Summary

This study on *converging technologies* is a forward looking study intended for practitioners and policy makers in the field of security, legislation, crime prevention, and law enforcement. We use three selected cases where converging technologies may fit in: monitoring and immediate action, forensic research and profiling and identification. This study takes the technological developments as its starting point. Four converging technologies are distinguished: nanotechnology, biotechnology, information technology and cognitive technologies. We estimated what the developments in the field of converging technologies would be, translated them to the application domain mentioned, and then set out to assess the trends in the social and normative impact of those developments.
In our approach, we started with the technology developments (independent of applications), wrote scenarios based on these developments (independent of an impact analysis), and then analysed the normative and social impacts of these scenarios in the form of eight trends that we consider to be important. These results may be used to start debates, either internally (the role of relevant Ministries, the impact of their policy on scenarios) or externally (social debate). In this way the technology forecasts, scenarios and impact analysis may be used to shape new policies, which in turn will possibly influence the technology developments.
Consequently, this report consists of three parts. The first part describes the state-of-the-art and future expectations on nano-, bio-, ICT and cognitive science and technology, as well as their convergence. The second part describes the (future) applicability of converging technologies to our application domain, in particular the three cases. This part ends with scenarios that are used as a means to 'visualise' the developments and an input for the impact analysis. In the third part the scenarios are analysed on their ethical, legal and social implications. This part describes the major social and normative trends we observe.

Nanotechnology

Nanotechnology is a generic term that encompasses technologies that operate with entities, materials and systems of which at least one characteristic size dimension is between 1 and 100 nm. A key aspect is the occurrence of specific properties because of the nanoscale (e.g., large surface areas, quantum effects). Commonly, three main areas are distinguished:

- Nano-enabled materials and nano-structured surfaces. Nano materials technology is currently the most mature of the nano-technologies and has the highest penetration in commercial products such as cosmetics, coatings, textiles, adhesives, catalysts, and reinforced materials.
- Micro/nano-electronics. Nano-electronics shows a mixture of ongoing improvements of established performance (as with hard disks and MRAM memories), nano-enabled developments (as in large-area

electronics) which are ready for use but do not always have the right performance yet, and speculations based on new discoveries and proof-of-principle only.
– Bionanotechnology and nanomedicine. DNA micro arrays are available for fast throughput analysis, and lab-on-a-chip technology is in place, even if not taken up widely. Sensors and actuators (MEMS/NEMS) are an important growth area, in particular biosensors 'on the spot' which will replace taking of samples for measurement in laboratories (so-called 'point of care' analysis). Targeted drug delivery is an important promise.

An interesting attempt at an overall view for future developments is the four-generation scheme of Mihail Roco, senior adviser to the US National Nanotechnology Initiative. The first generation has been the passive nanostructures. The second generation consists of reactive ('smart') materials and structures, that are capable of changing their properties in response to different external changes (like temperature, electromagnetic fields, humidity, etc.), and combine sensing and acting. The next step is to integrate some computing, so that choices can be made and acted upon. Nanotechnology will enable further functions and performances. The fourth generation will be molecular nanosystems, e.g., molecular devices 'by design'.

Biotechnology

Biological technology is technology based on biology, the study of life. Before the 1970s, the term biotechnology has mainly been used in the food processing and agriculture industries. Since then, the term biotechnology is also used for engineering techniques related to the medicine field, like the engineering of recombinant DNA or tissue culture. Nowadays, the term biotechnology is used in a much broader sense to describe the whole range of methods to manipulate organic matter to meet human needs. Biotechnology has developed far beyond seed improvement and genetically modified oats, rice, etcetera. Many of today's biotechnology applications have a medical or therapeutic focus. This has also drawn the interest of criminologists to look for medication and therapies from a systems biological, biochemical, neurobiological, or biopsychiatrical perspective.
In the coming years, genetic analysis is likely to improve both with regard to accuracy, speed, and ease of operation. An example could be the implementation of gene passports. Also, synthetic biology and synthetic medicine may lead to developing agents with various functional abilities, such as preventing pathogens from entering the body, exploit pathogens' vulnerabilities, or enhance the immune response to new pathogens.

