and intelligence, on the other, are two of the key business drivers for their police customers. Typically, most attention goes to the front-end systems that support the officers, investigators and analysts directly. A number of vendors indicate that police forces tend to underestimate the investment needed in the back-end infrastructure and systems to fully use the potential of information systems for police collaboration. Vendors expect that investment in infrastructure and back-end systems will be an important trend in the coming years, possibly related to the introduction of public and private cloud technology and off-the-shelf software.

Digital Geo References

Police also make use of the emergence of digital geographic references. Real time references of police cars, for instance, allow for improved coordination, while references of crime sites support evaluations. Moreover, digitally geo-referenced information supports statistics that can be accumulated and can be made accessible for decision makers.

In the **Czech Republic**, as also reported in the following theme, computing in cars allows to continuously track the location of the cars and make them available to command centres. Police cars thus become part of an efficient integrated rescue system and increase the level of coordination in emergency response.

In **Germany**, within the state police of Brandenburg, geo references are being introduced in a number of existing technologies. As in the Czech Republic, new interactive police cars are being tracked by GPS, with its position becoming available for command control. In another project on car accidents, a digital map allows police to analyse accidents by looking for patterns in the data. Integrating different maps and geo reference systems, for instance, enables officers to analyse road pavements and assess their influence on the danger of traffic accidents.

In **Italy**, the Corpo Forestale dello Stato deploys a nationwide system for monitoring and anticipating all natural risks, particularly in mountainous regions and regarding weather conditions. An integrated and geo-referenced system allows the collection of information directly from operators in the field and the transmission of information in real time to all Italian authorities involved in securing mountain areas and transport infrastructure. Additionally, new ways of publishing constant updates through web and mobile applications enhance access and the quality of service provided to industry and the general public.

In the **Netherlands** digital geo references from mobile phones are used to monitor crowd movements. This facilitates the coordination of resources, for instance, during large events.

In **Romania**, the border police makes use of the GPS signals from TETRA terminals in order to locate all assets in the field and to allow for real time monitoring and coordination.

In **Spain**, the Mossos d’Esquadra have been using a tool to analyse crime data geo referenced and to produce specific reports about crime mapping. On the one hand, the system should support current investigations by visualizing information related to different types of crimes. On the other, the system should support prevention and facilitate the observing and comparing of crime incidents to decide on countermeasures at operational, investigational and strategic levels. Also, as in other ‘in-car’ systems, the Spanish police work on creating location information from computing in cars to decrease the workload on command centres.

From a **vendor** perspective, geographic information in police ICT systems has become a common standard. Mapping solutions are mature and information exchange standards work well. All relevant products are able to deal with spatial data and either have geographical presentation or can easily be integrated with specialised software. Vendors report that in practice, many police forces are only partly using such technology and have not completely integrated and connected their solution silos as they use older software that does not integrate well with other geo systems as it was developed before the dominance of geo information. Vendors therefore suggest that it is only a matter of time before this technology is ubiquitously used.

Combining Intelligence among European Police Forces

Especially at border regions, police forces also work on combining intelligence from police forces of different nations.

In a collaboration between **Belgium**, **Germany** and the **Netherlands**, police forces share intelligence on certain crimes. The 'Euregion' Meuse-Rhine is an integrated socioeconomic area, which makes it important to compare neighbouring municipalities in different countries to understand if certain trends are local or regional. Currently, the efforts focus on burglary, human-trafficking and drugs. For burglary, data is already exchanged via email attachments that are automatically parsed and stored in a central database.

The police forces in this particular region also work on creating a shared intranet. Initially, a trilingual newspaper was created for police officers. With the vision to go beyond a newspaper, police forces currently investigate the possibility of making information available about police developments in the area, for example information from working groups on specific crime types. A current challenge in realising this cross-national intranet is posed by the need to protect information properly, requiring a shared secure connection and a costly infrastructure.

In addition to the effort by neighbouring countries, several European organisations and systems hold growing relevance for police collaboration and information exchange. Increasingly, cross-country police collaboration and information exchange is supported by pan-European organisations like Europol, Frontex, the European Commission (e.g. DG Home) and also Interpol. Similarly, information systems such as the Schengen Information System (SIS) and the Europol Information System (EIS) play a limited but important role. The different organisations at a European level are also important to help overcome legal boundaries, develop standards and stimulate the re-use of best practices.

Data Exchange between Police and Prosecution Authorities

Besides the linking of data within and across police forces, we also observed the effort to exchange data with prosecution authorities. Standardised data exchanges should increase efficiency by minimizing workload and errors when transferring data. The data exchange has to adhere to strict laws and regulations regarding the creation and handling of evidence.

In **Belgium**, the novel integrated police information system that has been previously described also handles and standardizes the exchange of police-reports with prosecution authorities in a structured and secured way. Both organisations, police and prosecution authorities are required to establish compatible, digital work flows.

