nanoforum.org

European Nanotechnology Gateway

Tenth Nanoforum Report:

# Nanotechnology and Civil Security

June 2007

# Nanotechnology and Civil Security

A Nanoforum report, available for download from www.nanoforum.org.

**Editor**: Mark Morrison (IoN) mark.morrison@nano.org.uk

| **Chapters** | **Authors** |
|---|---|
| 1 – introduction | Mark Morrison (IoN) |
| 2 – detection | Aline Charpentier (CEA Leti) |
| 3 – protection | Olav Teichert (VDI-TZ) |
| 4 – identification | Kshitij Singh and Tiju Joseph (IoN) |
| 5 – societal implications | Ineke Malsch (MTV) |
| 6 – conclusions | Mark Morrison (IoN) |

# Nanoforum reports

The Nanoforum consortium has produced a number of reports on nanotechnology in Europe, all of which are available for free download from www.nanoforum.org

**General Reports:**

- 1st Nanoforum General Report: "**Nanotechnology Helps Solve the World's Energy Problems**", first published in July 2003, updated in December 2003 and April 2004.
- 2nd Nanoforum General Report: "**Nanotechnology in the Candidate Countries; Who's Who and Research Priorities**", first published in July 2003, updated in November 2003. Revised edition published September 2005.
- 3rd Nanoforum General Report: "**Nanotechnology and its Implications for the Health of the EU Citizen**", first published in December 2003.
- 4th Nanoforum General Report: "**Benefits, Risks, Ethical, Legal and Social Aspects of Nanotechnology**", first published in June 2004, updated October 2005.
- 5th Nanoforum General Report: "**European Nanotechnology Education Catalogue**", first published in March 2005.
- 6th Nanoforum General Report: "**European Nanotechnology Infrastructure and Networks**", first published in July 2005.
- 7th Nanoforum General Report: "**European Support for Nanotechnology SMEs**", first published in December 2005.
- 8th Nanoforum General Report: "**Nanometrology**", first published in July 2006.
- 9th Nanoforum General Report: "**Nanotechnology in Aerospace**", first published in February 2007.

**Series socio-economic reports:**

- "**VC Investment opportunities for small innovative companies**", April 2003.
- "**Socio-economic report on Nanotechnology and Smart Materials for Medical Devices**", December 2003.
- "**SME participation in European Research Programmes**", October 2004.

**Series background studies to policy seminars:**

- "**Nanotechnology in the Nordic Region**", July 2003.
- "**Nano-Scotland from a European Perspective**", November 2003.

**Workshop reports:**

- "**Nanotechnology and the Environment**", report from Nanoforum workshop, May 2006.
- "**Recommendations for Business Incubators, Networks and Technology Transfer from Nanoscience to Business**", report from Nanoforum Nano2Business Workshop, February 2007.
- "**Nanotechnology in Civil Security**", report from Nanoforum workshop, March 2007.

- "**Commercialisation of Nanotechnology – Key Challenges**", report from Nanoforum workshop, March 2007.

**Short reports:**

- "**Nanotechnology in Agriculture and Food**", May 2006.
- "**Nanotechnology in Consumer Goods**", October 2006.
- "**Nanotechnology in Construction**", November 2006.
- "**Education in the Field of Nanoscience**", January 2007.

**Others:**

- "**Nanotechnology in the EU – Bioanalytical and Biodiagnostic Techniques**", September 2004.
- "**Outcome of the Open Consultation on the European Strategy for Nanotechnology**", December 2004.
- "**Funding and Support for International Nanotechnology Collaborations**", December 2005.

# About Nanoforum

This European Union sponsored (FP5) Thematic Network provides a comprehensive source of information on all areas of nanotechnology to the business, scientific and social communities. The main vehicle for the thematic network is the dedicated website www.nanoforum.org. Nanoforum encompasses partners from different disciplines, brings together existing national and regional networks, shares best practice on dissemination of national, EU-wide and Venture Capital funding to boost SME creation, provides a means for the EU to interface with networks, stimulates nanotechnology in underdeveloped countries, stimulates young scientists, publicises good research and forms a network of knowledge and expertise.

Nanoforum aims to provide a linking framework for all nanotechnology activity within the European Community. It serves as a central location, from which to gain access to and information about research programmes, technological developments, funding opportunities and future activities in nanotechnology within the community.

The Nanoforum consortium consists of:

| | |
|---|---|
| The Institute of Nanotechnology (UK) | www.nano.org.uk |
| VDI Technologiezentrum (Germany) | www.vditz.de/ |
| CEA-Leti (France) | www-leti.cea.fr/uk/index-uk.htm |
| Malsch TechnoValuation (Netherlands) | www.malsch.demon.nl/ |
| METU (Turkey) | www.physics.metu.edu.tr/ |
| Monte Carlo Group (Bulgaria) | http://cluster.phys.uni-sofia.bg:8080/ |
| Unipress (Poland) | www.unipress.waw.pl/ |
| ENTA (UK) | www.euronanotrade.com |
| Spinverse (Finland) | www.spinverse.com |
| FFG (Austria) | www.ffg.at/ |
| NanoNed (Netherlands) | www.stw.nl/nanoned/ |

For further information please contact the coordinator, Mark Morrison:
mark.morrison@nano.org.uk

# What is Nanotechnology?

Nanotechnology is the manipulation or self-assembly of individual atoms, molecules, or molecular clusters into structures to create materials and devices with new or vastly different properties. This can be achieved by reducing the size of the smallest structures to the nanoscale (e.g. photonics applications in nanoelectronics and nanoengineering) or by manipulating individual atoms and molecules into nanostructures, which more closely resembles chemistry or biology.

The definition of nanotechnology is based on the prefix "nano", which is from the Greek word meaning "dwarf". In more technical terms, the word "nano" means 10-9, or one billionth of something. To illustrate this, a virus is approximately 100 nanometres (nm) in size.

Nanotechnology opens a completely new world of opportunities and solutions in all kinds of areas. An example for daily use is copying the water and dirt-repelling effect of leafs of the Lotus flower, and to use it for applications like newly developed bathroom tiles and surfaces, windows and paints. Apart from the field of diagnostics and analytics, nanotechnology is already appearing in the textile industry, the energy sector, electronics and automotive industry, to name just a few.

Further information on a variety of nanotechnology topics (including introductory material) can be found on the Nanoforum website, www.nanoforum.org

# 1 Introduction

Security is becoming an increasingly important facet of global society. The issues are many-fold and include protecting citizens and state from organized crime, preventing terrorist acts, and responding to natural and man-made disasters.

In October 2003 the European Commission engaged a "Group of Personalities" in the field of security research "to propose principles and priorities of a European Security Research Programme (ESRP) in line with the European Union's foreign, security and defence policy objectives and its ambition to construct an area of freedom, security and justice". This group reported their findings in March 2004 "Research for a Secure Europe", which recommended the formation of a European Security Research Advisory Board (ESRAB). This was established in July 2005 with a remit to operate until the end of 2006. ESRAB reported in September 2006 with a comprehensive description of strategies, sectors to be developed, and implementation routes (the result of the efforts of over 300 individuals). It recognised that some R&D can benefit security as well as other sectors (e.g. sensors, protective clothing, communication, and materials for decontamination); however it recommended that an annual budget of at least €1 billion be set aside for specific security research at the European level, and that a European Security Board be established.

In the context of Framework Programme 7, the EC has divided security R&D into four activity areas: protection against terrorism and crime; security of infrastructures and utilities; intelligence surveillance and border security; restoring security and safety in case of crisis. These are seen to have applications in many sectors including transport, civil protection, energy, environment, health, financial systems.

Nanotechnology has been a key priority in the Sixth EU framework programme for RTD (FP6, 2002-2006) and this remains the case in the Seventh Framework programme (FP7, 2007-2013), with a budget of €3475 Million for the NMP programme (€399.263 Million in the first call in 2007). With regards to nanotechnology research projects aimed at security applications; the EC funded three projects in the final call for FP6: TERAEYE, which has the objective of developing an innovative range of inspecting passive systems, based on Terahertz (THz) wave detection, to detect harmful materials for homeland security; DINAMICS, which has the objective of developing an exploitable lab-on-chip device for detection of pathogens in water supply systems; and NANOSECURE, which has the objective of developing systems that can be widely deployed for early warning and detoxification of harmful airborne substances with far higher efficiency than current methods. It is expected that some nanotechnology and security projects will be funded in the second call for proposals in FP7.

This report describes nanotechnology applications for civil security and divides this into four broad sections:

- **detection**, including imaging, sensors and sensor networks for the detection of pathogens and chemicals;
- **protection**, including decontamination equipment and filters, and personal protection;
- **identification**, including anti-counterfeiting and authentication, forensics, quantum cryptography and the market for counterfeit and grey goods;
- **societal impacts**, including current regulatory and ethical frameworks, potential impacts on ethics and human rights, and public perception.

The report concludes with a summary of the Nanoforum workshop on "Nanotechnology for Security" and describes some of the activities that are taking place in the EU Member States.

# 2 Detection

## 2.1 Introduction

The ability to accurately and rapidly detect different substances (chemical and biological), objects and people is key to preventing many civil security problems. Improvement in detection technologies is driven by reduction in device size, increased sensitivity and selectivity, and the possibility of hidden detection systems. MEMS already offers advances in this sense, however nanotechnologies should provide further improvements, as well as easier to use and cheaper detection devices.

The function of such systems is to detect:

- biological agents like viruses, bacteria, DNA, RNA, proteins, nucleotides to prevent bioterrorism as well as bio dissemination of a dangerous agent (e.g. anthrax, ebola);
- chemical agents like poisons (e.g. sarin gas), industrial gases (e.g. hydrogen, carbon monoxide);
- radiation: α, β, γ rays;
- optical properties (wavelength measurement and imaging);
- other physical properties such as temperature and pressure

For the purpose of this report, three classes of detection devices for civil security have been identified that are influenced by nanotechnology advances:

- imaging devices- X-ray screening, infra-red detection, and the emerging field of terahertz imaging.
- sensor devices- biological and chemical applications.
- miniaturized sensor networks- also known as smart dust. These have specific constraints due to their portability and autonomy (energy, data management).

## 2.2 Image detection

Different image detection methods utilising different parts of the electromagnetic spectrum are possible (see Figure 2.1).

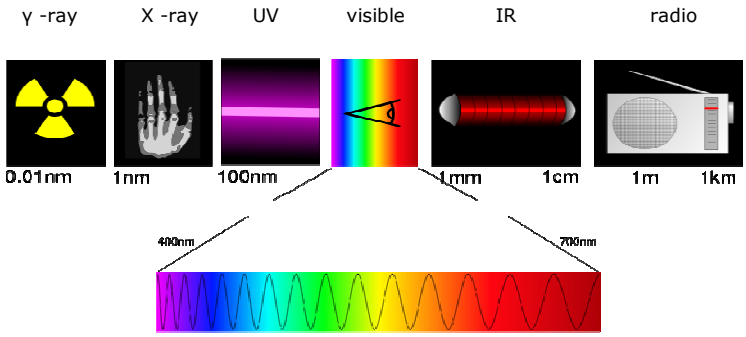



**Figure 2.1** The electromagnetic spectrum; http://fr.wikipedia.org/wiki/Image:Spectre.svg

The most common image detection methods are γ-ray and X-ray (to screen the inside of containers, luggage); visible light using cameras in public places to detect suspicious behaviour or known individuals; infra-red to detect body heat or that from weapons and vehicles. Finally terahertz frequencies are gaining huge interest for their use in both imaging and spectrometry.

### 2.2.1 Gamma-Ray imaging

Gamma-ray imaging ($10^{-14}$m<λ<$10^{-11}$m) can be used to quickly pre-screen containers in goods storage areas or transport vehicles. There were no nanotechnology applications found for this kind of detection device.

### 2.2.2 X-Ray imaging

X-ray imaging ($10^{-11}$m<λ<$10^{-8}$m) is probably the most widespread system used for security (e.g. for airport baggage screening, container inspection). An X-ray device needs an emitting source of X-rays and a receptor that converts the received signal. Nanotechnology has the potential to enhance both, however current applications are only found for emitters.

It has been shown that carbon nanotubes can significantly improve current X-ray devices. The key component of the device is a gated carbon nanotube (SWNT) field emission cathode comprising an array of electron emitting pixels that are individually addressable by a metal oxide semiconductor field effect transistor (MOSFET) based electrical circuit (see Figure 2.2). The carbon nanotube technology allows the device to be operated at room temperature rather than at 1000°C which conventional sources require. It can also be operated as a high speed X-ray camera, capturing clear images of objects moving at high speed. Carbon nanotubes also enable smaller, faster and cheaper scanners, using less electricity and producing higher resolution images (S. Wu, 2005). Various patents are already deposited and the technology, developed by scientists from University of North Carolina and Xintec Inc is under development for commercial application in the UNC start up, Xintec.

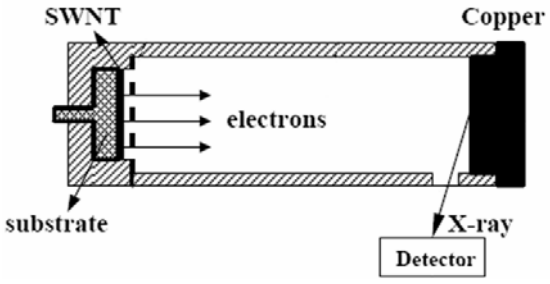



**Figure 2.2** SWNT field emission cathode for X-ray imaging. Source: http://www.physics.unc.edu/~zhou/muri/pubfiles/gyue_xray_appl.pdf

Another technique that shows promises to enhance the efficiency of X-ray detection (particularly for weapons of mass destruction or dirty bombs) is the dual energy X-ray technique (DXA or DEXA). DEXA employs two X-ray projection images of an object: a low and a high energy spectrum. There are no specific nanotechnology applications for this technology, but carbon nanotubes can be used for the cathode.

### 2.2.3 Visible imaging

Visible imaging (400nm<λ<700nm) concerns cameras, and more often closed circuit television (CCTV). No specific nanotechnology applications have been found that improve visible detection, but progress in several other areas has been made, including the transition from CCD to CMOS detectors. The CMOS process allows size reduction (in 2005 a 150 nm detector was designed), and better integration capacity for better imaging quality.

### 2.2.4 Infra-Red imaging

Infra-red imaging (1μm<λ<300μm) detects heat points. Two levels of IR detection are used: medium IR wavelength (3-5μm), for high temperatures emitted by, for example, combustion engines, and long IR wavelength (8-12μm), emitted by, for example, body heat.

An IR detector for an imaging device can take the form of a thermo detector (so-called bolometer); photo detector (based on semi-conductors); or optical antenna. Nanotechnologies can find applications in all three kinds of sensors.

**Bolometer**

A bolometer is an electromagnetic radiation detector. It consists of a thermally isolated material whose resistivity dramatically changes as a result of the temperature variation induced by incident electromagnetic energy (see Figure 2.3). Electrical bolometers used for IR radiation are much more sensitive than other sensors and are capable of operating at room temperature. The most commonly used sensor is a resistor made of material with a high thermo resistance coefficient (TCR) such as vanadium oxide or amorphous silicon.

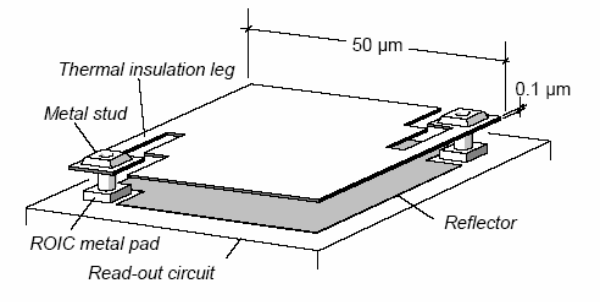



**Figure 2.3** Microbolometer pixel; http://www.save-u.org/download/PDF/AMAA_200305.pdf

Its disadvantage, compared to other IR sensors (such as photo detectors based on semiconductor diodes),[1] is a slower response. The sensitivity is partly limited by the thermal conductance of the pixel. The speed of response is limited by the thermal heat capacity divided by the thermal conductance. Reducing the heat capacity increases the speed but also increases mechanical thermal temperature fluctuations (noise). Increasing the thermal conductance raises the speed, but decreases sensitivity.

Most studies focus on increasing thermal conductance without affecting sensitivity. Carbon nanotubes (as a result of their exceptional thermal and electrical properties) are the most promising technology in this field. Carbon nanotubes, can be grown as single-wall tubes directly on the substrate between electrodes forming a 'nanobridge' that has particular photonic absorption properties in infrared wavelengths. Tunnelling contacts between the carbon nanotubes and aluminium electrodes are obtained and make it possible to reduce the resistance of the bolometer considerably (M.Tarasov, 2006, see Figure 2.4). The author interprets this phenomenon as "electron cooling".

[1] Megan Fellman, "Technology holds promise for infrared camera", august 2005
http://www.northwestern.edu/univ-relations/media_relations/releases/2005/08/infrared.html

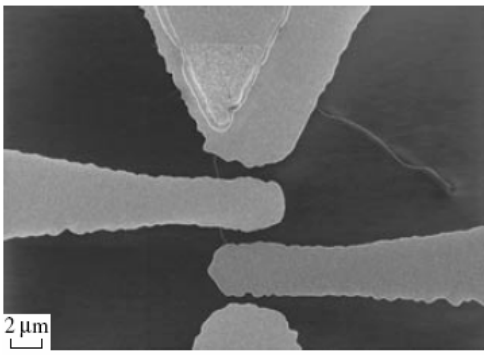



**Figure 2.4** Two nanotubes grown on the silicon substrate and covered with aluminium electrodes. Source : http://www.springerlink.com/content/8k4503l258h54387/fulltext.pdf

## Photo detector

Photo detectors are based on semiconductor materials and detect IR signals more quickly than bolometers. Mercury cadmium telluride (HgCdTe), which works at both medium and long IR wavelengths, is one of the most common materials used in photo detectors; however its limitation is the need to use a cryostat to manage heat generated in the device.

Researchers at Northwestern University have developed a less expensive hand-held infrared imaging device, that does not require cooling. Using an InAs/GaSB type II superlattice (an atomic assembly of layers of only a few nanometres thick) they have produced a non-cooled 256x256 pixel camera. The InAs/GaSb type-II strained layer superlattice (SLS) is of great interest for both mid- and long-wave infrared detection. As photonic detection is faster than thermal detection it can be used for operations in which speed is a necessity, for example missile detection.

Another possibility for the enhancement of IR photo detectors is the use of quantum dots. InGaAs quantum dots, grown by self-assembly on an InGaP matrix show several advantages for middle wavelength infrared detection, including: absorption of normally incident light, due to the three dimensional confinement of electrons; higher responsiveness due to the longer lifetime of excited electrons; and higher operation temperature due to the low dark current[2] (J. Jiand et al., 2004). Vertical aligned superlattices of multiple self-assembled Ge island layers, separated by Si spacer layers on Si substrates also show improved IR photodetection (W. Minsheng et al., 2004).

## Optical antenna

An optical antenna is a dipole antenna coupled to a transducer. The size of an optical antenna is in the range of the detected wavelengths and involves fabrication techniques with nanoscale spatial resolution. Due to their optical, electrical, and thermal properties carbon nanotubes have been studied as replacements for traditional antenna materials. Metallic rods of 50 nm in diameter and 200-1000 nm in length composed of multi walled carbon nanotubes (MWCNT) can interact with electromagnetic radiation like a dipole antenna, demonstrating both the polarization and the length antenna effect. The first effect is characterized by a suppression of the reflected signal when the electric field of the incoming radiation is polarized perpendicular to the nanotube axis. The second, the antenna length effect, maximizes the response when the antenna length is a proper multiple of the half-wavelength of the radiation. These effects can be used in a variety of optoelectronic devices including IR detectors (Y. Wang et al., 2004).