Biomedical engineering will continue to advance in the direction of producing more complex artificially grown tissues, such as cartilage. Gene therapy, and generally the modification of human genes will continue to be a major research area. However, the extraction of personal characteristics from genetic material for identifying or other purposes is far away, because DNA is a complex matter. It raises the question whether simpler biological clues to understand behaviour, health or body functioning are available.

Information technology

Information technology encompasses all the technologies related to the logical and physical definition, design and implementation of systems and applications for data acquisition, storage, processing, transmission, and management. Since almost all aspects of the current human activities heavily rely on ICT solutions, it is impossible to give a comprehensive view of all state-of-the-art applications. We considered the most relevant for the current study.

On the application layer, there is a current trend to create ambient intelligence through smart, context-aware surroundings, smart devices (e.g., automatic selection of washing programs based on the type and quantity of laundry, or the pre-tension of seat belts when an impact seems imminent). In camera surveillance systems there is a data explosion of an ever increasing number of sensor network calls for automatic recognition (identification or verification) of persons based on biometric features, and event detection as a form of pre-selection for human supervisors. Autonomy is key in future applications. A wide adoption of household robotics is expected. Applications are expected that allow observers of large datasets some visualisation. The sensor networks will be spread around in the living body, *in vitro* in living cells, in the air to probe the atmosphere, or on earth to sniff, listen, film, etcetera. And the quality of the data collected, will allow better understanding of many complex systems. For these systems to be really understood, these experience interfaces need to be available.

One of the bottlenecks in ICT may become the complexity of handling large volumes of data. That is, the data volumes may grow faster than the process capacity. For example, a single human genome is already six Gigabits of data. This volume of data is still small compared with the possibilities of millions of RFID tags being scanned in logistic streams, the number of sensors growing enormously, and persons being continuously on-line with human-computer interfaces becoming more friendly due to sensors, speech technology, etcetera. Quantum computing may be a solution for this problem, because quantum computing power is supposed to scale in an exponential way with the number of processors (whereas

current computers scale in a linear way). However, quantum computers are judged as a long-term and uncertain development.

Cognitive technology

For the purposes of this document, the most relevant aspects of cognitive sciences are the study of structures, functions, and processes that define, implement, or describe the perception and interpretation of stimuli, decision making, and experiencing of mental states.
Computational theories of cognition propose mathematical or algorithmic description of neural processes. The development of these theories is based upon observed *in-vivo* analysis of reactions to stimuli and *ex-vivo* analysis of neural structures. Brains, however, are complex to model. Empirical theories of cognition start from observed behaviours (or subjects' self-reports) and psychological assessments, and propose models that logically explain the observed behaviours and psychological properties. The theories concerning higher-level cognitive processes, such as mind states, experience, and consciousness, are mostly empirical, and some quite speculative. Within the artificial intelligence (AI) field many analytical, logical, statistical, and algorithmic models have been proposed for learning, reasoning, categorization and clustering, pattern discovery and recognition, data correlation, etc. But there are few agreements as to how they are sound models for biological intelligence.
Futurists believe in unravelling the secrets of human cognition and consciousness before 2020, but cognitive scientists are more sceptical. It is unlikely that the high-level cognitive functions (such as intentions formation, creative problem solving, and consciousness) will be fully explained. The general opinion is that 'brain reading' is over exaggerated. Techniques like fMRI and EEG are very valuable for pathological purposes, and brain stimulation is used for medical purposes as well, but there is too much noise in brain signals to allow the interpretation of, e.g., thoughts. Nonetheless, in the cognitive area there seems to be a lot of 'low-hanging fruit' to be applied for security purposes. Probably much more can be done with facial expressions. We know a great deal about emotions. Inferring emotions from facial expressions is likely to become accurate enough for using in a wide range of applications.