In **Germany**, the federal police wants to submit records that are currently stored in the police system digitally to prosecution authorities. Digital records should eliminate the need to manually copy the records in the systems of the prosecution authorities. The paper-based records are, however, still required to fulfil legal requirements. The federal police needs to integrate their systems with 16 state prosecution authorities that currently use different systems.

The state police of Brandenburg works on standardising digital photo and video media captured by police officers and the process to hand over this data to prosecution authorities. Tools need to respect the legal separation between the two organisations.

In **Macedonia**, police forces and other state organisations work on establishing a national coordinating centre for intelligence analysis that should bring about compatible ways of entering and changing criminal records and thereby support crime analysis by the police, law enforcement and other state institutions. A centralised, unified database system should strengthen different institutions in the fight against organised crime.

In **Italy**, the digitalisation of crime notice transmissions from law enforcement officers to prosecution authorities is currently under review. The use of a digital transmission system that fulfils legal procedures, also securing information through certified emails and digital signatures, may contribute to ensure a quicker, more effective and precise handling of crime notices.

In **Spain**, Mossos d'Esquadra work on a closer integration of police forces and prosecution authorities. A system allows the police to receive orders digitally, once the judicial secretary signs it. Once verified, the police digitally delegate the order to the responsible police unit. In another project the exchange also, as reported under the following theme, includes the sharing of digital biometric data.

Technology **vendors** realise that for police the exchange of data with criminal justice or with other relevant public authorities such as intelligence agencies, customs, border police forces or immigration authorities is not just a technical question. While vendors claim that requirements such as data security, fine-grained access control and full traceability can be fulfilled, they think that their police customers' culture, habit and caution in practice make them assume that technology is less mature. Increasingly, vendors consolidate and aim to offer a full suite of intelligence and or investigative case management tools. Most of the vendors claim that they do this in a way that police forces can still opt to work with other products if they prefer. In many cases, vendors can substantiate this claim, but not in all. It becomes increasingly difficult for police forces to distinguish between what different vendors have to offer and involve third party organisations for product assessment.

Theme 2:
Increasing Mobility

The second common trend was a need to increase mobile capabilities. Here, we found a broad overlap in mobile ICT solutions across countries.

Adapting digital radios, computing in cars and mobile and handheld PCs stretches the boundaries of what police officers can do in the field without returning to the police station.

Technology vendors describe these developments in terms of ‘intelligence led policing’: In any location, real time information and intelligence support police officers in their work. Sensor information is fed in real-time into police systems and processes.

For future socio-technical research, the drive for mobility changes the organisation of police work. Given that the police are traditionally a hierarchically structured organisation, the question arises as to how empowerment of officers by mobile devices interacts with the identity and current structure of the police.

Computing in Cars

By introducing computers or mobile devices in police cars, officers gain access to police databases. Additionally, they can offer services on-site to the public and thus reduce operational costs or even the number of police stations. Adding computing, cars can become mobile 'contact and coordination centres' for crisis situations. Increasingly, technology is made available in police cars to support police work in real time.

In the **Czech Republic**, different projects focus on computing in cars. Police cars should become mobile contact and coordination centres that will in the case of emergency provide the public with basic information. To inform the public, the car integrates an LED display and a megaphone and also can establish a radio station.

Another initiative introduces PCs in regular police cars that make its current position available for the command centre. It also establishes the computer as a platform to connect future devices.

Finally, another in-car system in the Czech Republic introduces mobile video recording. Here, a van is equipped with surveillance technologies to support on-site reconnaissance.

In **France**, the Gendarmerie Nationale introduce a bus that becomes a command post and a laboratory. It is designed to be sent to complex crime scenes as part of the national unit of criminal investigation. The command post includes radio technology, a satellite telephone link and an antenna switch with a capacity of 100 telephone lines. The laboratory offers a large set of modern forensic technologies. An auxiliary power unit ensures complete autonomy. In combination, all this equipment allows for the analysis of evidence directly on site crime scenes.

Also in France, new systems improve the ability to identify vehicles. Installed at the beacon light, an infrared film camera automatically scans the surrounding environment for cars and compares license plates with the national and international databases. The system can automatically read up to 4000 vehicles per hour.

In **Germany**, the state police of Brandenburg is currently introducing about 100 custom designed police cars that feature a computing system to perform standard police services on-site. The available technology and the need to cut costs motivated the introduction of the police cars that allow police officers to perform several services on-site for which they previously had to return to the station. To provide a stable data connection to the car across the state, several mobile networks are used in combination.

In **Italy**, the Carabinieri integrate a computing system in vehicles that can be controlled by voice commands or via a touch screen. While patrolling, the operating officers can have full control of vehicle instruments, check multiple databases linked from different organisations, exchange data, pictures and videos in real time, without further operator support. This new tools has the goal to make operations more safe, precise and well timed, and to improve the perceived respect by citizens, as a result of the enhanced effectiveness of inspection procedures.

In the **Netherlands**, cars will be equipped with access to internal police databases, automatic number plate recognition and video surveillance systems and in special situations also connected to systems of the tax authorities. Discussed are functions such as the real-time sharing of videos between cars, dispatch and offices. The intention is to speed up the availability and integration of information, and to increase the chance to identify criminals on the street.