[2] dark current is background electrical noise produced by a photodetector even in the absence of light. It is normally compensated for by decreasing the operating temperature.

### 2.2.5 Teraherz (THz) imaging

The THz (300μm<λ<3mm) range lies between millimetre radio waves and far infrared light waves and exhibits properties from both sides of the electromagnetic spectrum (see Figure 2.5).

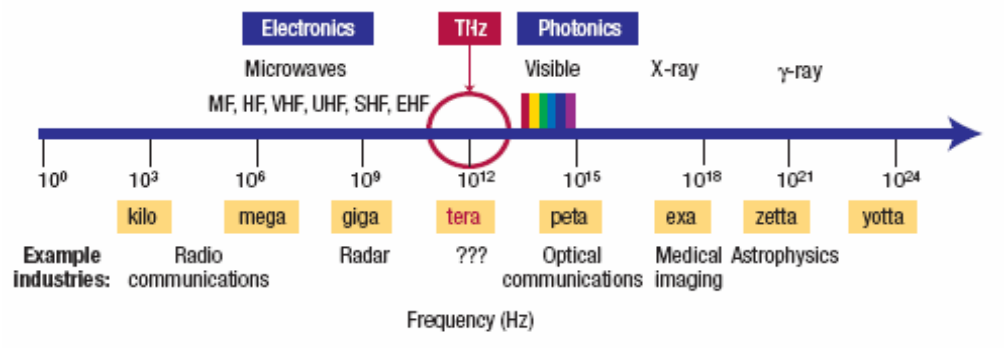



**Figure 2.5** Teraherz spectrum. Source: http://www.eleceng.adelaide.edu.au/thz/publications/ferguson_2002_npg.pdf

Like radio, THz waves can be transmitted through a wide variety of substances such as paper, clothes, ceramics, plastics, wood, bone, fat, various powders, dried food and so on. In addition, like light waves, they can easily be propagated through space, reflected, focused and refracted, using THz optics. Furthermore, the short wavelength (several hundreds of μm, which is much shorter than radio waves), allows a spatial resolution which is sufficient for many imaging applications (Y. Watanabe et al., 2003). As such, THz imaging has the potential to reveal concealed explosives; metallic and non-metallic weapons (such as ceramic, plastic or composite guns and knives); flammables; biological agents; chemical weapons and other threats hidden in packages or on personnel (see Figure 2.6). Because terahertz imaging employs safe non-ionizing radiation that penetrates clothing, people may be routinely scanned as well as packages (J.F. Federici, 2005).

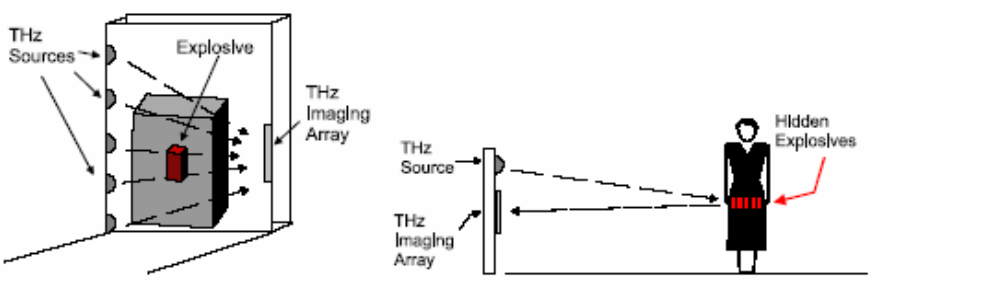


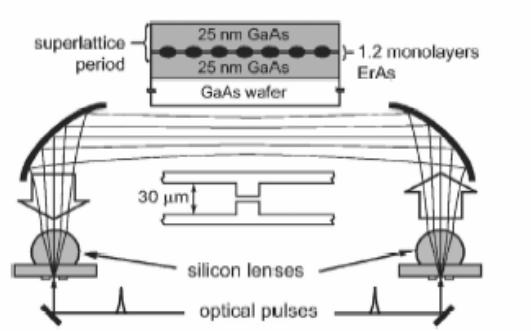

**Figure 2.6** Illustration of a potential implementation of a THz imaging array in transmission mode and reflection mode. Source : http://ej.iop.org/links/r9OMunlu1/9umxnYX52xG0dzZ9av5vpA/sst5_7_018.pdf

Both the emitter and detector components required by THz imaging devices can be enhanced by nanotechnologies, but most applications are in the detector components.

THz waves can be detected by photo detector-like antennas as well as transistors. Several kinds of antenna can be used to detect THz waves: bow-tie dipole antenna, corner reflector antenna, dielectric lens antenna, and planar antenna; however carbon nanotube antennas appear to have the greatest potential. A team of Chinese researchers simulated MWCNTs arrays and concluded that CNT have huge potential determined by the number of array elements, an appropriate inter-tube distance and controlled length of carbon nanotubes in the array (Y. Lan, 2006).

Self-assembled ErAs:GaAs nano-island superlattices have recently been demonstrated as potential photoconductive antennas (see Figure 2.7). The ErAs:GaAs based detector shows a strong enhancement in THz detection efficiency with respect to incident optical power, though optical saturation occurs more rapidly. Detected THz bandwidth and signal-to-noise ratios are simultaneously maintained or improved.

**Figure 2.7** Illustration of ErAs:GaAs based THz detector. Figure Source:




http://scitation.aip.org/getpdf/servlet/GetPDFServlet?filetype=pdf&id=APPLAB000088000025251119000001&idtype=cvips&prog=normal

The interaction between CNT and potassium ions could potentially be exploited for room temperature THz detection. A team at the Beckman Institute for Advanced Science and Technology, University of Illinois, has shown that potassium ions binding strongly with a CNT induce a dielectric field in the CNT and oscillate at a frequency of about 0.4 THz. This "nano oscillator" may serve as a THz wave detector which can operate at room temperature (Schulten et al., 2005, see Figure 2.8).

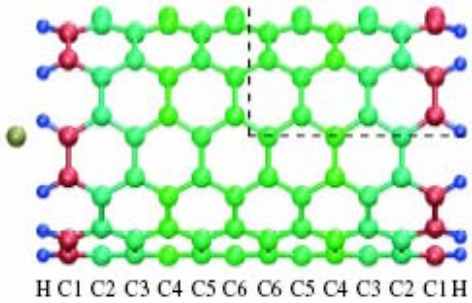



**Figure 2.8** Nano-oscillator: The nanotube is coloured according to initial atomic partial charges q0. Blue (H): positive; red (C1): negative.

Source:
http://scitation.aip.org/getpdf/servlet/GetPDFServlet?filetype=pdf&id=PRLTAO0000950000242468010000001&idtype=cvips&prog=normal

Quantum dots may also be useful for THz detection. A device, termed a "quantum dot infrared photodetector (QDIP)", has been designed which consists of multi-layered self-organized InAlAs/GaAs quantum dots that respond to THz radiation (from 20 to 75 μm) at temperatures up to 150K (X.H Su et al., 2006, see Figure 2.9). In addition, recent work has shown the potential sensitivity of an integrated quantum dot device that can transfer absorbed THz radiation at a level of $10^8$ electrons per photon (P. Kleinschmidt et al., 2007).

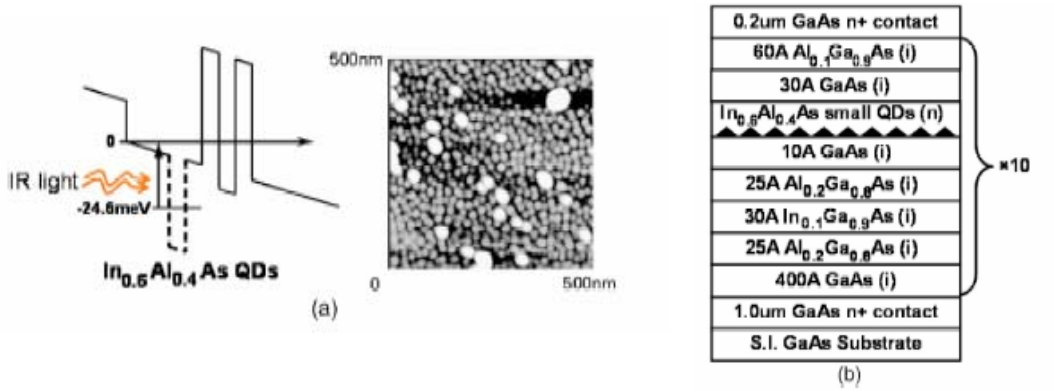



**Figure 2.9** (a) Single period conduction band schematic diagram and AFM image of In0.5Al0.4As/GaAs dots; (b) Schematic heterostructure of T-QDIP grown by molecular beam epitaxy.

Source:
http://scitation.aip.org/getpdf/servlet/GetPDFServlet?filetype=pdf&id=APPLAB000089000003031117000001&idtype=cvips&prog=normal

There is a vast array of potential THz sources, and progress in lasers, antennas and material research continue to provide new candidates where nanotechnology applications can be found. Concerning materials, the greatest potential is in the field of metamaterials. Metamaterials are artificially structured materials with novel electromagnetic and often optical properties. A lot of research has demonstrated the efficiency of metamaterials as THz emitters, but no nanotechnology applications were found in this field.

The recent development of the quantum cascade laser, consisting of repeating coupled quantum wells (nanometre thick layers of GaAs sandwiched between potential barriers of AlGaAs), has allowed Sandia National Laboratories to develop semiconductor sources of THz radiation capable of power output in excess of 100mW. Previously such powers could only be obtained by molecular gas lasers occupying cubic metres and weighing more than 100kg.[3]

## 2.3 Sensors

Nanotechnologies allow the development of new classes of sensors which can better answer current security constraints. Nanotubes, nanoparticles, and quantum dots enable sensors to be further miniaturized, become more sensitive, and to be used directly in the field rather than the lab. Such sensors can be highly selective while simultaneously detecting various hazardous agents. Two classes of sensors have been identified based on direct or indirect detection. It appears that nanotechnology applications for sensors are essentially for the detection of molecules or organisms, i.e. biological or chemical agent detection.

[3] "Sandia develops next generation of screening devices", Physorg, 22/01/2007
http://www.physorg.com/news88711571.html

### 2.3.1 Direct detection

Nanostructured materials such as carbon nanotubes and metal oxide nanowires promise superior performance over conventional materials due to selective uptake of gaseous species (based on controlled pore size and chemical properties) and increased adsorptive capacity (due to increased surface area).

**Nanotubes**

The binding of gas molecules to the surface of a carbon nanotube affects its electronic properties which can be exploited in sensor technologies. Such sensors can be based on single CNTs or CNTs assembled in arrays to provide simultaneous detection of different molecular species. Single walled carbon nanotubes (SWCNT) can be combined with a silicon-based microfabrication and micromachining process that enables the fabrication of sensor arrays with the advantages of high sensitivity, low power consumption, compactness, high yield and low cost (see Figure 2.10). SWCNT can be coated with specific chemical groups providing a selective adsorption of different analytes. By measuring changes in surface enhanced capacitance, real-time detection and quantification of different target molecules such as explosives and neurotoxins can be achieved (A.S Snow et al., 2005).

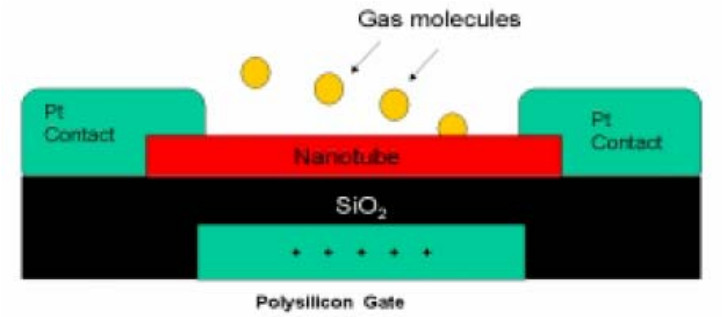



**Figure 2.10** Illustration of a CNT-based sensor. Source: http://people.nas.nasa.gov/~cwei/Publication/cnt_sensor.pdf

Various projects involving CNTs for sensor technologies have been awarded: Rensselaer researchers were awarded a 1.3M$ NSF grant in 2003 to develop CNT sensors for homeland security; Nanomix, a molecular electronics start-up which developed CNT based electronic devices secured a 1M$ grant from the Department of Homeland Security to develop sensing technology in 2007; finally NASA Ames research centre has already developed a CNT based chemical sensor array.[4]

**Nanowires**

Zinc oxide nanowires can be used to detect several substances as a result of changes in electrical conductivity due to chemical adsorption (e.g. nitrogen dioxide gas reduces current whereas carbon monoxide increases it). ZnO can also be used in the form of a thin film, however the nanowire has a larger surface to volume ratio. An additional benefit is the rapid dissociation of adsorbed chemical, allowing the nanowire to be "reset". Such sensors are under development at the University of South Carolina where researchers are working on the integration of several sensing units in the form of an array (to create a sort of electronic nose) and also on the feasibility of configuring an array of vertical ZnO nanowires vertically in an array for use as a solar powered battery.[5]

4 "carbon nanotube sensor for gas detection", http://www.nasa.gov/centers/ames/research/technology-onepagers/gas_detection.html

5 "ZnO nanowires may lead to better chemical sensors, high-speed electronics", physorg, 09/2006, http://www.physorg.com/news77303473.html

Other work reports the use of silicon nanowires functionalized with PNA (peptide nucleic acid) for real time, label-free detection of DNA. The PNA complexes act as "receptors" for specific sequences of DNA (see Figure 2.11).

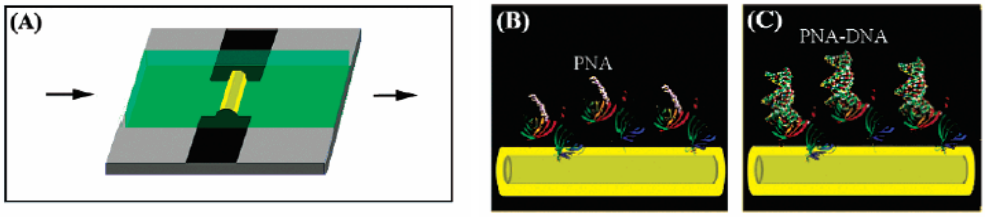



**Figure 2.11** (A) Schematic of a sensor device consisting of a SiNW (yellow) and microfluidinc channel (green), where the arrows indicate the direction of sample flow; (B) SiNW surface with PNA receptor; (C) PNA-DNA duplex formation

Source: http://pubs.acs.org/cgi-bin/article.cgi/nalefd/2004/4/i01/pdf/nl034853b.pdf

Concentration dependent measurements show that detection can be carried out to at least the tens of femtomolar range. The sensor shows extreme sensitivity and good selectivity and could provide a pathway to integrated, high throughput, DNA detection for different bio-threats. (J.I. Hahm and C. Lieber, 2004).

## 2.3.2 Indirect detection

Indirect detection involves an intermediary step between detecting the presence of the agent of interest and the actual readout. Such bio/chemical detection technologies involve nanoparticles, quantum dots, barcodes, cantilevers, and SERS.

### Nanoparticles

Nanoparticles can be involved in two kinds of indirect detection: electrical or electromechanical detection, and optical detection that provides a colorimetric or fluorescent response.

- **Electrical and electromechanical**

Electrical and electromechanical detection methods offer the possibility of portable assays that could be used in a variety of point-of-care environments.

For example, palladium nanoparticles can be used as a hydrogen sensor. The technology is based on the fact that hydrogen dissociates on the surface of palladium, dissolves into the crystal lattice and causes an increase in electrical conductivity. In thin films of palladium this allows a detection of 0.5% hydrogen, however lattices of nanoparticles of palladium show much greater sensitivity (around 0.001%). This sensor has a fast response time (in the range of seconds) and has been developed by Applied Nanotech Inc (I. Pavlovsky et al., 2006).

Nanoparticle sandwich assays combined with silver amplification can be used for the electrical detection of DNA in a handheld format. This makes use of two components to detect target DNA: a substrate with oligonucleotides (that can bind part of the target DNA) attached between two electrodes; and nanoparticles with a second oligonucleotide attached (that can bind sequences in a second part of the target DNA). In the presence of target DNA the nanoparticles are linked to the substrate between the electrodes, and can then be used for the deposition of silver, providing an electrical contact between electrodes (see Figure 2.12). This process exhibits a selectivity factor of 10 000:1 and eliminates the need for on-chip temperature control, dramatically reducing the complexity of a hand-held device for DNA detection.

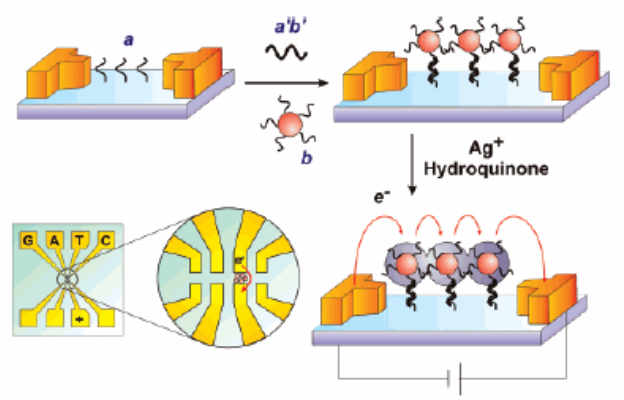



**Figure 2.12** When the capture/target/probe sandwich is positioned in the gap between two electrodes, catalytic reduction of silver onto the sandwich system results in a signal that can be detected electrically.

Source: Science http://www.aaas.org

Gold nanoparticles have been investigated for use in sensors for both chemical and biological warfare agents. One example, 'chemiresistors', makes use of thin films of gold nanoparticles encapsulated in monomolecular layers of functionalized alkanethiols that have been deposited on interdigitated microelectrodes. These reversibly absorb vapours leading to monolayer swelling or dielectric alteration in the thin film and production of a small current. The system appears to have minimal water sensitivity, and can detect harmful vapours down to the parts per billion level or lower. Selectivity of the sensors can be tailored by changing the structure and functionality of the alkanethiol. This sensor has been developed by STREM chemicals.

- **Colorimetric**

Nanoparticles have shown exceptional colorimetric properties that can easily replace traditional fluorescent detection systems. For example, a single 80 nm gold particle has a light-scattering power equivalent to the signal generated from about $10^6$ fluorescein molecules, and unlike molecular fluorophores, the light-scattering signal from metal nanoparticles is quench resistant. (N.L. Rosi and C.A. Mirkin, 2005).

Researchers from Georgia Institute of Technology have used 2.5 nm gold nanoparticles as quenchers in a molecular fluorophore nucleic acid probe, to detect the presence of target DNA (S. Nie et al., 2002, see Figure 2.13).