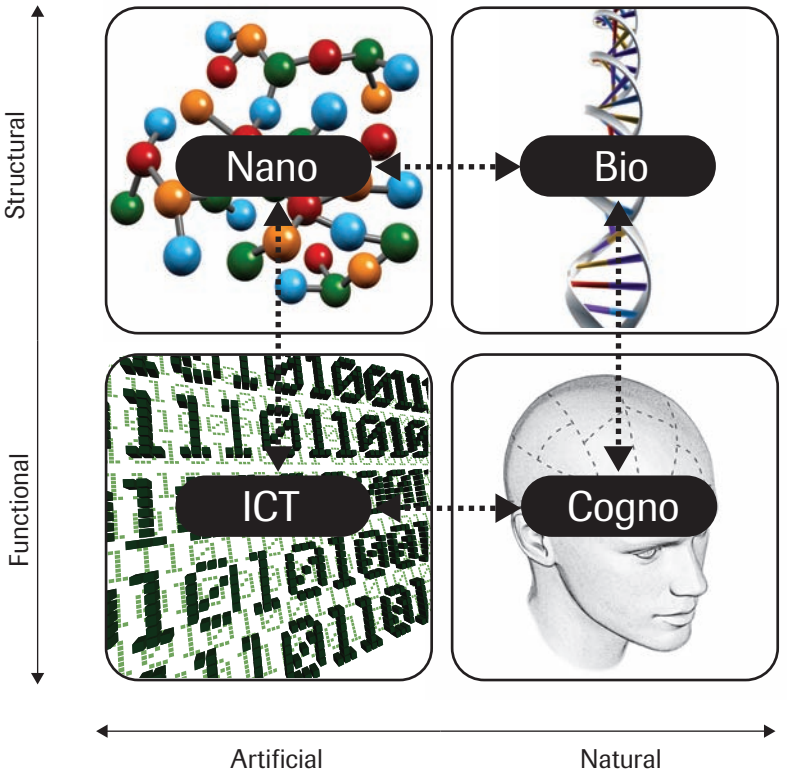
NBIC Convergence

All four NBIC fields are multidisciplinary in their own. Therefore, convergence is a process and not a property of this collection of technologies. The process leads to new paradigms in application areas. These shifts can

not be forecasted, but we argue that convergence occurs naturally along two dimensions: structures and functionalities, as follows (see Figure S1):

1 Nanotechnology and biotechnology deal with *structures* that have a different underlying nature, but evolve toward comparable architectural complexity.
2 Cognitive sciences and ICT deal with *functionalities* implemented on structures of a different nature, but evolve toward comparable algorithmic complexity.

Figure S1 A model for natural convergence along two dimensions



The main effect of these convergence processes is the achievement of reciprocal compatibility between the converging technologies.

Application of convergent technologies

Since convergence is a process, it becomes visible through applications. To focus the discussion on the meaning of convergent technologies for our application domain (i.e., the area of security and crime control), we restrict ourselves to three cases:

- Case 1: Monitoring and following objects or persons and remote intervention in case of undesired movements and relocations (in short: *Monitoring and immediate action*);
- Case 2: Improving and developing forensic trace analysis (in short: *Forensic research*);
- Case 3: Profiling, identifying and observing persons with an assumed security risk (in short: *Profiling and identification*).

For each case, we look into the expectations for the short (5 years), mid (10 years) and long term (15 years).
Monitoring and immediate action deals with, e.g., positioning and/or communication technologies like GPS, or RFID tags can be used to track and trace objects or persons. A special case is the tagging of persons as currently happens in experiments with prisoners. Besides monitoring people to prevent them from doing wrong, one may also monitor persons to protect them. The general belief is that people are willing to give up privacy in favour of individual or collective security. However, that does not necessarily mean that privacy becomes less important. Currently, mainly ICT technology seems to be used for monitoring and (remote) immediate action. Convergent technologies will allow the online registration of many variables (e.g., body sensors), advanced risk assessment by the combination of bio-, cognitive and ICT indicators, and restraining persons in well-defined cases. Besides, we have to deal with the issue of tampering. In our forecast, we suggest that the following applications in monitoring and immediate action will be technically feasible by 2022:

- Individually worn sensors, in particular tagging prisoners or persons being detained during her majesty's pleasure (the Dutch 'TBS') with an implanted RFID chip (short term).
- Wearable personal monitoring devices with data recording and online communications capability (short term).
- Tracking and tracing individuals in public civic areas.
- Implants (or prostheses) that mimic or even augment human biological functions, but no selective memory erasure and no behaviour manipulation by brain implants.
- Blocking cars automatically based on sensor information (short term).
- Objects (e.g., clothes) that respond to external stimuli (like location, heart beat).
- Wireless Internet available worldwide (short term).