In **Spain**, several police forces aim at integrating PCs in cars. In a recently started project the computer on board is envisioned to give the officers the chance to auto-manage their patrol so that the workload on the control centre will be decreased and the officers can focus on other tasks. To ensure safety, ergonomic issues are important and day and night time contexts are being considered. The keyboard, for instance, is designed with illumination.

Mobile and Handheld PCs

With the adoption of handheld devices and mobile PCs, police officers hope to gain visibility in the public (Figure 2) and lower response times. Novel mobile systems allow police to write fines, offer an on-site credit card payment option, take pictures of crime scenes, use maps to trace patrolling routes, fill out complaints or check police databases remotely.

In **Germany**, in the state of Brandenburg, local police officers are able to provide more services on-site as part of a structure reform that reduces the number of police officers and police stations, reflecting the shrinking population in a state. Police officers are provided a laptop that has access to all standard police applications. All laptops can be monitored remotely and need to be connected to the police network once per week to receive updates.

For the German federal police, mobile computing supports the border-control and identification work on-site. A mobile border control office can be folded into a suitcase. It includes a PC with a fingerprint scanner, a reader for digital documents and a printer. Another handheld system can be used by officers while patrolling on foot in the train or at the airport and comprises a fingerprint scanner and digital document reader.

In **Spain**, the Mossos d'Esquadra introduces PDAs (personal digital assistants) as a tool to process fines to reduce the number of intermediaries between the police force and the traffic office. The tool speeds up the process of charging and comes with a device for inserting credit cards. The PDA can also be used to look up police search warrants and enables police to document traffic accidents by digital photos. Currently, the PDAs have to be distributed throughout the territory and need to be integrated with the office of transportation. At the moment, there is one PDA per patrol that is shared by two police officers. There are plans to assign each officer a separate PDA and thereby to turn the PDA into a personal device.

In the **United Kingdom**, smart phones allow police officers to take photos and access back-office databases to see maps and images of wanted or missing people. Police officers also can upload text and photos as crime data. Additionally, officers receive the latest information or intelligence on their smart phones.

Driven by the introduction of the automatic number plate recognition technology, which caused many more vehicles to be stopped, the police also introduced handheld touch-screen devices by which police officers can scan digital fingerprints of suspect drivers when they are pulled over by the police. The fingerprints are then checked against a national database to learn if the individual can be identified from past criminal records.

In **Romania**, the local police are recording all traffic related contraventions using PDAs connected wirelessly to a database. The system significantly reduces the time that a local police officer needs to identify, report and sanction a traffic contravention.

Photo: Hans van Rhoon

Figure 2: Mobile devices as an intermediate between police and public

From a **vendor** perspective, using mobile devices to make information available at any place and any time is a commodity. After allowing officers to enter data using mobile technology, vendors plan to take the location of the officer into account and present locally relevant information to the officer, as a ‘location based service’. An officer, for instance, could receive a message when she is near the residence of people who have a fine due or are wanted in the context of an investigation. Vendors push the development of ‘apps’ and related technology and integrate new dimensions for police work, such as social media and the geographic presentation of data.

Vendors of mobile devices are in a highly competitive market. As a consequence, this line of technology drives innovation: Consumers become more selective in buying products and check if competitors offer better solutions. Consumer preference is highly volatile.

Digital Radios

To improve communication, police forces adopt digital radios. As analogue radios become obsolete, digital radios with nation wide coverage, encrypted and secure communication and interoperability with emergency systems take their place.

In **Germany**, all state and federal police forces currently adopt digital radios, well before the systems are in use by fire fighters and other security authorities. The € 4.5 billion project comprises the formation of the digital radio infrastructure and the integration of radio devices and command centres in daily practice. Digital radio is considered to be without alternative, as digital radios are cheaper and provide encrypted communication while analogue radios are no longer produced, nor supported. Currently, some German states finalize the introduction of the system while others plan its introduction in the next 2–3 years.

In **Macedonia**, a number of current and future projects introduce digital radio as part of the overall police reform. Currently, the various police forces use a number of different types of radio communication systems. In future, the adoption of the TETRA standard should ensure compatibility among the police forces and with other countries.

In **Romania**, for the border police, one of the requirements from the Schengen Acquis is the development and implementation of a secure and autonomous communication system in order to be able to join the Schengen Area by March 2011. The operational objective of digital radio is to ensure secure communications, at anytime and anywhere for the police force. This system also permits the use of an automatic vehicle location solution to share positioning information between the border police and other national security forces.

In the **United Kingdom**, inquiries into a series of public disasters in the 1980s and 1990s (e.g. Hillsborough Football Stadium; King's Cross Rail Station Disaster) highlighted poor communication between police officers as a crucial factor contributing to loss of life. These analyses contributed to the design of Airwave, the digital radio service that replaces the old analogue radios for police and other emergency services in England, Scotland and Wales. While the system is now in use, current initiatives deal with the migration to adopt the next generation of the network, also exploring how they may be integrated with private networks and beyond national borders.

