Summary

This research is about the combined use of forensic materials for combating high volume crime (e.g. burglary, auto crime). The cause of the research is the intention of the government to develop a 'national forensic database'. In such a system 'different forensic materials, such as fingerprints, tool marks, marks left on bullets or cartridges, shoe marks and marks that are left in a digital environment, are filed on a standardized way and then compared so that unsolved criminal offences can be grouped together and solved' according to the government. This must lead to increased clearance rates. The idea behind a 'national forensic database' is that unsolved crimes are grouped together into clusters according to the next principle:

1. unsolved crimes where the police found the same forensic material A, are clustered;
2. on one of the crime scenes the police did not only found forensic material A but also B;
3. other unsolved crimes where the police also found material B are linked to the cluster, etc.

This way the police are able to discover patterns in crime and patterns in criminal networks, which could help in tracking down the offenders of unsolved crimes. Also the police are able to form groups of related crimes without the intention of tracking down a certain offender. If for one of these crimes a person is arrested, the police know that this person should also be questioned about the other offences (the police are then prepared to *case enrichment*).

The main research question was what the possibilities are to realize a 'national forensic database' and what restrictions should be taken into account. We focussed on police practice concerning DNA material, finger prints, modus operandi, tool marks, marks left on the underside of bullets and the electronic recognition of faces ('face prints' left in a digital environment).

The name 'national forensic database' is misleading. The essence is not that 'all forensic materials' will be filed into a new integrated computer system. The idea is to develop a system for analysing information about forensic materials, with the intention to group cases. Conducting such an analysis is a not too difficult matter (automatically linking together similar forensic traces that the police have found at different crime scenes). Problems lie elsewhere. On the one hand the problem is how to select the information for the analysis system (input). The question is what information is useful, which means: good enough for making reliable analyses. On the other hand it is difficult to evaluate the clusters that one has determined and to prevent the police from developing a tunnel view. Also it is difficult to set the right priorities in detective work.

For law enforcement agencies it seems wise to continue developing a system for analysing information about forensic materials on a national level. Our research showed that one then needs to take into consideration the following.

1. The police should rely on different kinds of forensic materials, since all of these have their strengths and weaknesses. In doing so, the police may prevent herself from depending too heavily on a certain technology and from being too vulnerable to criminal counter-strategies.
2. Computerized comparison of forensic material demands that the characteristics of the material involved can be translated into a unique digital code (like with DNA and finger prints). Consequently in certain situations one may use a less detailed description of the forensic evidence, for example the type of tool that has been used (a screwdriver – code 123) instead of the mark that has been left by it (a tool mark can not be represented by a unique digital code).
3. A strict system of quality control is required. The police provides the system with information. One needs to make high demands on the quality of this information. Furthermore the quality of the information stored in the analysing system as well as the organisation that surrounds the system need to be thoroughly checked annually by an external organization.
4. To work with forensic evidence is to work with uncertainties and probabilities. Working with computers may raise the appearance of certainty and thus increase the risk of developing a tunnel view. The system therefore must help the end user to keep in mind that forensic information always is liable to error. The system should also help the end user to develop alternative ideas (working hypotheses) about the facts of the case.
5. To develop a forensic analyses system containing cases from all police forces means that different police forces might start to work on the same unsolved cases. A sound coordination system is needed.
6. A national analysis system should also help the police to reduce her workload. Consequently the police should develop knowledge (or let others develop knowledge) about what kind of patterns in forensic materials are related to what kind of crimes or what kind of criminals. This requires a new type of forensic-criminological research.
7. The police should not have high hopes for this new development. History shows that new police technologies are disappointing because expectations were too high. The above mentioned technology should therefore not be declared a breakthrough in crime fighting. That we do witness a breakthrough, is something the future might tell.