In forensic research, new technologies make it possible to establish new or radically enhanced ways of producing evidence. An example is using DNA material for identification. New technologies may even be required because of the necessity to analyse minute traces (level of molecules). NBIC technology may completely change the way of working. For example, due to lab-on-a-chip technology the analysis results may steer the

search for traces. The miniaturising and commodification also means that techniques that used to be available to large institutions only, become available to individuals, who can do the same analyses. 'Social software' may be used to involve larger communities for collecting information. Relevant technologies for the coming years include portable analysis instruments, large-scale databases, single molecule detection, biomarkers, DNA profiling and 3D imaging of crime scenes. In our forecast, we suggest the following applications in forensic research will be technically feasible by 2022:

- Rapid forensic evaluations from very small fragments of materials (short term).
- The use of new kinds of (miniaturized) highly selective, accurate and sensitive biological sensors.
- Computational devices – like 'lab-on-a-chip' – becoming commercially available.
- Objects (e.g., clothes) that respond to external stimuli like the availability of specific (biological) substances.
- Powerful wearable computers / laboratories (short term).
- 3D visualisation of crime scenes.
- Resistant textiles, showing hardly any trace (long term).

To search for persons with an assumed risk for society, profiling can be used. A risk analysis may be based on available information from any 'intelligence' applications. Then, profiling also becomes the prediction of (or anticipation on) expected behaviour based on all available information. Identification also deals with looking for a specific person – whose identity is known – in the crowd. In general, people leave more and more traces in the virtual world by browsing on Internet, using their mobile phone, carrying RFID tags, or being observed by cameras. The amount of data registered about persons and objects is growing enormously. For this case, information processing applications are expected and face recognition is important. 'Brain reading' applications are far off, and it is not expected for the coming 15 years to derive behaviour from a gene structure. Nonetheless, combining information from all kinds of bodysensors and cognitive analyses may make it possible to predict risk factors. In our forecast, we suggest the following applications in profiling and identification will be technically feasible by 2022:

- Widespread use of (real-time) surveillance and monitoring of humans and environments / presence of sensors in public areas.
- Increasingly smaller-sized unobtrusive camera surveillance and sensor networks.
- Widespread use of RFID tags (e.g., in the retail sector) that can be used to track persons (short term).
- Massive databases, e.g., holding genomic information (short term).

– Coupling of databases/sensor information, improved search capabilities and artificial intelligence to logically process collected information.
– Biometrics – probably combined with other available (context) information – widely applied for security functions (but no brain reading).
– Hands-free human-computer interaction enabled by input devices with fast and unobtrusive data capturing.
– Genetic screening for, e.g., clinical pictures, but not for predicting behaviour.
– Secure personal data transfer, like anonymous transactions or identifier removal.

Scenarios

We have sketched four scenarios to visualise the future application of converging technologies within our application domain. The scenarios have been based on the expected (realistic) technology developments for the coming 15 years. The scenarios have been written from a technology point of view and are a means to allow an impact analysis of converging technologies. We used two uncertainties to sketch four typical and related scenarios:

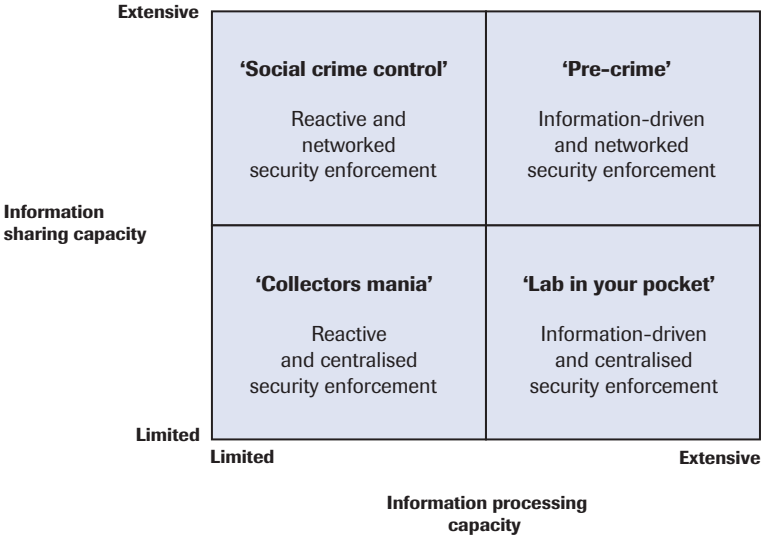
1 The degree of information sharing that can be realised between stakeholders involved in the security enforcement chain.
2 The degree of information processing: the capacity to store and analyse the growing amount of collected data.