From the **vendor** perspective, digital radio technology is mature and vendors see no specific open technological issues, with the exception that other applications may depend on or need to be integrated with the new communication infrastructure. For the industry, communication means are regarded a precondition more than an end by itself. Digital radio systems allow for a variety of potential applications that can only become effective if back end systems and infrastructure are in place.

Special Equipment

*In the **Netherlands**, we found projects focused on mobile tools that push the boundary of what is technologically possible and require technological innovations.*

An increasing number of crimes including weapons has motivated a project that aims to replace risky and intrusive body searches. Mobile weapon scanners—functionally comparable to the ones already in use in airports around the world—are being developed for patrol officers on the street.

In another Dutch initiative, a 'DNA shower' is employed to increase the number of convictions in shop burglaries. Shop-specific DNA particles are sprayed on the burglar while leaving the shop, as mobile tags that link the person unequivocally to the location. In a recent pilot, this technique was also found to work very effectively as a deterrent for crime.

In another project, the Dutch police develop alternative means for crowd control. Current research explores, for instance, the use of smells, bright lights or very loud noises to influence crowd behaviour. The idea here, is to exploit basic physical reactions to create 'less-lethal technologies' with a mass effect.

Apart from adopting existing mobile computing solutions, the Dutch police further employ innovation brokers who oversee these projects that require collaboration with technical research.

Theme 3:
Surveillance Technology

Surveillance technologies, especially video recording systems are being developed to support police work.

Currently, there are initiatives to introduce video systems for the observation of public spaces, but police also implement systems with automatic image processing algorithms that are used, among others, for number plate recognition.

Evidence of the effect on subjective and objective safety and security is mixed and case dependent. In general, police forces regard the use of this type of technology as helpful.

While technological issues still need to be resolved, especially with complex image processing algorithms, another issue of these surveillance technologies is its social implication. Depending on the respective country, policy makers and police forces need to balance the need for providing safety with the citizens' rights for privacy.

Observation

To support investigations, police forces adopt video surveillance systems, in both stationary (Figure 3) and mobile settings.

In the **Czech Republic**, special police cars perform video surveillance, as reported in the mobility theme. The in-car system consists of cameras mounted on the vehicle at a telescopic mast and portable cameras that transmit video signals wirelessly. The car system includes a recording system with monitors and video encoders and decoders.

Also in the Czech Republic, smaller units of local police forces currently adopt mini cameras to monitor interventions and to capture evidence of criminal acts. These police forces also promote the installation of static cameras at selected public spaces.

In **Macedonia**, the city of Skopje is working on introducing a centre for the management of road safety. As of today, 70 cameras were installed and have shown to prevent traffic accidents as drivers are increasingly cautious. As the project continues, more cameras are being installed.

In the **Netherlands**, efforts are undertaken to display video surveillance footage from shops in police cars to increase the potential to catch criminals 'red handed'.

Technology **vendors** point out that this technology is increasingly used in practically all countries. Apart from police and law enforcement agencies, they have sold systems to municipalities, public transport and traffic authorities, shopping malls and private security companies.

Automatic Recognition

Besides systems that allow for video surveillance manually, police forces make use of image processing software to automatically filter video feeds and process the resulting data.

In **France**, besides the system for automatic number plate recognition from within police cars that has been described under the mobility theme, other projects also aim at increasing the video recording and analytical abilities of the police.

A video recording kit aims at retrieving and combining video footage from numerous different sources and systems, to support criminal investigations. The project was triggered by the assessments of the Metropolitan police following the 2005 terrorist attacks in London and aims at improving efficiency in making use of video surveillance technology. Integrating mobile video sources, the analysis system indexes all data. Image processing algorithms are being developed to detect certain objects such as faces, vehicle license plates, specific types of cars and abandoned bags or certain situations, such as brawls.

Technology **vendors** report that this type of automated processing has become mature. Camera technology and image processing have improved over the years, further innovation is regarded as iterative and relatively minor. Vendors expect that the development of the back-end infrastructure, the processing, exchange and analysis of the relevant data and the use of such data in other systems or by other agencies, as far as it is regarded meaningful and proper to do so, is coming in the near future. Vendors acknowledge that this type of technology faces divergent levels of interest in different countries.

Border Control

Video processing systems are also used to perform border control, especially in complex contexts such as at sea borders, which are difficult to oversee.

Photo: David Adams

Figure 3: Video surveillance of roads and public places in a control centre

In **France**, the Police Nationale at the Mayotte island, a French territory in the Indian ocean, develop an infrared-based video analysis system to automate border surveillance. Every night, illegal immigrants reach the island in small wooden boats. As wooden boats make radars unusable, the police use traditional human surveillance with binoculars. Especially for surveillance at night, the new system should support officers in border control. Implementing the system, given the complex conditions at sea, including high humidity and changing temperatures, demands algorithms that withstand these conditions. As of now, the system is at an experimental stage and further technological enhancements are required.