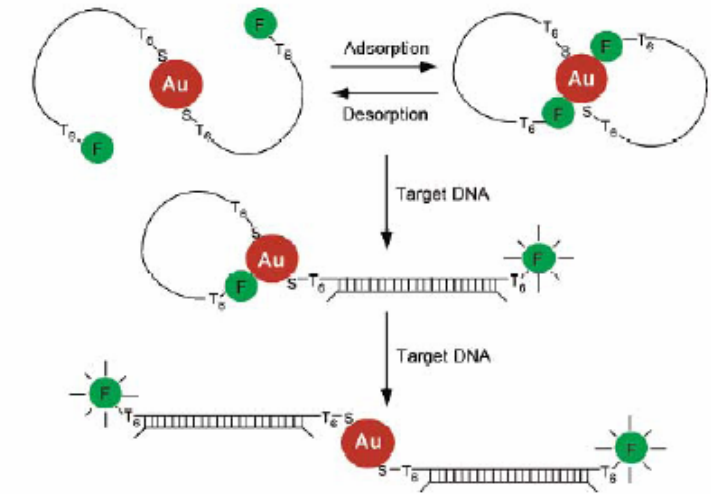



**Figure 2.13** Gold nanoparticles are modified with oligonucleotides functionalized on one end with a thiol and the other end with a molecular fluorophore. The thiol binds to the surface of the gold particle, and the fluorophore can interact non-specifically with the gold, resulting in a "loop" structure in which the gold nanoparticle quenches the emission from the fluorophore. In the presence of target DNA the "loop" is broken, separating the fluorophore from the nanoparticle quencher, and resulting in measurable fluorescence.
Source: http://pubs.acs.org/spotlight/november2002/ja025814p.pdf?sessid=7922

Gold nanoparticles can also serve as simple colorimetric test to detect mercury in water. Developed in 2007 in Northwestern University by Chad Mirkin and his team, the principle is based on the different colours of 15 nm diameter gold nanoparticles in solution- red when separated and blue when agglomerated.[6] Complementary oligonucleotides with a single nucleotide (thymidine-thymidine, T-T) mismatch are attached to the surface of the gold nanoparticles. These allow the nanoparticles to agglomerate, however they can be forced apart by heating the solution. In the presence of mercury (which binds strongly to T-T mismatches) the temperature required to break the interaction between nanoparticles is raised, and directly quantifiable with the amount of mercury present. The system is extremely sensitive (detecting mercury at levels as low as 100 nM). The team wants to extend research on other metals to provide simple, portable detection devices.

Researchers of University of North Dakota have developed fluorescent dye-doped silica nanoparticles functionalized with oligonucleotides as labels for chip-based sandwich DNA assays. The nanoparticles are composed of a silica matrix that encapsulates large numbers of fluorophores and can detect DNA target down to 1fM. They have also used similar particles to detect single bacterium cells by modification of the fluorescent nanoparticles with specific monoclonal antibodies. (Tan et al., 2003).

Recent work at UC Davis has seen the creation of a new type of nanoparticle, between 100 and 200 nm in size, which possesses magnetic and luminescent properties. These nanoparticles comprise a magnetic core of iron oxide doped with cobalt and neodymium ($Nd:Co:Fe2O_3$) encapsulated in a luminescent shell of europium and gadolinium oxide ($Eu:Gd_2O_3$). When stimulated with a laser, europium emits red light. The nanoparticles can also be manipulated with magnets and detected by fluorescence or coated with short pieces of DNA and used for bio analysis (e.g. ricin, botulinum toxin) (D. Dosev et al., 2007).

[6] http://www.sciencedaily.com/releases/2007/04/070427072203.htm

## Quantum dots

Quantum dots, with their broad excitation spectra, sharp emission spectra, and easily tuneable emission properties, are strong candidates for replacing conventional fluorescent markers in biodetection assays (N.L. Rosi and C.A. Mirkin, 2005).

Studies have looked at functionalising quantum dots directly with biomolecules (such as oligonucleotides) or incorporating quantum dots in microbeads, that are subsequently functionalised. By preparing a panel of quantum dots or microbeads functionalised with different oligonucleotides, for example, it is possible to simultaneously detect multiple target DNA sequences (multiplexing) by virtue of the different emission spectra of the quantum dots or microbeads (Nie et al., 2001, Medintz et al., 2005). See Figure 2.14 for an illustration.

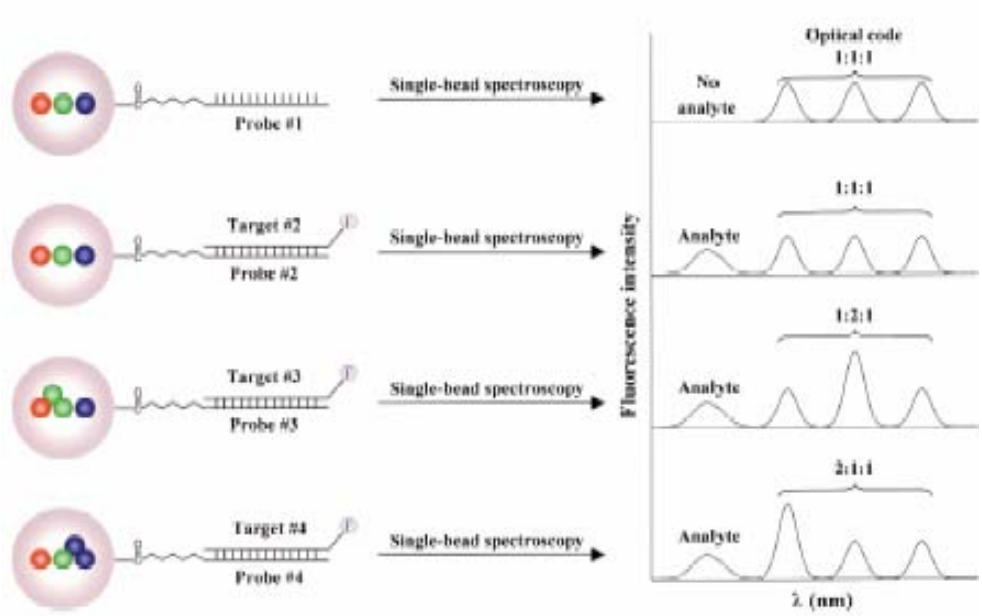



**Figure 2.14** Quantum dots (incorporated in beads) can be employed for detecting multiple targets in a single assay. Specifically, varying the numbers and ratios of different quantum dots per target results in a unique fluorescent signal for each individual target.

Source: http://faculty.washington.edu/xgao/Images/QD-beads.pdf

## Barcodes

The Bio Bar Codes Amplification principle (BCA) employs oligonucleotides that act as "bar-codes" for target DNA. It is composed of two parts: magnetic microparticles which are functionalized with complementary strands to the target DNA, and gold nanoparticles which are functionalized with both complementary strands to another part of the target DNA and hundreds of "bar-code" oligonucleotides. In the presence of target DNA, the magnetic microparticles and gold nanoparticles form sandwich structures. These are magnetically separated from solution and washed with water to remove the bar-code DNA from the gold nanoparticles. The "bar-codes" (hundreds to thousands per target) are subsequently detected using the scanometric approach (which involves hybridisation to a second series of functionalised gold nanoparticles, followed by silver deposition), resulting in detection limits as low as 500 zM (10 strands in solution). (see Figure 2.15, C.A. Mirkin et al., 2004)

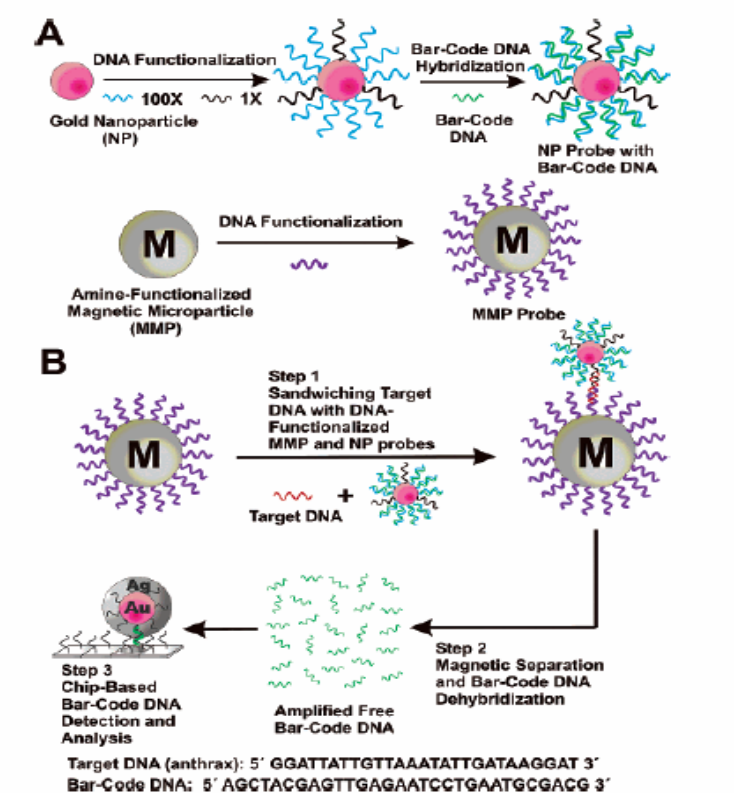



**Figure 2.15** A) Nanoparticle and magnetic microparticle probe preparation; (B) Nanoparticle-based PCR less DNA amplification scheme

Source: http://pubs.acs.org/cgi-bin/article.cgi/jacsat/2004/126/i19/pdf/ja049384+.pdf

Barcodes can also be used for the immuno-detection of biological agents. At Lawrence Livermore National Laboratory (LLNL) a bioweapon-recognition device has been designed which consists of nanowires patterned with bands of silver, gold and nickel. Different "bar-coded" wires are functionalised with antibodies to different pathogens, resulting in an optical indicator of the presence of different pathogens in a sample. The method is extremely efficient, as 100 different striped nanowires can be analysed in one snapshot.[7]

7 "Nanotechnology barcodes to quickly identify biological weapons", Nanowerk, March 2007, http://www.nanowerk.com/spotlight/spotid=1585.php

## Cantilevers

Advances in photo- and e-beam lithographic techniques enable the fabrication of more complex devices at the micrometre and nanometre scale. Microcantilevers (with nanoscale thickness) can be used to detect biomolecules, micro-organisms and chemicals by measuring changes in oscillating frequency as a result of binding (see Figure 2.16).

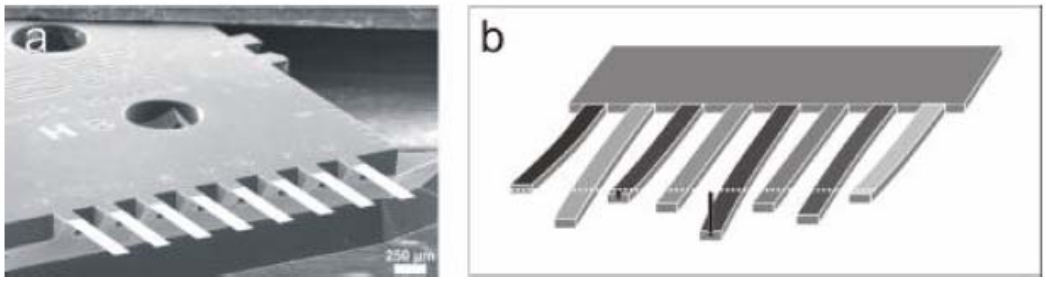



**Figure 2.16** (a) SEM image of an array of silicon cantilever (length: 500µm, width; 100µm, thickness: 500nm) (b) Schematic drawing of a cantilever array with different sensitive layers.

Source: http://www.ewh.ieee.org/tc/sensors/Sensors2003/Lang.pdf

Detection can be performed in both gas and liquid phases, however performances are deteriorated when detection is operated in liquid environments because the motion of the cantilever is dampened by the liquid. Recent work at MIT (Burg and Manalis) provides a solution to this by confining liquid to channels inside the cantilever. This is capable of weighing single nanoparticles, cells and proteins with a mass resolution of better than one femtogram.

Functionalizing microcantilevers with target capture DNA, for example, provides a platform for the formation of a sandwich assay between capture DNA, target DNA, and DNA modified gold nanoparticle labels. The gold labels provide a site for silver ion reduction, which increases the mass on the cantilever and results in a detectable frequency shift that can be correlated with target detection. The detection of viruses and bacteria is also possible using nanoelectromechanical devices (N.L. Rosi and C.A. Mirkin, 2005).

## SERS / Raman detection

Attaching Raman-dye-labelled oligonucleotides to gold nanoparticle probes generates spectroscopic codes for individual targets, thus permitting multiplexed detection of analytes (see Figure 2.17). The presence of the target is confirmed by silver deposition on the gold nanoparticle (as low as 1 fM), and the target identity is confirmed by surface-enhanced Raman scattering (SERS) signature. The advantages over fluorophore based systems are: narrower spectroscopic bandwidths per dye (hence less overlap and noise) but broader overall spectrum available (potentially allowing greater multiplexing); and only a single wavelength laser radiation is needed to scan a highly multiplexed array with numerous target-specific Raman dyes (N.L. Rosi and C.A. Mirkin, 2005).

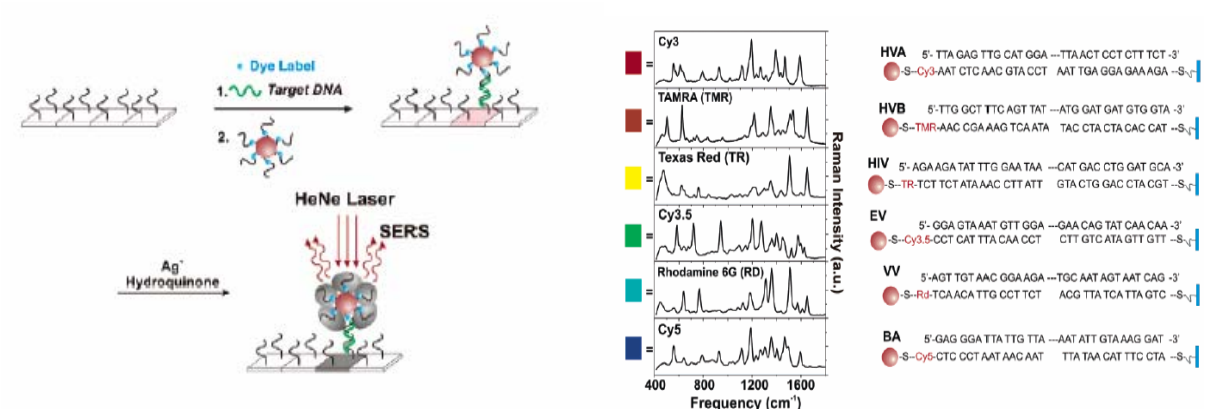



**Figure 2.16** SERS detection of target DNA sequences.

A simpler method using SERS detection was developed at the end of 2006 to detect viruses and potentially other bioagents. It works by measuring the change in frequency (Raman shift) of a near infrared laser as it scatters off viral DNA or RNA. But as the signal is weak, researchers from University of Georgia (Athens) patented a method that involves placing rows of silver nanorods at a density of 13 nanorods/mm$^2$ and a 72°±4° angle from the normal on the substrate that holds the sample and amplifies the signal (see Figure 2.17). With this method, it is possible to rapidly detect a virus directly inside a person with a portable device (30-50s). In initial experiments, the UGA group was able to measure the SERS response of different virus samples and detect differences between viruses, viral strains, and viruses with gene deletions in under a minute, which shows promises for fast response multi-detection devices. (S. Shanmukh et al, 2006).

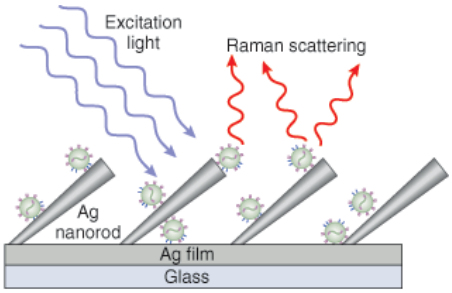



**Figure 2.17** SERS detection of target DNA developed by UGA. Source: http://www.laserfocusworld.com/display_article/282662/12/ARCHI/none/News/RAMAN-SPECTROSCOPY:-SERS-and-silver-nanorods-quickly-reveal-viral-structure

## 2.4 Sensor networks

The ultimate goal for sensor technologies is to create completely autonomous systems that are self-sufficient for energy, able to measure some parameter(s), store data and transmit it to other sensors or to the final user.

This is embodied in a technology system known as "smart dust" which is being developed in various research centres (such as the University of California Los Angeles (WINS project) and the University of California Berkeley, which is financed by DARPA to develop the Smart Dust project). Recently, Applied Nanotech Inc (a subsidiary of Nano-Proprietary Inc) announced that they had raised a 100 000 USD SBIR phase I to develop a "sensor Network Design Tool" from the Homeland Security Advanced Research Project Agency (HSARPA).

Smart dust can be described as a self-contained, millimetre-scale sensing and communication platform for a massively distributed sensor network. The entire device

contains sensors, computational ability, bi-directional wireless communications, and a power supply, while being inexpensive enough to deploy by the hundreds (see Figure 2.18). This kind of device is possible to build using state-of the-art technologies, but will require evolutionary and revolutionary advances in integration, miniaturization, and energy management.[8]

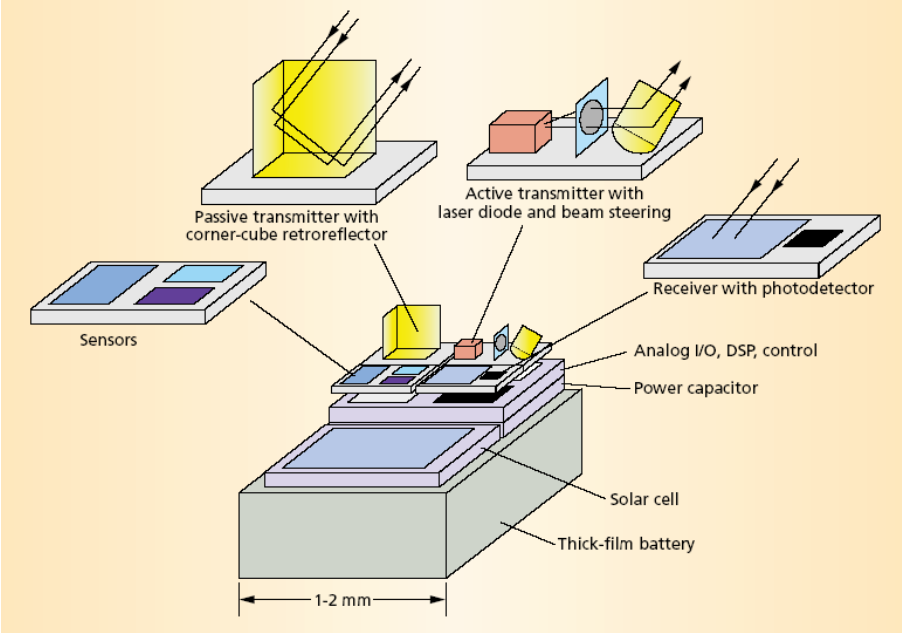



**Figure 2.18** "Smart Dust: Communicating with a cubic-millimeter computer": http://ieeexplore.ieee.org/iel5/2/19363/00895117.pdf?arnumber=895117

The advantages of this kind of device are: portability, autonomy, and small size for an exponentially decreasing cost. The goal is to use them in places that humans cannot go (e.g. in contaminated sites), and to allow continuous detection in strategic locations (e.g. airports). They can serve as sensors for biological, chemical or radioactive agents.

Nanotechnologies will not bring huge advancements in terms of miniaturization because the development of Micro Electro Mechanical Systems (MEMS) has already achieved this. The sensor component will use technology described in previous sections, however for smart dust to be successful will require advances in the fields of power (energy scavenging, generation, storage) and data (transmission, processing) management.