In all scenarios the technology becomes 'invisible', which results in a move towards what we have labelled 'ambient intelligent public security enforcement'. Depending on how the two uncertainties develop in the future (for the scenarios we choose the extremes limited versus extensive), four different scenarios are possible (see Figure S2). We have characterised these scenarios with the terms 'Pre-crime', 'Social crime control', 'Lab in your pocket' and 'Collectors mania'. In 'Collectors mania' we observe reactive authorities, collecting information and evidence to be used on purpose. In 'Pre-crime' we observe a shift from a reactive towards a proactive government, using technology to anticipate on and prevent crime. The technology is enabling in the sense of supporting the developments in society towards prevention. The two other scenarios focus on specific applications and show how converging technologies may be a driving force for new 'paradigms' in the security application field. They sketch a more participatory role of citizens in forensic research ('Lab in your pocket') or surveillance and law enforcement ('Social crime control).

The 'pre-crime' scenario is closely related to the profiling and identification case. It shows a shift towards prevention, from a reactive towards an

information-driven proactive environment. Sensors are available everywhere and the information can be processed to take the right decisions. The government policy is anticipation on and prevention of criminality. Characteristics of the future situation are:
– Persons with an assumed security risk are monitored;
– The widespread use of RFID tags in or on the body for monitoring and identification purposes;

Figure S2 Using two key uncertainties to build four 'related' scenarios



– The use of sensors (video surveillance, body sensors, brain scans, etc.) for, e.g., aggression detection;
– The coupling of public and private information sources for an all-embracing analysis of a person's behaviour and relationships;
– Actuators that restrict persons in their movements.

The 'social crime control' scenario is closely related to the monitoring and immediate action case. The scenario shows a paradigm shift with respect to (public-private) collaboration. Due to collaboration with private partners or citizens, small-scale, individual monitoring is possible in this scenario. It enables therapy close to someone's home environment ('prison without walls'). Characteristics of the future situation are:
– Individual tracking and tracing of persons with a smooth transition (seamless handover) from outdoor (GPS) to indoor (camera surveillance) or from public to private systems;
– The entire population is assessed for tendencies toward criminal behaviour;
– Blurring borders between virtual and physical behaviour;

– Citizens participate in tracing criminals and law enforcement; mutual observation and social control of citizens.

The 'lab in your pocket' scenario is closely related to the forensic research case. The scenario shows a paradigm shift with respect to the availability of specialised equipment for the common man. The scenario has been based on (trace) analysis tools becoming small, quick, accurate, low-priced and handy. Herewith their results steer and change the (forensic) research process. Also, these tools become a commodity and therefore are used by private researchers (or criminals) as well. Characteristics of the future situation are:
– Nano sprayers to detect the smallest traces;
– 3D reconstruction of crime scenes;
– Lab-on-a-chip technology available to everyone;
– Global sensor information becomes available as a service to citizens (tracking locations, camera data, etc.);
– Real-time analysis of data, e.g., for database matches (DNA, face recognition), trace analysis, etc.

In the 'collector's mania' scenario, none of the three application cases has a preference. The scenario extrapolates the current, somewhat reactive (rather than anticipatory) processes towards the future. This does not mean, however, that the scenario is less advanced, because the NBIC technologies still advance. Characteristics of the future situation are:
– Much information is collected, arranged, presented etc. In particular, the data are used for searching afterwards;
– Tasks shift from public partners to private partners (services) and eventually to citizens, but more on a service rather than a collaboration base;
– Enhanced camera surveillance, e.g., it is possible to distinguish voluntary or forced behaviour.