In the **Netherlands**, the border police currently develop a system for automated number plate recognition at the borders. Similar systems have been in use in **Italy** for some time now.

In **Romania**, the border police are responsible for the maritime border at the Black Sea and, as a requirement from the Schengen Acquis, have to establish an integrated system of surveillance and control of vessel traffic. The system to be installed should support the surveillance of the sea for a real-time overview of all the positions and movements of the present vessels, processing information from the radar stations and other sensors placed within the supervised sector. Currently, the border police is planning on upgrading the system's data transfer capabilities between radar stations and the command centre in order to keep up with the ever increasing amount of recorded data.

Technology **vendors** note that specific innovations may become relevant in the future, such as automated image processing at airports and the recognition of abnormal behaviour, as a trigger for further investigation.

Lawful Interception

Lawful interception is another specific case of surveillance technology. Typically, it is about intercepting and analysing information based on court orders.

While **vendors** explain that they offer different technologies for lawful interception, the often classified nature of the projects, does not allow them to discuss country specific cases. A few specialised companies have improved the ability to collect data in real-time from satellites, phone calls and, increasingly, the internet.

For this type of technology, European countries have individual laws and processes in place, beyond European guidelines on data collection and retention. Retention periods, for instance, can range up to two years, or be longer for specific data under defined circumstances.

The amount of data to be processed and analysed rapidly increases and has led technology vendors to develop scalable architectures and solutions. To make sense of all the data, infrastructure and intelligence software for an investigation unit or agency needs to be enhanced.

Vendors report that especially specialised units tend to adopt this type of technology shortly after availability. Consequently, this is an area that drives innovation, as technology vendors are rewarded for their investments and are able to sell their products without long time lags. The solutions developed, such as data integration, the work with large volumes of data and real time intelligence can then also be applied to other domains, such as number plate recognition or border security.

Theme 4:
Digital Biometrics

Biometric data has come onto the agenda of European police forces due to the implementation of digital identification documents and from the need to increase the effectiveness and efficiency of identifying suspects, on the one hand, and trusted persons such as authorised colleagues or legitimate border passages, on the other.

In consequence, police forces need to set up new infrastructures to deal with digital biometric data in mobile and stationary setups.

While opinions diverge about the use of this information, there is no doubt that biometric information will become a ubiquitous piece of digital personal information. Yet, fierce discussions on this issue show how sensitive public reactions are to police storing personal information. This raises the question of how these technologies may be designed and introduced to the satisfaction of both police and the general public.

Fingerprint Scanners

Digital fingerprints allow the police to increase the efficiency and effectiveness of fingerprint scans. Both stationary and mobile setups are used to identify suspects.

In **Germany**, at the federal police, as reported in the mobility theme, handheld devices allow police officers to take digital fingerprints while they are patrolling in trains and airports and verify digital identification documents. Dealing with digital documents requires a comprehensive computing infrastructure that handles digital certificates. Before verifying that the holder matches the document, the police have to authorize themselves against the digital documents in order to access the stored biometric data and to validate the documents.

In **Spain**, dedicated computer terminals should enable Mossos d'Esquadra to make use of digital fingerprints and speed up the identification process. Throughout Catalonia, 31 terminals are distributed to forensic police units and to units that have to handle a high amount of cases.

In the **United Kingdom**, as reported in the mobility theme, mobile scanners are used to identify people by digital fingerprint technology. The system is especially used to check drivers who were previously identified by the number plate recognition system.

Technology **vendors** explain that in itself the use of digital fingerprints has become a commodity. It depends on the application whether issues emerge on data quality such as from dirty fingers or from genetic background, as some fingers are easier to match than others. For these aspects, the quality and performance of technology is still improving. Increasingly, fingerprints are also used for data access control, also now available via touch screens on mobile phones, for instance.

Border Control

Digital biometric information, including fingerprint technologies, face and iris photos, are also used to improve border control.

In **Germany**, the federal police, as reported in the mobility theme, introduce a mobile office for border control at special events. The federal police also have completed trials with systems for automatic border control at airports. To handle the increased amount of international travellers, border control stations scan digital passports, take photos of people's faces or irises, match this information with the biometric data in the document and open gates automatically. Fewer officers are needed, as the monitoring process can be conducted remotely. Replaced officers are envisioned to check travellers from outside the Schengen area, who cannot use the system.

Technology **vendors** explain that they are involved in similar projects in other European countries too. Systems are in place for instance in the Netherlands, the United Kingdom and Portugal. In many other countries, solutions are being implemented. With digital fingerprints becoming available in the next generation of passports, a choice between facial recognition and fingerprint technology, which is widely used in the USA, can be made. In Asia, especially face recognition but also other biometric technology is used.