### 2.4.1 Power management

The power system may consist of a battery (essentially lithium ion or nickel metal hydride) and/or a solar cell with a charge integrating capacitor for periods of darkness. Other power systems are under study principally in the field of energy scavenging, e.g. using vibration to generate power.

**Batteries**

The lifetime and efficiency of charging and discharging cycles in batteries is critically dependent on storage and/or the intercalation properties of the anode material. Carbon nanotubes can provide an alternative to current anode fabrication technology (based on graphite). CNT anodic layers around metal cathodes, such as Cu, are under investigation as well as Li and K intercalation in SWCNT bundles and/or MWCNT. Other experiments report increasing reversible charge capacity by a 600% by introducing nanoparticles of cobalt nickel and ferric oxides in the electrode material of lithium ion batteries (Poizot et

[8] http://www-bsac.eecs.berkeley.edu/archive/users/warneke-brett/SmartDust/

al., 2000). Tin based anode materials are also in use and provide higher energy capacities and quicker charging rates.[9]

Cathodes can be built from carbon nanotubes, or other nanomaterials such as $TiO_2$, vanadium oxide or $LiCoO_2$-particles.

**Energy scavenging**

Energy scavenging is a promising mode for fully autonomous smart dust to provide system power.

The first application is solar cells. At present the most efficient solar cells are based on III/V-semiconductors such as GaAs and InP and have a conversion efficiency of roughly 30%. Quantum dots have the potential to increase this to over 80%, by virtue of their ability to absorb different wavelengths of light. The principle would be to use layers of quantum dots of different size or composition to harness more of the available light.

Other applications can be found in the field of nano-piezotronics. Recently, researchers at the Georgia Institute of Technology built a device that generates an electrical current from the vibration of a large array of zinc oxide nanowires (piezoelectric effect). The nanowires are grown on either gallium nitride or sapphire that serves as the bottom electrode. The nanogenerator delivers a high power density compared with similar microgenerators and improving the uniformity of the device should further increase the power output (X. Wang et al., 2007).

Other possibilities for energy scavenging include thermoelectricity (where nanostructured materials have greatly increased the conversion efficiency of heat to electric current) and energy from radio waves (as used by RFID tags).

For more information on energy see the NanoRoadMap report.[10]

### 2.4.2 Data management

**Data processing and storage**

Data processing and storage have to be very secure and efficient for a minimal size. Currently, processor power is still following Moore's law in terms of calculation power and memory densities. However, the limit of conventional materials is rapidly approaching and further increases in power and miniaturization will require nanotechnology advances in lithographic processes (e.g. nanoimprinting, dip pen lithography) and molecular electronics. Examples of future applications include: molecular memory, M(agnetic)RAM, Fe(rroelectric)RAM, PRAM (Phase Change Bridge Memory (PRAM) is a 60nm² cell size memory developed by IBM/Qimonda/Macronix PCRAM).[11]

To ensure the security of information processing and storage, efficient information encoding is needed, and solutions are presented in quantum computing and cryptography (see chapter 4).

**Data transmission**

Two main technologies are considered for data transmission: optical communication and radio-frequency communication

Nanotechnology applications are limited for radio-frequency communication, except the possibility to build more powerful antenna with carbon nanotubes.

Transmission data systems use optical communication most of the time. Berkeley's Smart Dust uses passive transmission through a corner-cube retroreflector, that only

[9] http://www.sony.net/SonyInfo/News/Press/200502/05-006E/index.html

[10] http://www.nanoroadmap.it/

[11] http://cnfrs.get-telecom.fr/pages/pages_evenements/journees_scient/docs_journees_2007/6.1%20-%20SENN_JS07.pdf

consumes on the order of 1nJ/bit (the device itself only consumes 670pJ/bit) or active transmission using a laser diode and steerable mirrors.[12]

For optical data communication the following are considered: nano optoelectronics, diffractive optical elements, optoelectronic transducers and photonic components. Nanostructured optoelectronic components include quantum wells, quantum dot lasers as well as photonic crystals. Already, two-dimensional photonic crystals can be routinely manufactured with high precision. At present, efforts are being intensified to develop three dimensional photonic crystals, which would open up new possibilities in optical data communication (light could be guided and branched in defined directions) and offer, in principle, the potential of purely optical circuits (optical computing).

Infrared sensors are an alternative approach for optical data communication. The miniaturization and further improvement of infrared sensors are based on, among other things, the application of two (quantum well), one (quantum wire) or zero-dimensional (quantum dot) nanostructures. With the help of quantum well or quantum dot structures the detection characteristics of infrared sensors can be adjusted selectively to the relevant spectral region (band gap engineering).

## 2.5 Conclusions

The topicality of civil security stimulates the support of technological advances by authorities as well as companies which see interesting market opportunities. Indeed, new detection devices are not only developed to replace or enhance currents ones, but to embed systems in public places in order to limit accidents as well as terrorist attacks. This requires cheaper devices that are easy to use, and able to detect a variety of agents quickly and with a high degree of accuracy.

To achieve this requires nanotechnology advances. Nanotechnologies have applications in several imaging devices (X-ray, infrared, THz detection), but it is in the range of biological and chemical detection that they are the most advanced. Biotechnology advances using nanoparticles and quantum dots as bio-detectors, have allowed rapid progress in security applications. Rapid progress has also been made in the field of chemical detection based on carbon nanotubes. Finally, nanotechnology offers the possibility of multiplexing, or performing analyses on a number of different targets on the same sensor in an array form. This application may be more of a mid- to long-term prospect, but will highly facilitate detection and accelerate results.

The most impressive advance allowed for by nanotechnology development is the possibility of autonomous sensor networks. These networks will be able to not only capture data but process information, transmit it, and communicate with others sensors in potentially hostile environments. The extremely small size of these devices, in addition to a very low price, could make them next generation of sensor for civil security. Indeed they have the potential to limit the requirement for human intervention in dangerous places.

[12] http://www-bsac.eecs.berkeley.edu/archive/users/warneke-brett/pubs/cbnp_workshop-summary.html

## 2.6 References


Dosev et al., 2007. "Magnetic/Luminescent core/shell particles synthesized by spray pyrolysis and their application in immunoassays with international standard" Nanotechnology **18** n°5

Federici et al. 2005. "THz imaging and sensing for security applications – explosives, weapons and drugs" Semiconductor Science and Technology **20** S266-S280

Hahm and Lieber, 2004. "Direct Ultrasensitive Electrical Detection of DNA and DNA Sequence Variations Using Nanowire Nanosensor" Nano Letters **4** pp. 51-54

Jiand et al., 2004. "High detectivity InGaAs/InGaP quantum dot infrared photodetectors grown by low pressure metalorganic chemical vapour deposition" Applied Physics Letters **84** pp. 2166-2168

Kleinschmidt et al., 2007. "A Highly Sensitive Detector for Radiation in the Terahertz region" IEEE transaction on instrumentation and measurement **56** n°2

Lan et al., 2006. "Simulation of Carbon Nanotube THz Antenna Array" International Journal of Infrared Millimetre waves, **27** N°6 pp. 871-877

Létant and Wang, 2006. "Semiconductor Quantum Dots Scintillation Under γ–Ray Irradiation" Nano Letters **6** N°12 2877-2880

Medinz et al., 2005. Nature Materials, **4** pp. 435-446

Minsheng et al., 2004. "Ge quantum dot infrared photo-detector" The Fourth International Workshop on Junction Technology (IWJT '04). IEEE

Mirkin et al., 2004. "Bio Barcodes Based DNA Detection with PCR like Sensitivity" Journal of American chemical Society **126** pp. 5932-5933

Nie et al, 2001. "Quantum-dot tagged microbeads for multiplexed optical coding of biomolecules" Nature Biotechnology, **19** pp. 631-635

Nie et al., 2002. "Self-Assembled Nanoparticle Probe for Recognition and Detection of Biomolecules" Journal of American Chemical Society **124** pp. 9606-9612

Pavlovsky et al., 2006. "Palladium Nanoparticle Hydrogen Sensor" Gases and Technology, July/August pp. 18-21

Poizot et al., 2000. "Nano-sized transistion-metal oxides as negative-electrode materials for lithium-ion batteries" Nature **407** pp. 496-499

Rosi and Mirkin, 2005. "Nanostructures in biodiagnostic" Chemical Review **105** pp. 1547-1562

Schulten et al., 2005. "Ion-Nanotube Terahertz Oscillator" Physical Review Letter **95**

Shanmukh et al., 2006. "Raman spectroscopy - SERS and silver nanorods quickly reveal viral structures" NanoLetters **6** p.2630

Snow et al., 2005. "Chemical detection with a single-walled carbon nanotube capacitor" Science **307** pp. 1942-1945

Su et al., 2006. "Terahertz detection with tunnelling quantum dot intersublevel photodetector" Applied Physics Letters **89**

Tan et al., 2003. "Ultrasensitive DNA Detection Using Highly Fluorescent Bioconjucated Nanoparticles" Journal of American Chemical Society **125** pp. 11474-11475

Tarasov, 2006. "Carbon nanotube based bolometer" JEPT letters **84** pp. 267-270

Wang et al., 2004. "Receiving and Transmitting light-like radio waves: antenna effects of aligned carbon nanotubes" Applied Physics Letter **85** n°13

Wang et al., 2007. "Direct-current nanogenerator driven by ultrasonic waves" Science **316** pp. 102-105

Watanabe et al., 2003. "Non-destructive terahertz imaging of illicit drugs using spectral fingerprints" Optics Express 2549 **11** n°20 p.2549

Wu, 2005. "CNTs used to produce multi-beam scanning field emission X-ray source" MRS bulletin **30**

# 3 Protection

## 3.1 Introduction - Nanoscience opportunities for protection

The physical protection of critical infrastructures, rapid response and rescue teams, and civilians against various forms of terrorism and organized crime is one of the most important tasks for future civil security in Europe. The main research and application topics for improved protection solutions are developing in relation to risks from the proliferation of chemical and biological warfare agents or dangerous goods and from the need for better protective systems against explosives, projectiles, and fire, especially in personal equipment for rescue forces. In addition to such intentional dangers, the growing potential risk of natural and man-made disasters or industrial accidents in an ever-increasing interconnected world, also requires new and robust protection solutions to minimize the raised vulnerability of vital infrastructures and supply chains on a local and transnational level.

Against this background and the specific security demands, the interdisciplinary field of nanotechnology plays an important role for the development of new passive and active protective applications. Nanotechnology offers novel materials with enhanced or new physical properties and functionalities including higher strength, durability, embedded sensory capabilities and active materials. In terms of protection, civil security applications will mainly benefit from the following material functionalities:

- **lightweight:** high strength nanocomposites are expected to replace metal or other hard materials, and thus reduce weight and enable improved construction designs in buildings, garments, bridges, and other protective applications;
- **smart components:** components with integrated sensory and reactive elements, smart materials for diffusion control and active mass transport, smart nanoparticles that recognize and sequester, incorporate or destroy specific toxins. In the long term- self-repairing or self-healing materials;
- **adaptive structures:** active structures that adapt to changing conditions such as adaptive suspension, flexible/rigid, etc.,
- **Electromagnetic Interference (EMI) shielding:** electromagnetic radiation absorption coatings or materials (Electromagnetic Pulses (EMP), microwave, gamma-ray, UV);
- **mechanical strength and robustness:** nanoparticle and nanofibre reinforced antiballistic structures; flexible antiballistic textiles; reactive nanoparticle armour; shock absorbing nanotubes; nanofibres, garments and nanocoatings for biological or chemical decontamination; switchable fabrics or materials for improved thermal control and fire protection.

Similar to other nanoscience application fields, the key indicators for the commercial realisation and integration of nanostructured protective materials in future smart and resistant security systems are considered to be manufacturing issues and approaches in directed self-assembly in multiple dimensions. Due to its position as a possible entry door market for nanomaterials, the development of improved protective components for civil security applications is on the one hand accelerated by the provision of a wide range of new material properties through nanoscale engineering, and on the other benefiting from basic defence research and technologies developed for protecting military personnel, especially in the USA.

## 3.2 Decontamination and Filter Applications

The use and development of decontamination and filter technologies for the protection of critical infrastructures and technical equipment are closely linked to the protection of people and natural resources. In the light of diverse, asymmetric threats arising from terrorism and organized crime, as well as from major industrial accidents, new challenges are emerging in civil security; particularly regarding the filtering and elimination of released chemical and biological toxins. These challenges are relevant when developing decontaminating coatings, active cleaning and decontamination agents, and catalytic filter systems. As can be seen by the increasing use of self-cleaning nanosurfaces and increasingly frequent integration of catalytically active nanoparticles in tailored, multifunctional coating systems; chemical nanotechnology is the main source of important innovation and a major provider of technical principles that can contribute to the further development of improved decontamination technologies with improved long-term stability and a wider range of uses. Other important focal points with regard to nanomaterials that are relevant to security applications are: photocatalytic systems (for example, using titanium dioxide or zinc oxide); quick burning or oxidizing/biocidal nanoparticles; and super-absorbent or super-hydrophobic nanocomposites/hydrogels.

Both the progress that has been made in membrane technology as a result of the use of nanoporous materials and the integration of biocatalysts and enzyme catalysts at molecular level are further important technological prerequisites for enabling the development of more effective chemical and biological filters, especially for air purification and the provision of drinking water in critical infrastructures. In the face of the potential dangers of bioterrorist attacks, the protection of public supply structures and the design of future purification, filtering, and treatment procedures in, for example, sewage works and water works or in food production is made more difficult both as a result of a large target spectrum of harmful substances that can be used, as well as significantly shorter reaction periods for the implementation of immediate protection and defence mechanisms. For this reason, the development of highly effective nanocatalytic materials and nanomaterials as well as tailored nanomembrane systems is an important innovation factor for the future development of effective filtering and decontamination factors in civil defence.

A prominent example of a decontamination technology based on nanoparticles, which has been developed to the point of being ready for production, is the highly effective metallic oxide decontamination system that has been developed by a task force led by Professor K.J. Klabunde at Kansas State University. By using ultra-fine magnesium oxide powder, these researchers have managed to destroy airborne bacterial spores such as anthrax, even at room temperature. Nanoscale Materials Inc. is now distributing a chemical hazard response system[13] which uses a mixture of magnesium oxide and photocatalytically active titanium dioxide nanoparticles. This system is capable of effectively and quickly neutralizing even chemical toxins such as VX nerve gas. Tests on different surfaces at the Battelle Memorial Institute in Columbus have shown that the FAST-ACT system catalytically neutralizes 99.9% of VX toxins in 10 minutes.

Another example of an application meeting the requirements for a future decontamination technology is a self-cleaning catalytic polymer filter system that was first presented in 2004. It was developed in the US at the Naval Research Laboratory (NRL) using a multifunctional nanocoating and is intended for use in the decontamination of respiratory air and for the purification of drinking water. The intelligent combination of chemical and biological catalysts has enabled the researchers to produce filter prototypes which are suitable for the active neutralization of various chemical toxins such as pesticides or nerve gas. The direct coupling of active biological and chemical catalysts in a single system was achieved by means of spraying an adsorption layer of charged

[13] www.fast-act.com

nanoparticles onto the respective substrate layers during the progressive development of the reactive filter system. It was then possible to obtain a filter-sandwich structure with chemical catalyst complexes and catalytically active enzymes on top of this 'anchor layer'. The filter-sandwich structure can be adjusted in line with various filter substances and security requirements in air and drinking water purification procedures. Tests on the catalyst system with accordingly coated polyethylene filter beads have shown that pesticides in drinking water can be reduced by 99% in less than 2 minutes at a continuous flow rate. The filter performance during the tests was sustained for a period of 60 days (see Figure 3.1).

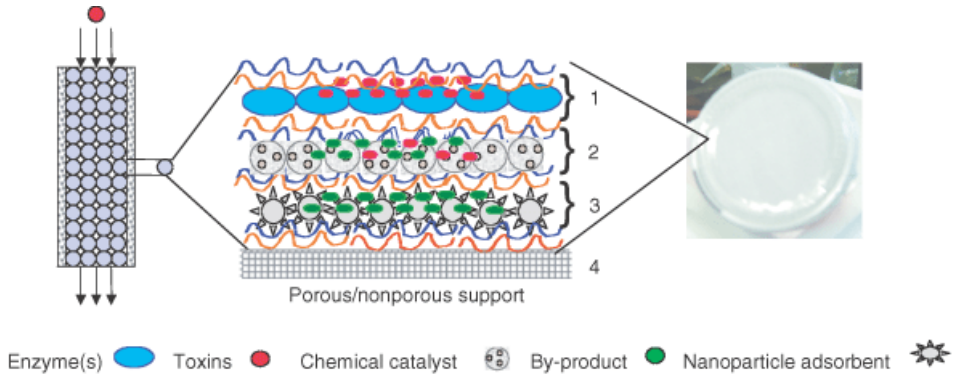



**Figure 3.1** Self-cleaning filter system using chemical and enzyme catalysis (source: Naval Research Laboratory)

Also in the US, the Argonne National Laboratory has developed a security system using a super-absorbent gel which enables radioactive residue to be neutralized and removed from porous surfaces of buildings or monuments in the event of, for example, a nuclear attack using a 'dirty bomb'. If such an event were to occur, civil security forces would apply the super-absorbent polymer gel to the contaminated surfaces in the form of an aqueous suspension using a spraying device. The foam acts by penetrating the porous surface and trapping the radioactive particles within the polymer structure, where they bind to tailored nanoparticles that are contained in the gel. The contaminated gel can then be removed and recycled using a vacuum device so that only a small percentage of the decontamination material has to be disposed of as radioactive waste. Efficacy trials with various radioactive elements on building facades of cement and brick have shown that the use of super-absorbent polymer gel can remove over 98% of radioactive elements from cement components and over 80% of radioactive elements from the entire building surface.

An example of the relevance of nanotechnology applications for civil security is a titanium dioxide-based semiconductor photocatalyst developed by Erlangen-Nürnberg University. It is able to use a larger proportion of sunlight in order to achieve a higher level of self-cleaning in coatings than previous photocatalysts. Normally, titanium dioxide particles can only use UV light, which only makes up around 2 – 3% of sunlight and accounts for even less of artificial light in internal spaces. In order to sensitize titanium dioxide to the far greater visible light spectrum, Professor Kisch's team doped the photocatalytic material with elements such as carbon. They achieved an optimum catalytic effect with 2 – 3% carbon doping of the titanium dioxide crystal lattice. Moreover, the method developed by the researchers for the production of the carbon-doped titanium oxide is simpler, more easily reproduced, and has scope for wider use than the traditional titanium dioxide production technique, which involves the oxidation of titanium sheet metal in a natural gas flame. The different property profile achieved by the doping method in comparison with traditional titanium dioxide photocatalysts should enable the production of new photocatalysts with a higher degradation potential for chemical toxins in the medium term. Materials coated with the doped photocatalysts were able to

degrade solute toxic substances such as chlorophenol and azo-dyes as well as harmful gases such as acetaldehyde, benzene, and carbon monoxide even in diffuse daylight in internal spaces.