Impact analysis

Obviously, the technological developments, applications, and scenarios are closely related to social and normative issues. Eight possible social and normative, i.e., moral and legal, trends may condition the impact of the use of converging technologies for security tasks and law enforcement. The social trends are concerned with implications of increasing polycentric and multi-actor crime surveillance and challenges to governability. The normative ones focus on new privacy concerns, issues of self-control versus control by others, the moral foundations of the law and the legitimacy of new forms of regulation. It should be noted that these trends will often overlap and intertwine in real practice. In order to highlight possible salient developments, it is, however, useful to distinguish them *in abstracto*.
The approach with regard to the impact analysis and assessment in this report is one of several possible alternatives. We have projected a certain

future technological performance, in order to consider possible impacts. In discussing such impacts and assessing them, we had to *quasi* reify that technological future; assume that it would be there, somehow, without further discussion. The implication is that a discussion of social, moral and legal impacts, here of converging technologies, will have an exemplary character rather than offering a picture of the future world. Still, this can draw attention to issues and challenges that deserve to be paid attention to in the here and now.

Eight trends have been distinguished:

1 Shifts in data collection and data processing: More and more data are being created; they are disseminated more widely, to a larger number of parties; access to data is made easier for the government, and control over these data is becoming increasingly difficult for data subjects. The consequence of this trend is that, even with the same investigative powers, governmental authorities are in a position to collect and use significantly more data about citizens than before, and this increase is not only quantitative, but also qualitative. This in turn enables the government, in principle, to know better than ever before what citizens, including criminals and terrorists but also 'the man in the street', are doing.
2 Shifts in methods of surveillance: Increasing possibilities of surveillance will induce more normalising effects on conduct, self-perception, personality, and world-view, than ever before.
3 Shifts in power relations: Regulation will be delegated more from persons to technology and from public, governmental parties to private organizations and citizens.
4 Changes in the governability of technologies themselves: Growing uncertainty and complexity will increasingly complicate the governance of the emerging technologies and their applications.
5 Shifts in privacy concerns: As new possibilities of observation and surveillance show both centralising and decentralising tendencies (that do not mutually neutralise each other) and instruments for observation and surveillance become increasingly unobtrusive, both the perception and the nature of privacy invasions will change.
6 Shifts in the focus of criminal law, away from reaction, retribution and rehabilitation, towards prevention and risk control.
7 Shifts in the conceptions of freedom and personal responsibility: These may affect the ways in which persons perceive their own and others' identities; they need not automatically undermine conceptions of morality and law that take personal responsibility and free will as their starting points.
8 Growing fusion of norms and enforcement: The inclusion of norms in technology that influences behaviour will involve increasing challenges to moral outlooks in which the free choice to act morally or

legally right is primordial, and new challenges regarding the legitimacy of arrangements for regulation and enforcement.

As the world changes and technology develops, normative outlooks can be expected to change as well. Some of these changes have been indicated in the description of the trends. It is nonetheless important to note that the trends could also be seen as explicating a necessary additional element in the scenarios. Impacts occur in context, and are co-produced through technological developments and social and normative developments. Impact assessment has to take this into account, up to the further possibility of normative outlooks changing in the course of this co-evolution.
If the scenarios (and their background considerations) are combined with the present discussion of trends, key issues (and trends, and challenges) seem to be poly-centric governance, particularly in relation to infrastructures, the role of private actors in the new governance structures and self-control versus control by others. An important general challenge for the future will not be about government actors, but about the role of private actors and their accountability.
There is a general role of government vis-à-vis new and emerging technologies: to stimulate exploration and exploitation of new and emerging science and technology for what they can do and mean; but also to set boundaries to such developments because of possible negative impacts and the opening up of further, possibly undesirable applications. Here, co-evolution returns, now of technology, society and normative outlooks, including the expectations that norms and values might shift.
One should be very careful not to engage in an evaluation of the scenarios on the basis of the trends that were sketched. Nonetheless, in a kind of *addendum* to the report, the scenarios and the trends have been confronted with the principles and starting points that form the normative framework of the current Dutch criminal law system.
Eliciting the principles that lie at the heart of the Dutch constitutional state can help to assess the boundaries of the adoption of converging technologies for the purposes of monitoring people, improving forensic techniques, and profiling, identifying and monitoring potentially dangerous individuals or groups. These principles are not set in stone for eternity, however. They are co-evolving with the social and technical developments and with the changes in the relation between the interests of society at large and those of the individual. The inventory of principles and current (fundamental) rights merely clarifies where choices and trade-offs could be made.