Theme 5:

User Acceptance

The issue of acceptance of technology by police officers is a recurrent problem. Technical issues put police officers in positions where they are not able to use key features. Lacking social acceptance, devices are not used at all or, lacking training, only in their basic functionality. Introducing novel technology in an aging police force becomes a central problem. To decrease the speed of innovation for police officers, sometimes the introduction of technology is delayed.

Some technology vendors stress the importance of training, also highlighting that technology is becoming increasingly user friendly. They struggle, with the demands for customisation, on the one hand, and simplicity in use, on the other.

Confronted with the need to retain its operational effectiveness, the police have to stay up-to-date with technological developments. Especially in aging police forces, the question is how to speed-up the adoption of new technologies while remaining a stable, credible force. Moreover, to the extent that new ICTs are used for operations across borders, the issue arises how cultural values influence acceptance and use of ICT.

Problems in Introducing ICT in Police Forces

The issue of user acceptance is complex. Problems arise from technical issues or in handling the interaction with the devices but also from the need to change organising structures.

The design of ICT for police environments is a technological challenge given the high legal and security requirements and the need to support operations anytime and anywhere. Users face difficulties given technical malfunctions and limitations. Limited network coverage, for example, can greatly reduce the benefit of mobile applications. Frequent problems in hard- or software put the usefulness of new systems into question.

Other issues focus on the interaction between users and computers. Centrally managed systems confront users with interfaces that are different from the interaction learned with standard operating systems. Especially while on patrol, mobile systems add a layer of complexity to be handled by the officer on-site. Limited resources to provide training also restrict the extent to which the novel functions are used. Instead, as with digital radio devices, users only make use of the functions of the previous analogue devices.

Beyond issues that could be resolved by improved technology design or training, novel ICT faces acceptance problems as the new systems also change police practice, organisation and culture.

Exchanging data requires a new culture of cooperation with other agencies. Previously established local responsibilities and ownership of data are blurred and shifted in digital systems. Previously informally negotiated practices are not reflected in ICT systems.

The rapid changes of work practice caused by ICT confront police officers with an ever-increasing amount of ICT to deal with (Figure 4). The technology can become overwhelming, especially for elderly police officers. IT departments sometimes need to decrease the speed of innovation and delay the introduction of new systems to ensure that the users can keep pace.

In some cases, novel devices are simply not being used. But even if systems are adopted well, police officers report on the danger of people stopping to use their own judgement and relying blindly on technology.

To confront all such issues, police forces establish training structures and help desks, they involve users in design processes. Pilot projects are frequently used to introduce technologies in a limited scope.

Vendors also discuss the organisational and cultural issues in introducing technology, such the cultural obstacles in sharing data. They also point to the preconditions of having a streamlined back office and a high level of data quality before the successful introduction of mobile devices. To tackle the issues, vendors call for unified standards and requirements to boost innovation and collaboration.

Despite these problems, vendors report that there is often a loud call for the introduction and innovation of technology. Police officers actively look for mobile technology and ways to enter data directly in the field, so that they can avoid coming back to the police station just to enter their data. They press their chiefs to ensure that they only need to enter data once. They are frustrated when offenders can go unnoticed in one country or force whilst being signalled in ICT systems elsewhere.

As the industry reports, many police forces struggle with the speed of innovation. Often, the largest amount of their ICT investments is bound by the existing IT landscape. Hardly any budget or attention is available for innovation. Consequently, innovation often takes place in a half-hearted manner, leading to new user acceptance problems described in this section.

E-Learning

One way of the police to deal with the challenge of user acceptance is the introduction of e-learning systems.

In **Germany**, the state police of Brandenburg introduce a system that allows police officers to book training courses online and additionally, provides e-learning materials. The system is especially used to train police officers on new ICT such as the novel digital radio devices.

Photo: David Adams

Figure 4: Police officers are confronted with an ever-increasing amount of ICT

In **Romania**, the border police seek to introduce an e-learning platform that is currently undergoing tests. The e-learning platform communicates in daily briefings the results of a risk analysis to the officers responsible for taking action. Also, the e-learning platform provides a means of training officers in the use of new technologies and updated procedures.

Theme 6:

Social Media

The most recent issue identified in our data is the use of social media such as Twitter, Facebook, or Skype for police work. Although only some countries were found to make extensive use of them at the time of data collection, other police forces pointed to the rise of social media as the most important upcoming topic and as an opportunity, as well as a threat.

Social media can become a means to support investigations. Increasingly, police forces use of social media to gain support from civilians for police investigations. Additionally, social media can become a new source of intelligence.

The fast pace and public nature of social media also changes public discourse about policing. Police actions or non-actions come under constant commentary. Social media thus puts additional pressure on the status of police in society and its legitimacy.

Operational practices need to be rethought while a greater transparency influences public perceptions of police work and in consequence the legitimacy of police forces. On a more fundamental level, the presence and role of police in virtual spaces needs to be defined.

Making Active Use of Social Media

The use of social media serves three main purposes: to raise public trust in the police by raising accessibility and transparency, to increase operational efficiency by broadening public participation in criminal investigations and internal cost savings.