Another interesting research approach in connection with the photocatalytic decontamination potential of nanomaterials was recently reported by American researchers from the University of Arkansas. They have created assemblies of nanowires with photocatalytic activity that show potential in applications such as bacteria filters or for the decomposition of pollutants and chemical warfare agents. Using a hydrothermal heating process, the group created long nanowires out of titanium dioxide that can be assembled into free-standing membranes. The result looks like a conventional flat piece of paper, but has the flexibility of polymer foils since it is reinforced with fibres. The "nanopaper" is cheap, environmentally friendly and can easily be shaped into three-dimensional devices (see Figure 3.2). Because of its composition, the nanowire paper is chemically inert, remains robust and can be heated up to 700°C. The robustness makes it possible to sterilise the paper with a torch flame or ultraviolet light, which also make it ideal as a reusable filter membrane in gas masks. According to the researchers, it is possible to adjust the pore size of the paper during the casting process so that the holes are big enough to let oxygen in but small enough to block toxins, for example. The university has applied for patent protection on the process used to create the free-standing membranes for filtration and catalysis, and is now looking for industrial partners to license it and commercialize various applications.

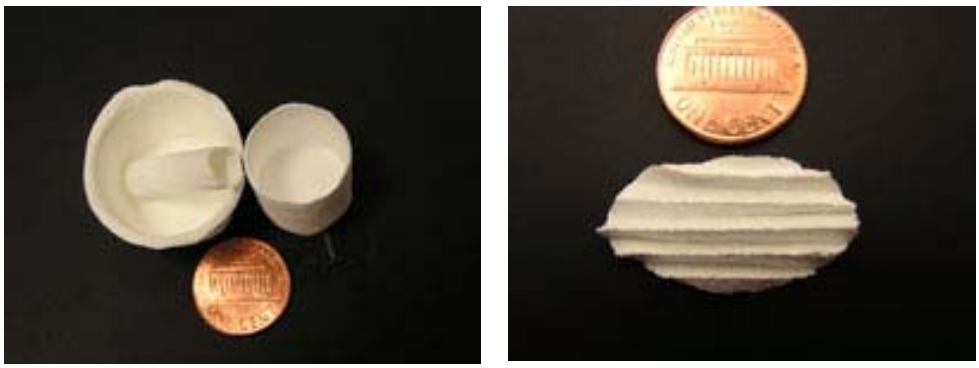


**Figure 3.2** Photocatalytic "nanopaper"-devices created with nanowires out of titanium dioxide (source: University of Arkansas)

Research-based evidence of the significance of nanomaterial systems in the field of modern membrane technologies comes in the form of a research project carried out at the Technical University of Braunschweig's *Institut für Werkstoffe* (Institute of Materials) in Germany. The project deals with the development and production of nanoporous membranes on extremely temperature stable nickel-based superalloys. The production of nanoporous metallic membranes takes place using a new procedure that involves the thermo-mechanical pretreatment of the basic material and selective phase extraction in order to create an extremely regular, homogenous structure of pores of between 300 and 500 nm diameter (see Figure 3.3). Depending on the alloy chosen and additional procedural factors, the parameters of the resulting nanoporous structure can be set within a wide range in a targeted manner. The porosity of the nanomembrane is between 30 and 70 percent by volume. In addition to the structural integrity, the pore size, and the regular nature of the pores; metallic membranes produced in this way have characteristic features such as thermal and electrical conductivity and weldability, in contrast to porous nanoceramic materials. In addition, the membranes are relatively less susceptible to ripping and breaking and are pliable. These properties give rise to a range of possible applications for nanoporous superalloys in civil security products such as the filtering of minute particles (such as bacterial spores and dust) from respiratory air or in

gas separation. If required, thermal sterilization or cleaning of the structure is possible. However, further research and development hurdles need to be overcome in order to enable the cost-effective production of large-area nanoporous membranes of high, reproducible quality before these membranes can be used extensively.

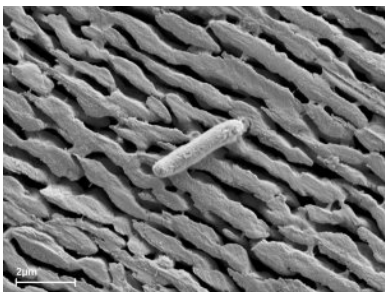


**Figure 3.3** Nickel-based superalloy nanomembrane with E. coli bacterium (source: TU Braunschweig)

At the Pacific Northwest National Laboratory (PNNL) in the US, chemically modified nanoceramics with a mesoporous sponge structure have been developed on the basis of SAMMS technology (Self-Assembled Monolayers on Mesoporous Supports, see Figure 3.4). They can remove hazardous substances from water significantly faster than conventional filter technologies such as active carbon filters. The nanosponge is produced using mesoporous silicon dioxide ceramics with pore sizes averaging 6 nm, depending on the hazardous substance targeted. The pores are filled with a self-assembling capture layer. Mercury, for example, is removed using modified mercaptan molecules, whereas chelating ligands are used to neutralize anionic heavy metal compounds such as chromate. Tests with mercaptan SAMMS showed that with three treatments, 99.9% of the mercury in contaminated waste water could be removed within 5 minutes. This technology is also suitable for removing radionuclides and works in non-fluid media. The PNNL researchers are working towards the integration of the filter system in membrane and fibrous materials and on marketing the system for purely security-related technical applications.

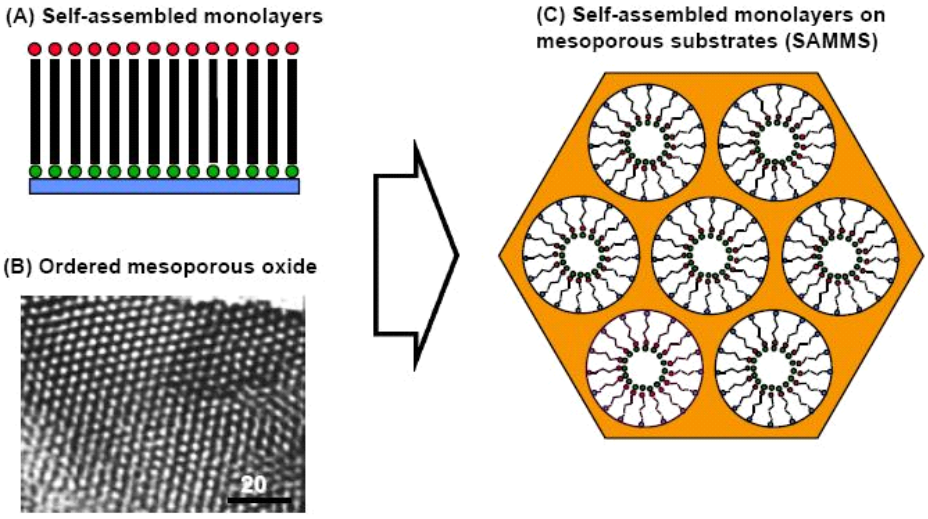



**Figure 3.4** SAMMS filter technology (source: Pacific Northwest National Laboratory)

## 3.3 Personal Protective Equipment Applications

The development of textile/personal protective systems for providing better protection against hazardous CBRNE (Chemical Biological Radiological Nuclear Explosive) substances, explosions, and projectiles for the police and rescue workers gives rise to numerous material-related technical challenges, and not just in the light of the attacks of September 11$^{th}$ 2001. In addition to the development of technical textiles with microbiocidal, antiviral, or sporicidal properties, attention is also being turned towards the improvement and reduction in weight of ballistic protective systems (such as bullet-proof vests), and fire-resistant clothing. The main aim is to enhance passive materials with active systems that integrate monitoring and protective systems with textiles and automatically trigger countermeasures based on the combined sensor and actuator properties of the material systems used (for example, by forming temperature-resistant or bullet-proof layers or by triggering medical measures such as closing wounds). The vital development of robust, light, and intelligent nanomaterials for this purpose is being discussed and promoted in relation to perceptions of the 'soldier of tomorrow'. The long-term aim of the concepts in relation to the security requirements of civil rescue workers and relief units is the standard integration of nanomaterials in both passive and active protective structures as part of personal biological feedback and monitoring systems. This includes functions such as the monitoring of the vital functions of the wearer, the investigation of the surrounding area in the case of warfare agents or radiation, and enabling trapped or injured personnel to be located.

The implementation of passive protective textiles and active personal protective systems is heavily influenced by new innovative materials and procedures for the manufacturing of nanofibres, nanotextiles, and biocidal nanocoatings, and the development and functionalization of switchable/controllable nanoparticles. The anticipated security-related development steps include the use of high-tensile, impact resistant carbon nanotube (CNT) fibres in bullet-proof vests, polymer nanocomposites (based, for example, on shape-memory plastics) and magnetorheological (or shear-thickening) nanofluids, or the integration of piezoelectric ceramic fibres into textile sensor and/or actuator systems. Other relevant developments for these application fields include drug delivery systems based on lipid nanoparticles, dendrimers, fullerenes, or inorganic nanoparticles and in the development of chemical and temperature resistant clothing with self-healing properties.

As is the case for other industrial sectors, the modification and integration of established nanomaterial and coating solutions also constitutes an important synergy factor for the development of technical security applications. Significant technology developments include super-hard nanocoatings (based, for example, on boron nitride or diamond), polymer nanocomposites (in fire-resistant components), carbon-based nanomaterials (for aerogels with cushioning properties), and nanocrystalline alloys or powders with targeted functional properties. Depending on the role of the personnel in question or on the degree of protection required for critical infrastructures (for example, if the intended use relates to explosions or natural disasters), heightened physical or static functional requirements may need to be taken into account, and materials modified accordingly, before integrating into security applications. As well as giving rise to the development of new, passive protective systems targeted at the requirements of civil security, this also opens up the possibility of providing established security products such as safety glass, plating, and fire protection material with self-healing properties or other additional security functions. The innate security properties of existing passive protection systems can be gradually improved through the replacement of traditional materials/building materials such as steel or glass with increasingly common, lightweight nanomaterials such as metal foams.

An important example of the development of passive protective textiles with a specific security-related focus is the development of a super-thin, self-decontaminating coating material at the Naval Research Laboratory's Center (NRL) for Bio/Molecular Science and Engineering in Washington (see Figure 3.5). This material actively neutralizes pesticides

and similar chemical substances. The coating consists of a multi-layer, 500 nm composite coating with incorporated immobilized enzymes in polycationic/polyanionic polymer layers. The reactive layers benefit from high stability and can destroy hazardous chemicals for long periods of time. Pesticide tests using natural and synthetic textile fibres coated with the NRL catalytic enzyme system demonstrate its high neutralization capability and robustness in comparison with traditional chemical decontamination systems. Substantial R&D efforts are currently striving towards an additional increase in the stability of the system and the realization of suitable industrial procedures for the coating of various fibre materials and the consequent mass production of protective clothing.

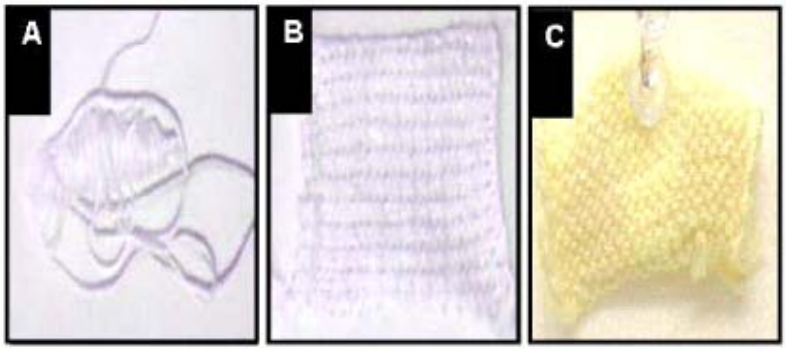



**Figure 3.5** From left to right: A cotton thread coated with the NRL enzyme catalytic system (A) and woven into a piece of textile fabric (B). Following contact with a pesticide solution, the textile takes on a yellowish colour (C) that is characteristic of the completed neutralization process (source: Naval Research Laboratory)

At the Nanotech Institute of the University of Texas in Dallas, researchers have developed a method for creating a multi-layer, tear-proof yarn from multi-walled carbon nanotubes. The yarn has a tensile strength of more than 460 MPa and has cushioning properties that approach those of materials used for bullet-proof vests, such as Kevlar. The nanotubes, which are grown individually on a substrate in a 'nanotube forest', are mechanically extracted and twisted into yarn at the same time (see Figure 3.6). Unlike normal fibres and yarns, the strength of these nanotube yarns is not decreased by knotting, and their flexibility and strength is retained even after heating them to 450°C for an hour or immersing them in liquid nitrogen. The mechanical properties of the nanotube fibres can be further improved by combining them with polymer fibres — without impeding electrical conductivity. The main focus of further development efforts is on the production of longer yarn lengths for industrial production. To date, yarn lengths have reached 50 m with a diameter of 2 µm at a production speed of 80,000 turns per minute. In comparison, conventional textile fibres with a diameter 80 times larger have a production speed of 1,000 turns per minute.

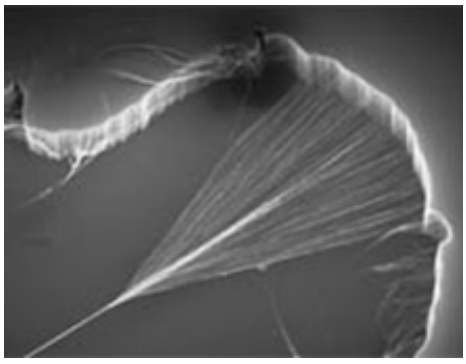


**Figure 3.6** Dry spinning of a carbon nanotube yarn from the edge of a multi wall carbon nanotube forest (source: Baughman/University of Texas)

The University of Hawaii and the Rensselaer Polytechnic Institute in the US have collaborated to develop a technology that is based on a CVD (Chemical Vapour Deposition) procedure and enables the production of approximately 1 mm thin cushioning layers made of thousands of upright, multi-walled carbon nanotubes (MWCNT). The tubes, which are around 20 nm thick, take up around 13% of the space between the flat surfaces and are produced from a high-temperature carbon environment. During pressure tests at 15 MPa, researchers proved that the nanotubes in the cushioning layer form a reversible zigzag pattern without being destroyed (see Figure 3.7). Only after several thousand pressure tests are they no longer able to regain their original dimensions. They then return to a length that is reduced by around 7.5%. The cushioning material therefore benefits from far higher compressibility and pressure resistance than foams made from polymer materials such as latex or polyurethane. In addition, the cushioning layer has a resistance to chemicals and other external influences that is equal to that of metal foam. This unique combination of properties should enable the future development of extremely lightweight and stable layers that can be used in security applications such as earthquake-proof and explosion-proof building construction as well as for the protection of sensitive electronics. However, at present these materials only exist in the form of laboratory prototypes, but the production of larger surfaces is conceivable.

**Figure 3.7** Folded MWCNT cushioning element produced at 15 MPa (source: Cao/Rensselaer Polytechnic Institute)

At the Weizmann Institute of Science in Israel, a promising material alternative to the use of carbon nanotubes in passive protective systems has been developed in the form of a new inorganic fullerene-like nanoparticles based on sulphides of tungsten ($WS_2$), molybdenum ($MoS_2$), titanium ($TiS_2$) and niobium ($NbS_2$), see Figure 3.8. Thanks to their closed-cage structure, they have high mechanical stability and shock resistance. In comparison with organic fullerenes, these nanomaterials are easier and more cost-effective to produce, and have higher chemical stability. Studies have shown that material samples based on $WS_2$ can withstand shockwaves of 300t/cm$^2$, meaning that they are twice as stable as the next most stable materials to date – silicon carbide (SiC)and boron carbide (BC) – and are five times more shock-resistant than steel. These fullerene particles can be combined with polymers, metals, or alloys to produce super-hard or elastic coatings with high wear resistance and shock resistance, making them particularly suited for use in armour and security coatings for protection against explosives or firearms. The inorganic fullerenes have already been marketed as a nanopowder under the name NanoLub$^{TM}$ by the Israeli company ApNano and are currently mainly used as an anti-friction agent for lubricants.

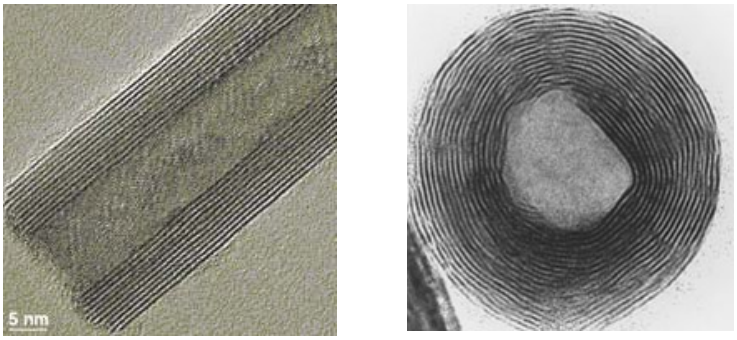



**Figure 3.8** Cross section and longitudinal section of an inorganic fullerene-line nanoparticle with an onionskin structural pattern (source: ApNano Materials and Tenne/Weizman Institute of Science)

One of the most promising research directions for the development of active personal protective systems is the "Liquid Armour" concept based on shear thickening fluids (STF) or magnetorheological fluids. Liquid armour technology using shear thickening fluid is being developed at the US Army Research Laboratory. The STF of this new protective system is made up of hard silica nanoparticles suspended in polyethylene glycol, a non-toxic fluid which can withstand a wide range of temperatures. To make liquid armour, the STF is soaked into every layer of a standard Kevlar vest. The saturated fabric can be soaked, draped, and sewn just like any other fabric. During normal handling, the STF in the vest is very deformable and flows like a liquid. However, once a bullet or other splinters or projectiles hits the vest, it transforms into a rigid material, which prevents the projectile from penetrating the body.

At the Massachusetts Institute of Technology (MIT), the Institute for Soldier Nanotechnologies has been working on a form of liquid armour that uses magnetorheological fluids to produce new protective uniforms or armour vests for the US Army. The nanofluids consist of iron nanoparticles suspended in a thick oil or syrup. When a magnetic field is applied, the iron nanoparticles align and the fluid becomes extremely stiff (see Figure 3.9). The degree of stiffness varies depending on the strength of the applied field. The change happens extremely quickly — in about 20 milliseconds — and the research team hopes that eventually, the fabric-fluid combination could resist even a shockwave or shrapnel. The researchers at the MIT emphasize that their so-called "instant armour" system needs another five to ten years of research before this material is truly bullet-resistant and can be applied in personal protective systems for soldiers or rescue forces and in other civil security systems.

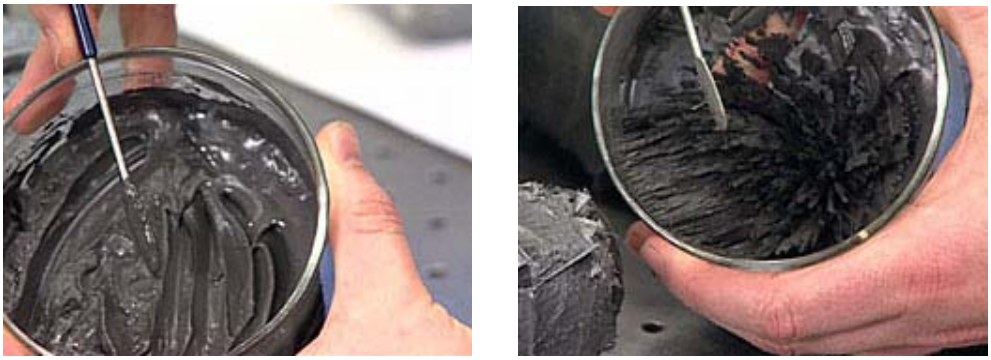


**Figure 3.9** Oily fluid full of tiny iron particles before being near a magnet (left); and after (right) (source: Massachusetts Institute of Technology (MIT), Institute for Soldier Nanotechnologies)

In addition to physical inviolability, another important factor in the development of personal protective equipment for rapid response teams will be the possibility of automatically triggering medical treatments. As well as the development of wound-closing nanofibre systems, promising nanotechnology developments in drug delivery systems could provide means for automatic administration of medicine in response to injury or exposure to biological or chemical agents.