In the **Netherlands**, the adoption rate for social media is particularly high, where police forces increasingly integrate services such as Twitter, Facebook, Blogs or SMS into their daily operational practices. Twitter messages and RSS feeds, for instance, inform about recent activities or newest crime investigations. Instant messaging provides subscribed users customised safety updates for the own neighbourhood.

Twitter is also regularly used to broaden the circle of informants. On December 16, 2010, for instance, the Dutch police posted "Police looks for witnesses for carjacking by a fake officer, Aagje Deken Street, Rotterdam-West" (translated from Dutch original). Police forces ask the general public to report crimes on twitter (Figure 2). Hints from the public are also requested via SMS alerts. The 'Burgernet' (Figure 5), organised by the police, informs citizens in real time through mobile phones, when the police reports, for instance, a missing person, a suspect or a stolen vehicle.

In this way, social media replaces more traditional media such as radio and TV. In the future, social media may further increasingly replace personal contacts between officers and the public. A recent Dutch pilot project, for instance, tests the use of Skype for crime reporting.

The Dutch police also experiment with patrolling on social media by showing virtual presence. 'Neighbourhood officers' work as visible police officers on social networks such as Habbo Hotel and Second Life.

In the **United Kingdom**, the use of social media is closely linked to the concept of community policing. A review of the London terrorist attacks revealed the need to build a closer, more trusted relation between police forces and the general public. Therefore, social media is envisioned to become a central tool for communication on a local level. Test runs, in which local police stations use twitter to update citizens about their activities throughout the day, show a great public interest in this type of information.

Social Media as a Publication Channel

Police forces also use social media as an additional channel to publish and promote their work online. Here, the focus is on distributing information to the public.

In **Macedonia**, the Ministry of the Interior uses social media as a public relations' channel to promote police work. On Youtube, videos contain scenes related to organised crime, showing the use of special investigative measures and demonstrating to the citizens the effectiveness of police in dealing with crime.

In **Romania**, the border police uses Facebook and Youtube to disseminate its achievements and actions to the public. Videos and pictures of successful operations are posted online, showing the border police officers in action.

Defining the Role of Police in Social Networks

As the workshop with the COMPOSITE end-user board underlines, the rise of social media is an issue that is making its way onto the strategic ICT agendas.

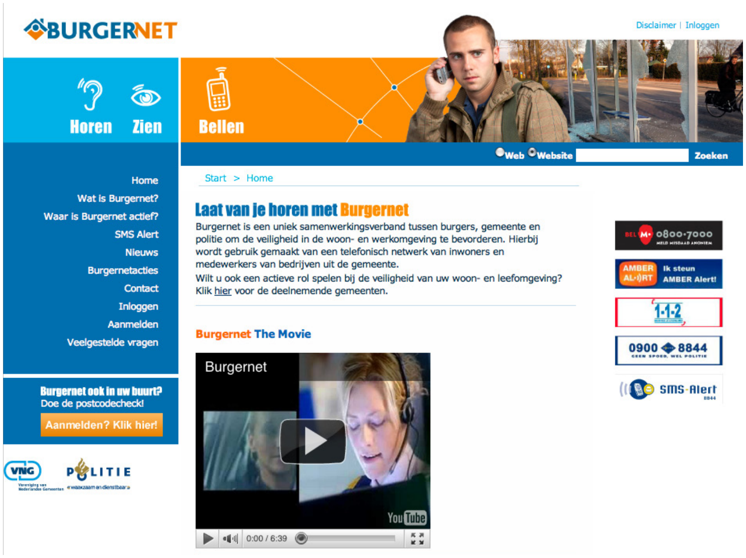
In **Germany**, the emergence of social media is part of the strategic agenda that sets future topics. Currently, guidelines are being developed on how to perform investigations in social networks.

In the **Netherlands**, the police have informally introduced a Police 2.0 website to share ideas, experiences and information on social media for police work.

Vendors indicate that social media and related technology can support core police work in many more ways than currently applied.

As offenders use social media to plan, carry out or announce their plans, vendors expect a growing need in monitoring social media in order to aid investigation or to prevent criminal activities. Additionally, data produced by the general public such as photos may serve as a source for the recognition of both offenders and victims. A new generation of tools supports officers in making use of social media not only as a medium for communication with the public but also as a space for police investigation. Software solutions perform searches on social networks and draw links between previously unrelated information from public internet sites, from inside social networks and from police databases. Such systems also implement mechanisms to protect police operations on the internet from becoming public.

Vendors, however, report resistance towards new technology, stemming from concerns about issues such as security, traceability, access control and the connec-



Laat van je horen met Burgernet

Burgernet is een uniek samenwerkingsverband tussen burgers, gemeente en politie om de veiligheid in de woon- en werkomgeving te bevorderen. Hierbij wordt gebruik gemaakt van een telefonisch netwerk van inwoners en medewerkers van bedrijven uit de gemeente.

Wilt u ook een actieve rol spelen bij de veiligheid van uw woon- en leefomgeving? Klik hier voor de deelnemende gemeenten.

Burgernet The Movie

Figure 5: Burgernet connects Dutch police forces with the general public

tion with legacy systems. Vendors describe a contradiction between the officers’ ICT home experiences and the tools that they work with in their office.

Discussion:

Informing Future Research

The screening of trends resulting from research with police forces in 10 European countries and with 20 vendors reveals a number of topics for future research.

In the scope of the COMPOSITE project, the themes will support the upcoming tasks. First, we will study best practices in the design and introduction of technologies for selected themes and second, we will investigate ICT as an intermediary between the general public and the police.

ICT Trends in European Policing

The six themes present the current direction of ICT at European police forces, as pointers for future research.

Stemming from interviews with police forces and ICT vendors, we have presented six themes. The first two, 'Integrating Systems' and 'Increasing Mobility' are dominant ongoing developments. With a more specific focus, the themes 'Surveillance Technology' and 'Digital Biometrics' point to the rise of certain types of technologies. The theme 'User Acceptance' addresses a common challenge in designing systems while 'Social Media' describes a rising issue to be dealt with by police forces.

With this report and the research conducted, we cannot claim to have covered all ICT projects or issues at European police forces. Indeed, while including police forces from 10 European countries, our data covers only the initiatives and projects of selected police forces and officers in these countries. Counter cybercrime activities, for instance, are not covered by our data and therefore did not become part of our list of themes. Here, future research can provide more insights to understand if the topic is not relevant, underestimated or if it is a topic that is covered by units and forces we did not include in our interviews.

Since we only investigated current ICT activities at European police forces and did not map all the existing solutions, we also cannot interpret the absence of activities in specific countries as signals of limited relevance or already completed adaptation. Answering such questions requires a more specific focus on a certain theme and needs to become a part of future research.

While these limitations do not allow us to make absolute statements about the relevance of the identified trends, we understand this report as a screening of current ICT developments in European police forces that should serve as a starting point for future research.

As described in the summaries of the themes, each trend poses issues that go beyond technology and touch the organisational work flows, culture, identity of police forces. Roles and tasks need to be reconsidered, new skills need to be built. ICT impacts the nature of police work.

Technology vendors provided a view of what may be technologically possible. Technology has developed and matured further than what police forces currently use. Explaining this gap, we identify a number of potential causes such as budgetary limitations, the need for a more mature ICT infrastructure, legacy systems and technology that requires a lot of attention and investment, standards and guidelines that hinder the application of innovative solutions, a culture of not sharing data, a mismatch between the knowledge and experience of police officers and what is required to most effectively work with some of the technology solutions.

In addition to issues of technology and culture, legal issues will require special attention. While police forces envision data to be intrinsically connected and available in real time and anywhere in a way that is directly relevant to the police job at hand, this vision can only be realised in accordance with legal regulations. A proper political process, a public debate and the implementation of legal changes will require special efforts.

The Need for Monitoring ICT Initiatives

As our studies show, there is value in making visible the different technological programmes on a European level.

Mapping of ICT projects, as done in this report, is of high relevance. While some projects involve multiple police forces from different countries, most initiatives remain local and we found that police officers are not necessarily aware of similar projects in other countries. Indeed, they showed great interest in information about projects taking place in other countries.

One suggested future result of the COMPOSITE project, the European Police Monitor, a database on change processes in European police forces, therefore appears to represent an important tool in sharing knowledge and practices across Europe.

Future Research in COMPOSITE

Following this trend analysis, the work package 'Technology Adaptation' will first look for best practices in selected themes and second, perform research on technology as a boundary object between the police and the general public.

As the next step, the research on ICT for the police in the context of the COMPOSITE project will work on formulating technological best practices. Workshops will bring together experts from the different police organisations to discuss and describe best practices for selected topics.

Following that step, the task in the work package is to build an understanding of the ongoing societal appropriation processes motivated by existing and emerging ICT in police work. The work package will research the interaction between ICT in police forces and the general public. In a multi-sited, cross-national ethnography, observational on-site field studies will provide an account of the role, relevance and impact of technology as a mediator between police forces and the general public.

Both tasks will be informed by this trend analysis and contribute to a deeper understanding of the individual themes and issues that have been described in this report.

Acknowledgments

We would like to thank all our interview partners, from police forces and ICT industry, for their invaluable support in this research. This work is partially funded by the European Commission in the context of the COMPOSITE project.

Feedback and Contact

If you have comments or feedback to this report, please contact us.

Sebastian Denef
Fraunhofer Institute for Applied
Information Technology FIT
Address: Schloss Birlinghoven,
53754 Sankt Augustin, Germany
sebastian.denef@fit.fraunhofer.de
Phone: +49 2241 14 2702
Fax: +49 2241 144 2702

Nico Kaptein
Capgemini
nico.kaptein@capgemini.com
Phone: +31 30 689 1222

You can find more information on the COMPOSITE project, general contact information and local project partners at:
www.composite-project.eu

www.composite-project.eu