A new medical technology to clean the blood of victims of radiological, chemical and biological terrorist attacks is being developed jointly by Argonne National Laboratory and The University of Chicago Hospitals. In addition to cleaning biological and radiological toxins from blood, the technology shows promise for delivering therapeutic drugs to targeted cells and organs. This technology uses a novel approach to magnetic filtration. The key is biodegradable poly(D,L-lactide) nanospheres 100 to 5,000 nm in diameter, which are injected into the patient's bloodstream and are small enough to pass through the smallest blood vessels, yet too large to be filtered from the bloodstream into the kidneys (see Figure 3.10). The nanoparticles contain a magnetic iron compound (40 weight percent magnetite) and are coated with a derivative of polyethylene glycol that prevents white blood cells from attacking them. Attached to the particles' surfaces are proteins that bind to specific toxic agents. The system offers a number of advantages over existing methods to clean human blood of radioactive and other hazardous materials. Current medical procedures to detoxify human blood are restricted to a few types of toxins and can take several hours to complete. They require the turnover and filtration of large volumes of blood, are rather inefficient at removing toxins and can be risky for the patient.

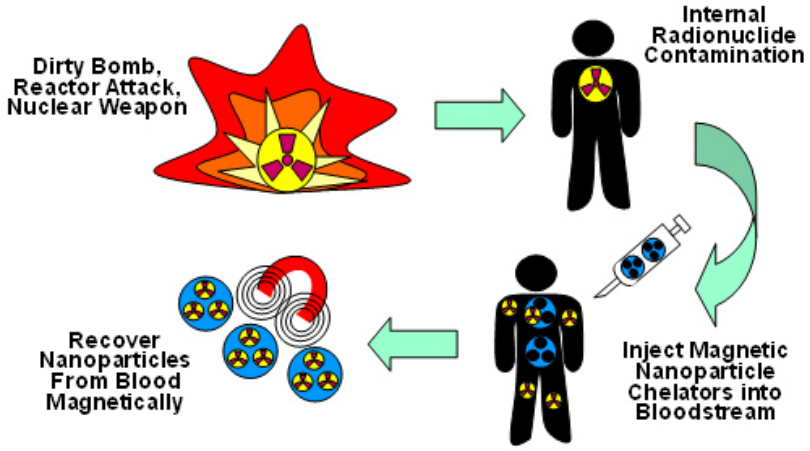



**Figure 3.10** Intravenously injected into victims of radiological, chemical or biological attack, biodegradable nanospheres circulate through the bloodstream, where surface proteins bind to the targeted toxins. They are removed from the bloodstream by a small dual-channel shunt, inserted into an arm or leg artery, that circulates the blood through an external magnetic separator. Strong magnets in the shunt immobilize the iron-based particles, and clean blood flows back into the bloodstream. (Image courtesy of the Armed Forces Radiobiology Research Institute)

## 3.4 Electromagnetic Shielding

The future protection of wireless information and communication networks against data manipulation or transmission will depend on the implementation of improved electromagnetic shielding measures (against electromagnetic fields or pulses). More than anything, the possibility of deliberately generated electromagnetic pulses (EMPs) as a

result of a thermonuclear explosion or an E-bomb presents a real threat to the security of critical information infrastructures. Research efforts in the shielding of electronic components concentrate on the realization of passive material systems for the neutralization of electromagnetic radiation.

Nanostructured materials for electrostatic shielding and absorbing microwaves are being investigated as part of the development of antireflection and optical interference coatings in both the visible and ultraviolet spectra. Among other things, important efforts are being made towards the development of innovative radar stealth coatings. The most significant procedures for the realization of antistatic or absorbent coatings are based on carbon nanotube polymer composites, nanocomposites made from transitional metal mixed oxides in a polymer matrix, and cenospheres (hollow porous ceramic spheres coated in a metallic nanoscale coating). The development of targeted dynamic shielding technologies is also being discussed. Such technologies involve the selective generation of electromagnetic absorption bands using the combination of mutually interacting nanoparticles in an absorption coating. These bands can then be modulated and controlled externally.

One example of the numerous international research projects dealing exclusively with the modification of carbon nanotube-based materials for use in security applications is the thin polymer layer system developed at the Korea University in Seoul. This system is suitable for being used as an EMI (Electromagnetic Interference) shielding system for electronic components, among other things. In relation to the development of flexible nanocomposites coating, tests have been carried out using different proportions (between 0.1 and 40 percent by weight) of multi-walled carbon nanotubes in the polymethylmethacrylate (PMMA) matrix. Researchers used SEM (scanning electron microscope) micrographs and conductivity tests to demonstrate the formation of a conductive nanotube network in the polymer matrix. An increase in DC conductivity was observed as the nanotube percent by weight increased. Concurrent measurements of electromagnetic shielding efficiency showed that the SE (Shielding Efficiency) value for a 40% nanutube content gives a maximum value of 27 dB, giving rise to possible applications in the far field range (above 10 MHz). Because of the moderate conductivity of the nanocomposite, the absorption portion of the total SE value is larger than the reflection portion, giving rise to extremely promising application possibilities for shield coating in the microwave/radiowave frequency range for military purposes and for telecommunications. The main intended initial areas of use for this flexible, cost-effective, and mass production-capable shielding material are mobile electrical devices and equipment.

## 3.5 Conclusions

There is a wide range of research, application and security related product examples that prove the important enabling role of nanotechnology for the development of future personal protection and decontamination technologies. In view of new threats and the growing demand for improved civil security technologies, it can be anticipated that the ongoing progress in the development of security filter applications and the implementation of robust and multi-usable decontamination technologies in particular will be dominated in the mid-term by the controlled design and use of nanostructured materials and coatings. Nanoscience and nanostructures will enable revolutionary advances in adsorbent materials, separation technologies, neutralization/decontamination of agents, and prophylactic measures. The main research targets in this field are related to the:

- development of smart nanoparticles or tuneable photocatalysts that recognize and sequester or destroy specific toxins;
- smart and designed nanostructured membranes with controlled porosity for selective migration and separation;

- high surface area materials with templated structure and nanofibres or nanotubes with improved and selective adsorption/neutralization of agents and radioactive materials;
- "prophylactic" nanostructured solutions, which include e.g. drug delivery platforms, nanostructured reactors in skin creams or nanostructured materials for wound cleaning and treatment.

In addition to the requirements for improved decontamination and filter applications in civil security, there is also an urgent need for personal protective equipment applications, through which especially rapid response and rescue teams are better prepared and protected in case of terrorist attacks or catastrophic emergencies in connection with explosives, harmful chemicals, biological agents or radioactive materials. In this context new nanocomposites, nanoscale molecules and compounds, and polymers for tougher, explosion- or puncture-resistant materials are needed that combine low weight and impact resistance with low production costs. Applications of these materials might also include containers for luggage/cargo being transported in airplanes or other vehicles, barriers within high-security buildings, barriers to protect VIPs at high profile events, and stronger building materials and technical textiles that can be employed in buildings, bridges or in other civil security infrastructures. In addition to these physical protection applications, the use of magnetic nanoparticles and nanostructured materials is a core element in the development of electromagnetic shielding coatings for future security related electronic and communication devices, and an important factor in the ongoing development of active protective equipment with integrated medical and monitoring functions.

There are two major research lines for the development of future passive and active personal protective systems. In the near-term, the application of nanomaterials will have a strong impact mainly in the enhancement of standard and established passive textile protection products. Within a timeframe of 5-10 years, the further dispersion and use of nanomaterials and nanocoatings with enhanced or new physical properties is expected to have a key role in the development of flexible, wearable and smart passive or active protective systems tailored for remote and embedded monitoring of rapid response and rescue personnel. Important research targets and concepts which have been pursued or are now being developed are related for example to:

- nanocomposites with tailored properties for wearable or integrated protective systems in protective clothing or equipments and in building structures;
- multifunctional nanofibres and garments for smart textiles (sensoric, biological and chemical decontaminating, high strength);
- magneto-restrictive or shear-thickening nanofluids for passive and active protective systems ("Liquid Armour");
- tailored and switchable nanocoatings for electrostatic and electromagnetic shielding of components in security related computer and communication systems;
- nanomedical applications based e.g. on biodegradable nanospheres or controllable magnetic nanoparticles in active personal protective systems.

Summing up, it is conceivable that nanotechnology developments in the long-term will play a key role in the continuous transition from clear passive to fully autonomous protective systems where decontamination, filtering and physical protection properties are combined with fully integrated sensoric, medical or other smart security-related functions.

Up to now, there are only few examples of nanotechnology products which are principally developed for the civil security market. Most of the previously described developments and application examples in the field of decontamination, filter or personal protective

applications are either completely based on defence driven demands or still at a demonstration or prototype level. Especially in the USA, but also in Europe, the market of civil security related products is mostly state-driven by inner security requirements or public expenditures, and closely connected to the market formation in the homeland security sector during the last five years. Market research specialists predict that the US homeland security market volume will increase to 115 billion US-Dollars by 2010. According to market analysis, Europe is the second largest market for civil security equipments and products with 9 billion US-Dollars in 2005. Because of the lack of homogeneity of the civil security world market, predictions about the role and market share of nanomaterials in future decontamination and filter technologies or personal protective solutions are difficult and strongly related to future trans- and international security policy targets, e.g. concerning pan-European investments for the continuous improvement of emergency preparedness and response capabilities in the civil protection and stronger physical protection standards in critical infrastructures like the transport sector.

Similar to other application fields, there is a naturally high overlap between the "classical" nanomaterial research development lines and hurdles on one side and specific civil security research targets for decontamination and personal protective systems on the other. In order to avoid redundant research and funding efforts there is an urgent need to integrate basic research efforts and results of other nanotechnology programmes and to create a systems-level approach to security research; integrating relevant projects and expertise of nanotechnology at each stage of the value chain. Further research and development strategies in the civil security sector also have to take into account that nanotechnology as an enabler for improvement in other industrial sectors also promotes generic technology developments with indirect impact on security.

Therefore, sustainable research and funding efforts in the field of nanotechnology contributions for future civil security protection solutions require a true multidisciplinary research orientation with nanomaterial scientists, informatics or electronics experts, and systems engineers working together at project level, e.g. developing and characterizing new nanomaterials with specific security-related properties, incorporating them into protective textiles or microdevices, and developing all of this into a fully integrated protective system.

## 3.6 References


Argonne National Laboratory Media Center: "Biodegradable nanospheres offer novel approach for treatment of toxin exposure and drug delivery" from October 20, 2006; http://www.anl.gov/Media_Center/News/2006/CMT061020.html

Army News Service: "Army scientists, engineers develop liquid body armor" from April 21, 2004; http://www4.army.mil/ocpa/read.php?story_id_key=5872

Chemical & Engineering News - Cover Story: "Inorganic Menagerie", 29. August 2005, Vol. 83, Nr. 35, S. 30-33; http://pubs.acs.org/cen/coverstory/83/8335inorganic.html

Civitas Group Llc.: "The Homeland Security Market", market study, 2004

Gao et al., 2005. "Super-Compressible Foam-Like Carbon Nanotube Films", Science **310** p. 1307

Kim et al., 2005. "Electrical conductivity and electromagnetic interference shielding of multiwalled carbon nanotube composites containing Fe catalyst" Applied Physics Letters **84** pp. 589-591 (or homepage of Prof. J. Joo: http://smartpolymer.korea.ac.kr/research/research.html

NanoScale Materials Inc.: FAST-ACT Technical Report (www.fast-act.com) and homepage of Prof. K.J. Klabunde; http://www.ksu.edu/chem/personnel/faculty/grad/kjk/klabunde.html

Nanotechweb.org: "Carbon nanotubes fill up with magnetic nanoparticles" from April 1, 2005; http://nanotechweb.org/articles/news/4/4/1

Naval Research Laboratory - Center for Bio/Molecular Science and Engineering: "Self Cleaning Catalytic Filters Against Pesticides and Chemical Agents"; http://www.nrl.navy.mil/content.php?P=04REVIEW121

Naval Research Laboratory Press Release: "NRL Develops Self-cleaning Smart Fabrics Capable of Environmental Toxin Remediation" from June 6, 2005; http://www.nrl.navy.mil/pressRelease.php?Y=2005&R=27-05r

Pacific Northwest National Laboratory: SAMMS Technology Summary; http://samms.pnl.gov/samms.pdf

Rösler & Mukherji, 2003 "Design of Nanoporous Superalloy Membranes for Functional Applications" Adv. Eng. Mater. **5** pp. 916-918 (or homepage of the Institute of Materials, TU Braunschweig: http://www.ifw.tu-bs.de/ifw/deutsch/forschung/neue_werk/nanoporoes/

Sakthivel & Kisch, 2003. "Daylight Photocatalysis by Carbon-Modified Titanium Dioxide" Angewandte Chemie International Edition **42** (40) pp. 4908-4911

Science Central News: "Instant Armor" from April 12, 2003; http://www.sciencentral.com/articles/view.php3?language=english&type=&article_id=218392121

University of Arkansas Daily Headlines: "Nanowire-Paper Offers Strength, Flexibility" from August 22, 2006; http://dailyheadlines.uark.edu/9049.htm

Zhang et al., 2004. "Multifunctional Carbon Nanotube Yarns by Downsizing an Ancient Technology" Science **306** pp. 1358-1361

# 4 Identification

## 4.1 Introduction

The section gives a brief overview of the various nanotechnology developments that are focused on identification of goods, products, and devices and verification of personal identity. The first part provides an overview of the various authentication and anti-counterfeiting solutions being pursued for brand protection such as nanobarcodes and nanoparticles. This is followed by an overview of the tools and techniques used in forensics for detecting fingerprints and forgeries and confirming the identity of objects. The third part provides an overview of the potential of quantum cryptography in secure information transfer. While some of these technologies are under field trial, others are not likely to be implemented for many years. In the final part, the market size of counterfeit and grey products has been presented to emphasize the seriousness of the problem.

## 4.2 Anti counterfeiting and authentication

Laser surface authentication (LSA)$^{TM}$ is a technique that uses a laser to examine and store a "map" of the microscopic roughness on the surface of objects, through the diffused scattering of a focused laser (a phenomenon called laser speckles; Cowburn & Buchanan, 2005). The identity "code" obtained from this process is similar to biometric codes obtained from iris scans and fingerprinting. This code is stored in a database that can be accessed at a later stage to determine the authenticity of a given product. The probability of any two codes from different objects matching has been shown to be $10^{-72}$ for paper and $10^{-20}$ for matt finished plastic cards and coated cardboard paper.

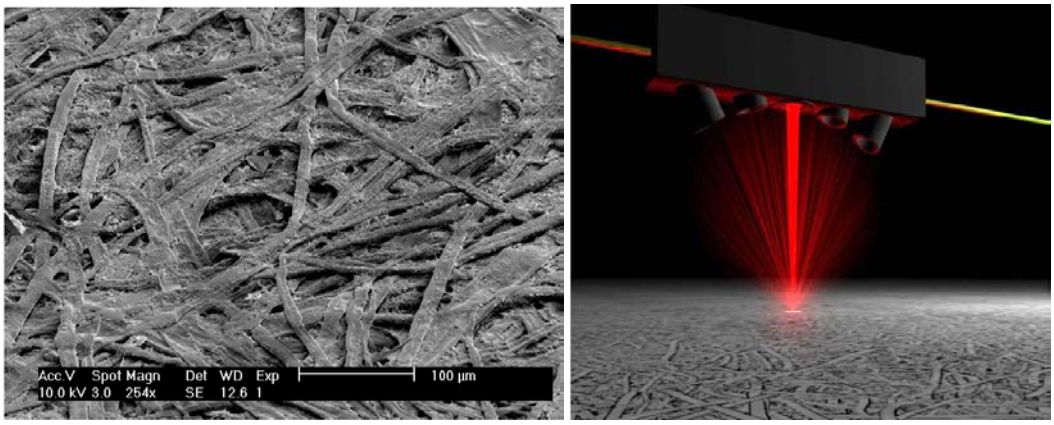



**Figure 4.1** a). Microscopy image of paper surface: the pattern on surface of paper will survive soaking, b). Optical Geometry of LSA$^{TM}$

The advantage of the LSA$^{TM}$ technique is that natural surface roughness cannot be replicated through any process, unlike holograms and watermarks. Among other advantages is 100% accuracy, robustness against wear and tear, low cost of hardware, high uniqueness of feature, covert ability, speed of scanning on production line and low additional cost for products due to absence of chips. The main disadvantages are that it cannot be used on transparent and reflecting surfaces, the acceptable limit of alignment being 1mm; and high memory requirement of between 125 -750 bytes for each code (adding up to considerable memory requirements for whole product batch runs; Cowburn, 2007). The solution is being developed by Ingenia technology for paper, plastics, metals and ceramics at product, packaging and transportation stages of the

supply chain. The implementation of this technique is expected to reduce forgery and brand theft. The main design challenge at present is the scanning apparatus and database of codes.[14]

Physical Unclonable Function (PUF) is an anti-counterfeiting technology being developed at Philips Research for application in optical, integrated circuits and S-RAM. The PUF technology has two components, a cryptographic component and a physical protection layer. The physical layer acts as a unique "fingerprint" (analogous to that described above for LSA), and protects the underlying digital signature. Tampering is prevented by requiring verification of both components. The derived fingerprint can be printed onto the product or packaging for verification. The benefit of PUF is its tamper resistant nature, covert security ability, ease of evaluation and the manufacture not being reproducible. PUF can be embedded in an RFID tag with digital signatures thereby making the tags physically unclonable. Other developments include the S-RAM PUF (Tuyls, 2007).

Singular ID is based in Singapore and uses magnetic "fingerprints" to tag items for the brand theft security market. It produces unique fingerprints by randomly distributing micro to nanoscale magnets through a non-magnetic matrix material. The type specific process used to synthesise the magnetic nanoparticles depends on the application and specification of the tag. For example, aluminium oxide (a porous material) can be used as the matrix. Nickel-based magnetic materials are deposited throughout the pore structure by an electroplating process, resulting in a random pattern, or unique magnetic signature (Burden, 2007). These fingerprints are read using a scanner with GMR heads, the same as those used in tape drives or hard disk drives. The information obtained from the scan is stored on a database. Figure 4.2 gives a representation of the spectra produced by the random distribution of these magnetic nanoparticles. These magnetic nanoparticles can be embedded in materials such as metals, plastics, or glass. The tags are covert in nature and therefore provide additional security to pharmaceutical, medical, engineered components, and financial products such as bank cards.[15] Singular ID is currently producing tags for anti-counterfeiting and brand security for automotive parts, premium fashion and the pharmaceutical industry.[16]

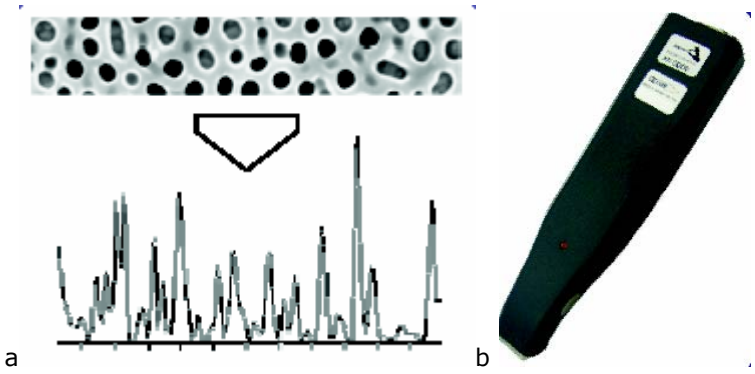



**Figure 4.2** a) Spectra generated from embedded magnetic nanoparticles, b) Hand-held scanner used by Singular ID

[14] Ingenia Technologies. 2007 [Online]. [Accessed on 15th of May]. Available from World Wide Web: http://www.ingeniatechnology.com/solutions.php

[15] Singular ID. Technology Brief. 2007 [Online]. [Accessed on 18th of May]. Available from World Wide Web: http://www.singular-id.com/downloads/Singular%20ID%20Technology.pdf

[16] Singular Id. 2007 [ Online]. [ Accessed on 18th of May]. Available from World Wide Website: http://www.singular-id.com/Applications.html

Oxonica has developed the Nanobarcodes™ particle system which consists of striped sub-micron scale metallic rods. The Nanobarcodes™ make use of the different reflectivity of gold, silver and platinum. The codes are read using an optical microscope through proprietary software. One thousand of such rods can generate trillions of unique codes. For example, 5 stripes with 2 different metals can generate 20 unique codes and 3 metals can generate 135 unique codes. An illustration and microscopy image of Nanobarcodes™ is given in Figure 4.3. These nanobarcodes can be used for covert security in inks, adhesives, laminates, paper, packaging, and films. The proprietary technology can also be used for applications in textiles, thread, and glass (Wakefield, 2007).

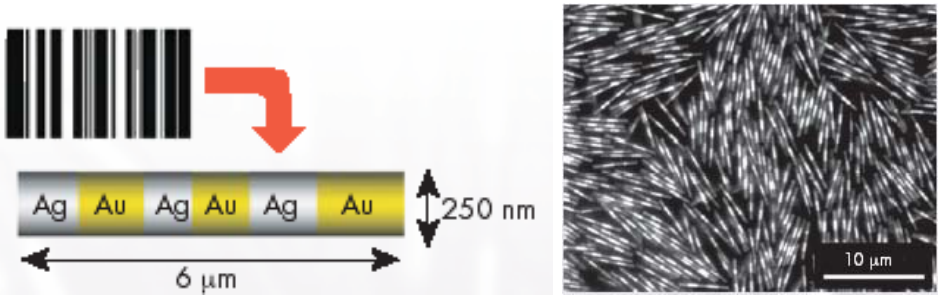



**Figure 4.3** a) Schematic of the Nanobarcodes™, b) Microscopy Image showing dark and light strips of silver and gold based on the difference of reflectivity at the observation wavelength.[17]

SERS tags, originally developed by Nanoplex technologies, use the principle of Raman scattering. Since all substances have unique spectra of scattered light, it can be effectively used as an identification tool. A SERS tag (as shown in figure 4.4) would typically consist of a core metal nanoparticle, SERS reporter and a coating of a material such as silica. Nanoparticles of gold and silver are primarily used for SERS tags. The applications of SERS tags include bank notes, paper, packing, clothing and pills. The main disadvantage in Raman scattering is the weak signal, however this can be enhanced by using surface enhancement. The advantage of SERS tags is that they are difficult to counterfeit due to the infinite number of unique codes. They are covert, non-toxic, and multifunctional. The tags can be read without contact at a distance of up to 1000 metres, in one second. These tags are also used in diagnostic applications (Wakefield, 2007).

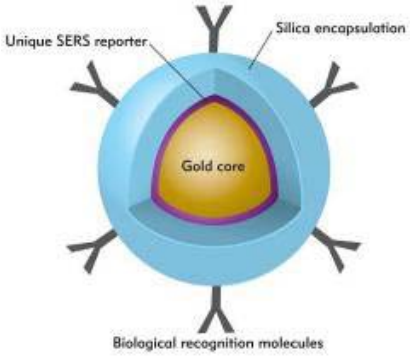



**Figure 4.4** Image of a SERS tags used in diagnostic applications

[17] Dougherty, G.M.: Microfluidic systems for solution array based bioassays http://www-eng.llnl.gov/pdfs/mic_nano-1.pdf

Massachusetts Institute of Technology (MIT) has patented a method for producing semiconductor nanocrystals (also known as quantum dots) for identifying and locating products and items. Quantum dots are interesting because they fluoresce and produce a characteristic emission spectra based on their composition and size. The MIT technique utilises one or more sizes of quantum dots as barcodes for authentication. The patent adds that the intensity of the emission at a particular wavelength can be varied to produce a binary or higher coding scheme. The materials used for quantum dots are semiconductors from groups II-VI, III-V and IV, for example zinc sulphide coated with cadmium selenide. According to the patent the application of this security tag can be to consumer items such as jewellery, vehicles and paper. It can also be used in biochemistry to track the location of biomolecules such as DNA (MIT, 2002).

For the authentication of a person's identity, biometrics is seen as class-leading. This encompasses recognition methods for human fingerprints, iris and retinal, facial and hand features. Storage of this data in a more secure manner has been the focus of research at the University of Toronto. They have developed nanostructured polymer materials to record data such as fingerprints, photographs and signatures. This consists of a thin polymer film containing three fluorescent dyes (anthracene, NBD and Nile Blue), which have non-overlapping emission and absorption spectra. The information is recorded in this polymer film by photo-bleaching the dyes in different layers of the film as shown in Figure 4.5. Information about the fingerprint, photograph and signature is recorded one on top of the other. This thin film can be read under different wavelengths of light. Identity cards based on this technique are expected to last up to 5 years and are extremely difficult to counterfeit (Pham et al., 2006).

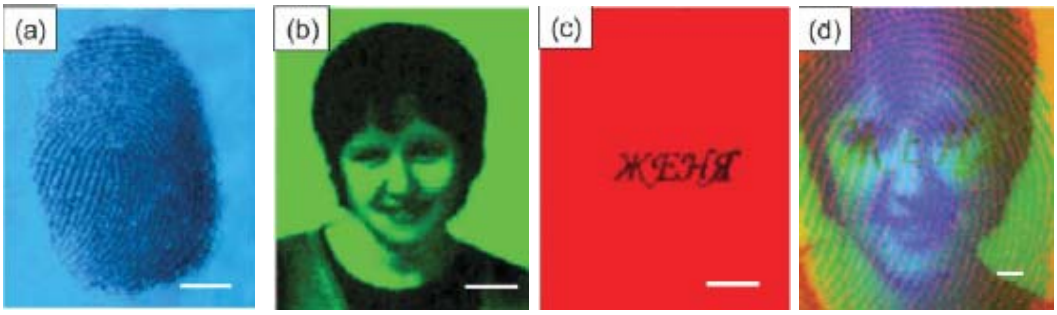



**Figure 4.5** a) Finger print encoded in anthracene, b) Photograph recorded by photo bleaching NBD, c) Signature produced by photo bleaching Nile blue by laser, d) Spatial overlap of three images (Source – University of Toronto)

## 4.3 Forensics

A fingerprint is considered as one of the most powerful types of evidence to link a suspect with a crime. Fingerprints are classified in three categories – visible, impression and latent. Visible fingerprints can be photographed and documented, however latent fingerprints are difficult to detect, document and analyse. Fingerprints are formed primarily from perspiration. The main components of a fingerprint are water, organic and inorganic chemicals (such as amino-acids, salts, glucose, peptides, salts, lactic acid, ammonia, riboflavin, and lipids). As the water evaporates these chemical residues are left behind (Ciencia Inc, 2002). Technology based on nanoparticles can detect the residues of latent fingerprints.

Texas Technical University (2002) has developed a method for photoluminiscent detection of latent fingerprints. This is achieved by binding quantum dots to fingerprint residues, illuminating them with the appropriate spectrum of light and detecting the fluorescence. Quantum dots of cadmium sulphide, cadmium selenide or indium phosphide of less than 10 nm diameter have been attached to latent fingerprint using encapsulating agents such as fatty acids or amino acid components. The excitation of the quantum dot is carried out using a laser of near ultra-violet wavelength or filtered lamp (see Figure 4.6).

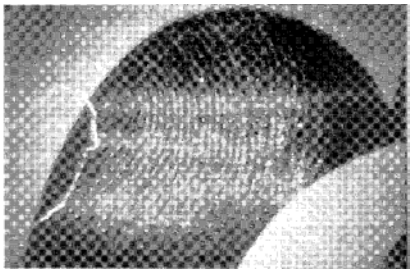


**Figure 4.6** Fingerprint detected on a soft drink can

The University of Sunderland has developed fluorescent nanoparticles for identifying latent fingerprints. These are produced as sol-gel particles in the presence of fluorescent dye derivatives. Nanoparticles with intrinsic fluorescence such as cadmium sulphide and cadmium selenide may also be used. Spherical nanoparticles with diameters between 30-500 nm have been produced. A variety of fluorescent dyes such as Texas red-labelled gelatin can be used in the process of developing the nanoparticles. These nanoparticles are coated with hydrophobic molecules such as phosphatidylcholine and phosphatidylethanolamine. Sol-gel derived nanoparticles with an embedded Texas Red-porcine thyroglobulin conjugate have been shown to bind latent fingerprints (University of Sunderland, 2004).

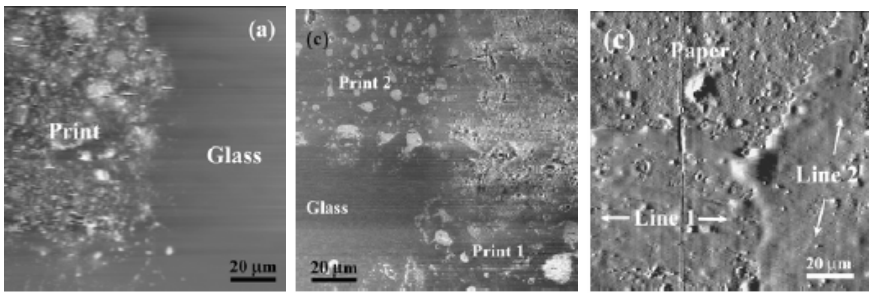
In comparison with metal particles used in "traditional" fingerprint analysis, the small size of nanoparticles makes it possible to discern the substructure of the print with greater detail and accuracy. The advantage of this technique is a better definition of fingerprints recorded from crime scenes. The technique not only enhances the sensitivity, but also makes the identification easier by allowing even a small part of the print to result in identification (see Figure 4.7).

**Figure 4.7** Image of partial latent fingerprint

Ciencia Inc has developed a method and apparatus for imaging and documenting fingerprints, which uses lipid-sensitive dyes. These fluoresce when bound to lipids (such as in the residue of a latent fingerprint) and exposed to light (Ciencia Inc, 2002).

MS Macrosystems has developed the only commercially available forensic digital imaging spectrograph. This is used in both large- and micro-scale document examinations. It utilizes digital imaging spectroscopy hardware that is analyzed through two-dimensional and three-dimensional images. Forensics experts examining the authenticity of documents that may be forged, use this tool to objectively compare physical parameters. The application of spectral imaging technology and advanced processing allows the identification of small differences between inks and papers, and it can also reveal any information that has been removed. The prime benefits of this technique are the non-destructive evaluation of documents and high resolution colour images available in three dimensions.[18]

The Scanning Probe Microscope (SPM) is useful for characterising surfaces based on topographical features, and physical and chemical properties. It has applications in the non-destructive evaluation of forged documents and micro-nanometre resolution of latent fingerprints. Watson & Watson (2007) have elaborated the use of scanning probe microscopes (including atomic force microscopes, AFM) for forensic sciences. They demonstrated that an AFM could be used to identify fingerprints under air or liquid, with no discernable differences. They also demonstrated the identification of two overlapping fingerprints. An example of document analysis was demonstrated by depositing a thin layer of pen ink on the surface of the paper. The line profile was shown to have an average height of 200nm. This information, obtained using the AFM, can be used to verify the writing history on a sample (see Figure 4.8). The main limiting factor of this technique is the long time for data acquisition and the small scan area.

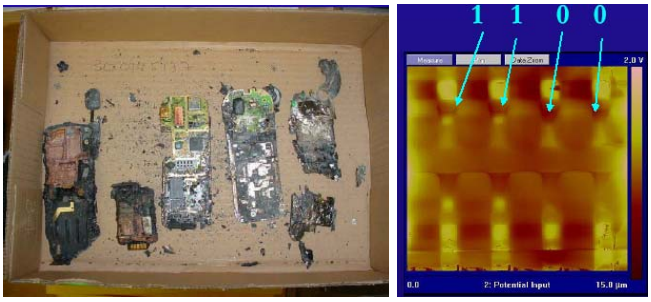



a b c

**Figure 4.8** a) Topographical image of a fingerprint on a slide, b) Topographical image of two overlapping fingerprints in three dimensions, c) Line crossing of pen ink on paper

Scanning Probe Microscopy techniques can also be used for the analysis of electronic devices, including single bits (0's and 1's). According to Dr. Silvia Valussi of the Forensic Science Services, it is possible to recover raw data from damaged specimens. For example, sim cards recovered from mobile phones after the London bombing still yielded information despite strong vibrations from the shock waves (figure 4.9). She emphasised that, "nanotechnology was having an impact in forensics" and also identified Lab-on-a-chip as an extremely useful for forensics due to its high sensitivity, high specificity and portability. However, the high cost is considered as a barrier to implementation (Valusi, 2007).

[18] MS Macrosystems: http://www.msmacrosystem.nl/Forensic/forensic_xp.html




a b

**Figure 4.9** a) Damaged mobile recovered from blasts, b) Single bit analysis using SPM

Scanning electron microscopes (SEM) play an important role in forensic examinations. SEM is considered useful for a range of applications and materials due to its extremely good depth of focus and high to low magnification. SEMs have been used in gunshot analysis, firearm identification, identification of gemstones and jewellery, examination of paint particles and fibres, handwriting and print examination, counterfeit bank notes, trace comparisons, examination of non-conducting materials, and high resolution surface imaging. In gunshot residue analysis of the specimen stub (cartridge), SEM identifies the particles due to their high contrast with the stub background. In bullet comparison tests, bullets fired from the same gun can be identified from marks left as a result of the barrel of the gun and the firing pin. The high depth of focus of an SEM provides an advantage over optical microscopy in such examinations, and the backscattered electron detectors can enhance markings on the bullet while suppressing detection of dust particles.[19] Yang *et al.* have conducted an investigation into metallic nanoparticles of gun shot residues using Electron microscopy. Their study has determined the method by which these nanoparticles are formed and proposes a model for their synthesis. The additional information obtained from this synthesis is expected to help in solving crimes through forensic studies (Yang et al., 2006).

Intel has developed a cantilever based identification method for analysing molecules. This method has application in identity testing for criminal investigation and forensic studies (also known as DNA testing). The method is based on the identification of target molecules (or analyte) using probe molecules (which bind the analyte). The probe or the analyte is attached to the cantilever, and if it binds to its counterpart then the cantilever is deflected. A magnetic counterbalancing force is used to balance the cantilever, and detection is based on the magnitude of the counterbalancing force. The following probe – analyte combinations have been successfully demonstrated, oligonucleotides-nucleic acids, and protein/peptides-antibodies (Intel Corp., 2006). Integrated Nano-technologies have patented a method for detecting a target nucleic acid. In this method, oligonucleotide probes are integrated in an electrical circuit such that they are not in contact with each other. This gap is bridged when a complementary target nucleic acid joins the two probes. This results in a current that can flow through the probes (Integrated Nanotechnologies, 2002).

## 4.4 Quantum Cryptography

Cryptography is the art of writing secret codes and is commonly used to send information from one place to another without third party interference. In modern times, cryptographic techniques form the central part of information security and related applications. The most popular and commonly used cryptographic technique is the Public Key system also known as the RSA encryption (named after mathematicians - Ronald Rivest, Adi Shamir, and Leonard Adleman). This method is widely used in software

[19] Carl Zeiss: http://www.smt.zeiss.com/C1256E4600307C70/EmbedTitelIntern/forensic/$File/forensic.pdf

products, digital signatures and for encrypting small blocks of data. The system derives the keys by factorizing the products of two large prime numbers with hundreds of digits. It is based on the view that factorizing large numbers is computationally infeasible and so the public key system will be secure. However, quantum-computing models have proved that a quantum computer can factorize very large integers much faster than a classical one, implying that the Public Key Cryptography is secure only until quantum computers are built. The main advantage of quantum cryptography over the classical one is that it provides a great alternative to the problem of key distribution. Quantum cryptography is based on two main principles in quantum mechanics - uncertainty and entanglement. Based on these quantum principles, two types of cryptographic models are proposed (Joseph, 2007).

The first approach uses the polarization of photons to encode information. Pulses of polarized light or photons represent the bits of information, encoded from the sender to the receiver. The vertical polarization ↑ represents 0 and horizontal polarization → represents 1. In order to protect the information from third party interference, the sender uses diagonal polarizations to encrypt the message, so that ↑ is encrypted as ↗ and → is encrypted as ↙ . Once the key has been securely transmitted, the message can be encrypted with this key and sent by any classical methods like, email, phone or post.

The second approach to quantum cryptography is entangled photons. This technique utilizes the properties of entanglement to make the information transfer secure. The entangled, or paired, photons are distributed such that both the sender and recipient receive one photon from each pair. If a key needs to be sent from A to B, the paired photons are distributed so that both A and B receive one photon from each pair. Once the photons are received, both A and B will measure the polarization of the light. Due to entanglement, measurements on both sides will give the same answer. This implies that if B measures the photon polarized in one direction, then A will also get the same measurement. These measurements are then added into strings of 0s and 1s to give the key (Jennewein et al., 2000).

There have been significant breakthroughs in cryptography using entangled photons. In 2004, a team of scientists from the University of Vienna and ARC Seibersdorf Research transferred funds between Vienna City Hall and Bank Austria Creditanstalt using entangled photons. Similarly, a group of scientist from Northwestern University has sent entangled photons over a distance of 100 kilometres through optical fibre, a record distance for entangled photons even without the classical signal (Greene, 2006). Some of the companies providing security solutions using quantum cryptography include the Geneva based ID Quantique and New York based MagiQ.

## 4.5 Market of counterfeit and grey products

The United States Chamber of Commerce has estimated that counterfeiting and piracy cost US companies, between $ 200- 250 billion per annum and roughly 750,000 jobs in employment in all sectors.[20] Industry Week has classified piracy into three categories – theft, counterfeits and grey markets. Theft of manufactured goods is done within and outside the compound of the manufacturers by organised crime. Counterfeiting is a form of theft, where high or low quality copied products are produced. Customers cannot readily distinguish between the authentic and counterfeit products. Grey markets are created by real products that are released into the market without the regulator's knowledge, or the consent of the owner or manufacturer. This is manifested in the form of unreported sales, leaking of excess inventory, illegal sales across borders, and multiple sales of the same product (Ferreira et al., 2007). According to the US Customs and Border Protection agency, $155 million worth of counterfeit goods were seized in 2006. It

[20] US Chamber of Commerce: http://www.uschamber.com/ncf/initiatives/counterfeiting.htm

was further reported that 81% of these goods originated from China, 6% from Hong Kong, 1% from Taiwan, 1% from Korea and 10% from other locations (Catto-Smith, 2007).

Oxonica has estimated that in 2003, the total revenue lost due to counterfeit products was € 600 billion. In the EU alone this figure amounted to € 65 billion (equivalent of 200,000 jobs lost).[21] Philips has estimated that illegal overproduction in grey and black markets is worth $400 billion (Tuyls, 2007). Figures published by the European Commission showed that € 85 million worth of counterfeit goods and pirated articles were seized at EU borders in 2003. It was also reported that 66% of these good came from Thailand and China.[22]

According to Interpol estimates, counterfeiting in 2004 resulted in $512 billion of lost sales. In Asia, this has been identified as an acute problem in pharmaceutical and medical products, as counterfeiting has not only lead to loss in sales but there are also health risks to consumers.[23]

According to a survey conducted by Japanese banks, fake credit cards rank only next to lost or stolen cards. This phenomenon is rampant in Asia though it is also growing rapidly in major cities in the USA, UK, Europe, Canada and Latin America. It has been reported in United States that each card generates an average of $2,000 of fraudulent charges before being stopped.[24]

There has been an increase in the market of counterfeit and grey products in recent years. It has become amply clear that there is a growing evidence for over-production and under reporting. These growing problems can be addressed by using enhanced security features that are cheap and extremely covert. Nanotechnology based solutions offer opportunities to address the growing crisis of losses in revenue, and intellectual property.

## 4.6 Conclusions

Nanotechnology applications in identification of products are increasing. Development work related to identification technologies is being conducted both through start-up companies and established multi-nationals. There are a range of issues which need to be considered such as who controls the reading of the covert codes.

The new identification techniques offer the promise of reducing the piracy of goods and products. With overproduction leading to creation of grey markets, it is imperative that EU governments should, through tax incentives, support the development of identification technology in order to stop fraud. However, ethical issues regarding privacy have been raised relating to RFID tagging of products (as discussed in Chapter 5). Whether nanobarcodes or other new methods of identification will face the same treatment, remains to be seen.

Nanoscience and nanotechnology know-how is having an impact on forensic studies. Tools for analysis such as SPM and SEM are being widely used to solve crime by analysing evidence at the nanoscale. The analysis work is principally being carried out within government agencies. However, the development of analytical tools and methods is being carried out in large companies. Further development is expected to help law enforcement agencies successfully solve difficult crimes using partial evidence such as latent fingerprints and DNA. Quantum Cryptography is expected to provide a highly secure method for encrypting data transfer on the Internet. However, there are many

[21] Oxonica: http://www.oxonica.com/security/security_intro.php

[22] Interpol: http://www.interpol.int/Public/News/Factsheet51pr21.asp

[23] Singular Id.: http://www.singular-id.com/downloads/Protection%20for%20drugs%20and%20medical%20products.pdf

[24] Singular Id.: http://www.singular-id.com/downloads/Security%20for%20financial%20products.pdf

outstanding challenges that need to be addressed before quantum computing can become a reality.

## 4.7 References and further reading


Burden, 2007. *Query regarding products*. [Online]. Personal communication to Kshitij Singh, 28th May.

Catto-Smith, 2007. Nanowerk: http://www.nanowerk.com/news/newsid=2014.php

Ciencia Inc. 2002. "Method and apparatus for imaging and documenting fingerprints." US patent 6,485, 981 B1. 26-10-2002.

Cowburn & Buchanan, 2005. "Fingerprinting documents and packaging." Nature **436** p. 475

Cowburn, 2007. "Laser Surface authentication: Biometerics for everyone", distributed through the post event proceedings for Nanotechnology for security and crime prevention. Ingenia technologies. Royal Society, 18th January.

Ferreira, et al., 2007. Industry Week: http://www.industryweek.com/ReadArticle.aspx?ArticleID=13925

Greene, 2006. "Making quantum practical." Technology Review: http://www.technologyreview.com/Infotech/16691/

Integrated Nanotechnologies. 2002. "High Resolution DNA detection methods and device." US patent 6,399,303 B1. 4-6-2002.

Intel Corporation, 2006. "Detecting molecular binding by monitoring feedback controlled cantilever detection." US patent application 7,105,301 B2. 12-09-2006. Jennewein, et al., 2000. "Quantum cryptography with entangled photons." Physical Review Letters **84** (20) pp. 4729-4732

Joseph, 2007. "Introduction to Quantum Computing." Nanoforum report (www.nanoforum.org).

Massachusetts Institute of Technology (MIT) 2002. *Inventory Control.* US patent 6,774,361 B2. 10-8-2004.

Pham et al., 2006. "Polymer nanostructured material for the recording of biometric features." J. Mater. Chem **17** pp. 523–526

Texas Technical University. 2001. "Fingerprint development method." US patent 6,306, 662 B1. 23-10-2001.

Tuyls, 2007. "Anti-counterfeiting technology based on physically unclonable function", presentation at the Nanotechnology for security and crime prevention conference. Philips. Royal Society, 18th January.

University of Sunderland. 2004. "Nanoparticles as agents for imaging fingerprints." British patent application 0400235.8 7-1-2004

Valussi, 2007. "Advances in Nanotechnology for forensic application", presentation at the Nanotechnology for security and crime prevention conference. Forensic Science Services R&D. Royal Society, 18th January.

Wakefield, 2007. "Nanotechnology Enabled Solutions for Anti-counterfeiting and Brand Protection", presentation at Nanotechnology for security and crime prevention conference. Oxonica. Royal Society, 18th January.

Watson & Watson, 2007. "Potential applications of scanning probe microscopy in forensic science." Journal of Physics: Conference Series **61** pp. 1251-1255

Yang et al., 2006. "Nano-Forensics - Nanoparticles in Gun-Shot-Residue." IEEE Conference on Emerging Technologies - Nanoelectronics **10-13** pp 269-272

# 5 Societal Implications

## 5.1 Introduction

Traditionally, the EU was not allowed to fund security research, but national and EU politicians are rapidly developing the Common Foreign and Security Policy and European Security and Defence Policy. At the end of FP6, some security research projects were already funded under the Preparatory Action for Security Research (PASR) and under FP7, a total budget of €1400 Million is reserved for security research (€86.9 Million in the first call in 2007). This budget can be increased due to joint calls involving the security programme and another programme. In 2007, there is a joint call of the ICT and Security programmes. For 2008, a proposed joint call of the Security and Nanotechnology programmes is being discussed. These figures give an indication of the considerable importance and novelty of the technology developments and potential societal impacts being discussed in the present report.

This chapter discusses four questions with regards to the societal implications of nanotechnology based security technologies:

1) What is the existing regulatory and ethical framework that is relevant to nanotechnology based security technologies?
2) What impacts on ethics and human rights are expected from new nanotechnology based security technologies?
3) What is known about European public opinion of nanotechnology and of justice, freedom and security policies?
4) What are the key issues for further research in social sciences and humanities, public debate and political decision–making, based on the analysis in this chapter?

## 5.2 Regulatory and ethical framework

In this section, the central question is: "What is the existing regulatory and ethical framework that is relevant to nanotechnology based security technologies?" A number of European and International declarations, regulations and guidelines are introduced, and their relevance to nanotechnology based security technologies is assessed. The section ends with conclusions summarising the main established legal and ethical requirements which impose boundaries on the development of nanotechnology based security technologies. Different types of technologies and applications are regulated differently.

### 5.2.1 EU regulatory and ethical framework

The existing regulatory and ethical framework relevant to nanotechnology based security technologies at EU level is laid down in a number of declarations, legislative documents and ethical codes. The "Charter of Fundamental Rights of the European Union" (EU, 2000) includes several values which are affected by security applications of nanotechnology. These are: human dignity, right to integrity of the person, prohibition of … degrading or inhuman treatment, right to liberty and security, respect for private and family life, protection of personal data, freedom of the arts and sciences, equality and non-discrimination, environmental and consumer protection. The Charter explicitly prohibits any abuse of these fundamental rights which infringes on the rights of others.

Human dignity is not defined in the Charter, which simply states that it is inviolable and must be respected and protected.

J-P Wils (2006) defines Human Dignity as a key ethical concept, including a descriptive part delineating what is a Human being, and a prescriptive part, laying down rules for treating a human being. The concept has a long history and was already discussed by Cicero in ancient Rome, as well as numerous classical and Catholic/Christian authors. Immanuel Kant made human dignity a central ethical concept. He defined it in his book

Grundlegung zur Metaphysik der Sitten (Foundation of the Metaphysics of Morals): In the domain of the Goals, everything has either a price or a dignity. You can replace what has a price with something else as equivalent. What is above any price, and has no equivalent, has a dignity.[25] Kant based human dignity on the autonomy of the human person to make ethical choices. The intention of the concept human dignity is the categorical imperative: Always act in such a way that you treat humanity and each individual human being as an end in itself and never as means. There is no agreement on the meaning on the term "Human dignity" (Wils, 2006).

More generally, human dignity can be used as a moral concept or a legal term, but it is controversial whether human embryos or non-human beings are covered by the terms (Wikipedia, 2007). The meaning of human dignity can be considered to be specified in other articles of the Charter.

Nanotechnology based security technologies which involve the insertion of a device into the human body or integration of the human brain or nervous system with a technical system, (either within the body or wirelessly) have implications for an individual's right to physical and mental integrity. Such intrusions are not allowed without the free and informed consent of the person, as specified by law.

The Charter prohibits degrading or inhuman treatment of anyone. This is relevant to nanotechnology based security technologies which enable others to view the naked body of a person, or that can be used to control a person's movements or thoughts by someone or something else.

The right to liberty and security is ambiguous if applied to security technologies, because it does not allow for conflict between individuals or groups, where one person or group takes the liberty to threaten others' security. Since the Charter explicitly prohibits abuse of fundamental rights; governments are entitled to protect the security of citizens by limiting the freedom of offenders. However, the right balance between respecting the right to liberty as well as security must be determined on a case by case basis.

Respect for private and family life, home and communications imposes restrictions on nanotechnology based security technologies which enable governments or others to collect information on someone without informed consent. Nanotechnology based miniaturised sensors, tags and smart dust motes may contribute to the problem caused by other security technologies, because they enable invisible spying on unsuspecting persons.

Protection of personal data means that personal data "must be processed fairly for specified purposes and on the basis of consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified." Infringement of the protection of personal data is not specific for nanotechnology based security technologies. Coupling of databases of public transport use, shopping, medical dossiers, and data mining techniques are currently the most pressing concern for legislators. Justice departments and the police are interested in using new technological possibilities to fight crime. What is legitimate and which procedures should be followed to ensure data protection is a political issue currently in debate.

Equality and non-discrimination may be at stake if nanotechnology based security technologies are used to set apart and limit the rights of a group of people sharing a particular characteristic (e.g. adhering to a particular religion, suffering from some disease or disability). However, such issues are related more to the coupling of databases than specific nanodevices or nanomaterials applied in security technologies.

The EU must protect and improve environmental quality and ensure a high level of consumer protection. Nanotechnology based security technologies must be assessed on a

[25] Kant, 1965, p 58, quoted in Wils, 2006. Translation Ineke Malsch

case by case basis for compliance with these objectives, as part of regular risk assessment practices for allowing products on the market. Environment, Health and Safety aspects of nanomaterials are high on the policy maker's agenda. This is relevant to all applications including for security.

Two EU directives specify the rules for personal data and privacy protection:

- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (EU, 2002).
- Directive 95/46/EC of the European Parliament and of the Council of the European Union of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (EU, 1995).

The European Commission is working on better implementation of the Data protection directive 95/46/EC (European Commission, 2007). The Directive does not cover public security, defence, state security and the activities of the state in areas of criminal law. The Commission proposes to protect personal data processed in the framework of police and judicial cooperation in criminal matters (COM(2005) 475 final, 04.10.2005). EU Member States may restrict data protection principles under certain circumstances including the need to fight crime or to protect public health in emergencies. Directive 95/46/EC limits these restrictions in article 13. The Commission strives to protect personal data as guaranteed by article 8 of the Charter of Fundamental Rights.

EU regulations on classified information currently in force cover the access rights of EC officials and employees to classified information held by the Commission (COM1999/218/EC) and agreements with associated states to the EU laying down rules for exchanging classified information. This is not particularly suitable for security research projects handling classified information. In 1992, the Commission had sent a proposal for a Council Regulation (EEC) on the security measures applicable to classified information produced or transmitted in connection with EEC or Euratom activities (COM92/56 final). However, this was rejected by the European Parliament in 1993 (OJ C176, 28.6.1993).

**Research**

Freedom of the arts and sciences, as guaranteed in the EU Charter for Fundamental Rights (EU, 2000) is relevant for the research done in EU funded projects on nanotechnology as well as on security technology. This imposes restrictions on the influence the EC, national governments, users and other stakeholders can exert on the outcomes of the research. On the other hand, researchers are not allowed to abuse their academic freedom, and must abide by ethical principles relevant to their investigations. This implies respecting the rights of people participating in experiments, ensuring the safety, security and ethical acceptability of the technologies they are developing, and taking precautions to avoid dual use of their results for illegitimate purposes, such as weapons of mass destruction. It also implies a responsibility to notify policy makers promptly of new potential safety and security risks resulting from the technologies they are developing.

The different rights can conflict in individual cases, therefore the EC has established ethics review boards and a European Group on Ethics (EGE), to determine a good balance of the rights in EU funded projects. With regard to security technologies, the EGE published opinion number 20 on ICT implants in the human body, which is relevant to nanotechnology-based security applications that involve the incorporation of electronic devices into the human body. In opinion 20, article 6.4 on non-medical implants, the EGE warns "that non-medical applications of ICT implants are a potential threat to human dignity and democratic society." The principles of informed consent and proportionality must apply. ICT implants for surveillance purposes threaten human dignity. "The EGE insists that such surveillance applications of ICT implants may only be permitted if the legislator considers that there is an urgent and justified necessity in a democratic society

… and there are no less intrusive methods." Surveillance applications must be specified in legislation and monitored by an independent court (European Group on Ethics, 2005).

The checklist of ethical issues for FP6 proposals is mainly focused on biomedical research. However, informed consent in case the project involves human data collection is also relevant to some nanotechnology based security technologies. Other relevant aspects are privacy issues, both processing of genetic information or personal data, and tracking the location or observation of people. Research involving developing countries (use of local resources or benefit to local community) and dual use aspects (research having potential military or terrorist applications) are also relevant to some nanotechnology based security technologies (Cordis FP7 webpages, 2007).

### 5.2.2 Other international declarations

The Declaration of Principles of the World Summit on the Information Society (WSIS) of 12 December 2003 includes four articles on ethical aspects. Articles 56 and 57 address fundamental values and ethics for the Information Society as a whole. Article 58 states: "The use of ICTs and content creation should respect human rights and fundamental freedoms of others, including personal privacy, and the right to freedom of thought, conscience and religion in conformity with relevant international instruments." Article 59 states: "All actors in the Information Society should take appropriate actions and preventive measures, as determined by law, against abusive uses of ICTs, such as illegal and other acts motivated by racism, racial discrimination, xenophobia, and related intolerance, hatred, violence, all forms of child abuse, including paedophilia and child pornography, and trafficking in, and exploitation of, human beings." (WSIS, 2003).

The Organisation for Economic Co-operation and Development (OECD) has adopted guidelines on the protection of privacy and trans-border flow of personal data, which forms the framework for harmonising national and EU legislation (OECD, 1980). This was followed by a "Ministerial Declaration on the Protection of Privacy", at a conference in Ottawa, Canada, 7-9 October 1998 (OECD, 1998). An OECD Working Party on Information Security and Privacy (WPISP) monitors trends and discusses policy options.

The Council of Europe also lays down rules for personal data protection in the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe of 1 January 1981." (Council of Europe, 1981).

The main issue in the global discussion on privacy and data protection is related to differences in legislation between the USA and Europe, e.g. concerning personal data of airline passengers. This is not related to any particular technology, but an element of the legal and ethical framework in which some nanotechnology based identification and tracking devices are being developed. In the present globalising information society, the EU is not free to determine its own legislation independently of other countries.

### 5.2.3 Conclusions on regulatory and ethical framework

The main established legal and ethical requirements which impose boundaries on the development of nanotechnology based security technologies are summarised below:

- For active nanodevices implanted in the human body or which can wirelessly connect to the human brain or nervous system, or enable others to view the naked body of a person; the right to physical and mental integrity and prohibition of degrading or inhuman treatment are valid. These are apparently not relevant to other applications of nanotechnology for security.
- RFID chips and other nanoelectronics and sensor based technologies which can be used to collect personal and group data for storing in databases, are covered by legislation and ethical guidelines for protection of private and family life, home and communications; personal data protection; and equality and non-discrimination.

- All products must respect legislation aimed at protecting and enhancing environmental quality and consumer protection. This could imply that non-medical implants or RFID chips introduced inside the body which are not safe should be forbidden. This raises the question of whether current legislation is adequate for regulating the use of sub dermal RFID chips for tagging people or for their use as an e-wallet?
- In the research phase, a balance must be struck between academic freedom and responsible science and technology development. This is particularly sensitive for dual use technologies with civil as well as defence applications, requiring a new balance between openness and handling classified information.
- The debate on relevant European legislation is continuing, especially on privacy and personal data protection. This discussion is clearly embedded in global discussions, e.g. in the OECD or in bilateral negotiations such as with the USA. The EU will in the coming years develop new rules for handling classified information in EU funded projects.

## 5.3 Impacts on ethics and human rights

To assess potential impacts of nanotechnology based security technologies on ethics and human rights, strategy documents discussing the aims and scope of European Security research policies are major sources of information. As nanotechnology based security technologies currently do not exist or are only just entering into the market of security technologies, the actual impacts on ethics and human rights can be observed only to a limited extent, e.g. in the case of RFID chips, which are currently being discussed in the European and national Parliaments, other policy making circles and the public. The following discussion should be considered preliminary and progress in the field should be monitored to identify emerging unforeseen impacts as soon as possible, enabling adequate policy making.

### 5.3.1 Impacts of Security technologies

In 2003 the EC engaged a Group of Personalities in the field of security research (Group of Personalities, 2003), who proposed priorities for European Security Research and the integration of civil and defence technology development activities of the EU and member states.[26] The Group of Personalities launched the concept of 'Internal Security' in Europe: "… a concept aimed at protecting citizens from threats like terrorism, organised crime, etc. The fundamental objective of 'Internal Security' is hence to protect the freedom and integrity of European citizens." "Europe's vision of security must … embrace a notion of 'Internal Security' that can include a genuine feeling of well-being and safety for its citizens, while respecting its values of human rights, democracy, rule of law and fundamental freedoms." The Group of Personalities believed in the benefits technology can bring to security: "Technology itself cannot guarantee security, but security without the support of technology is impossible". This view is not without controversy and needs more corroboration than is offered.

During the Nanoforum "Nanotechnology and Security" workshop, Dr Donald Bruce stressed the need to "suspend belief that innovation is always good". Before deciding on developing any new security technology, the question should be asked whether there is a real need for the innovation. Do existing measures no longer suffice? (Morrison, 2007). Such an assessment of gaps in present security which require new technological solutions is lacking in the report from the Group of Personalities. The main motivation is the lower level of investment in security and defence technologies in Europe compared to the United States, and the lower efficiency in research spending due to a lack of cooperation between member states. There is no clear demand from the technology end users. To

[26] In this report, we can only discuss civil security aspects, leaving aside military applications.

stimulate such demand should be one of the aims of a European Security Research programme, according to the Group of Personalities. Security research is clearly a technology push area. There has been no analysis of the real needs of public and private organizations in the security and defence areas. This is even more pressing in the case of nanotechnology based security technologies, where both the technical characteristics and the potential applications are still largely undefined.

The Group of Personalities also pointed out that the distinction between military and civil technologies is becoming less important, and the same technologies can be applied for both purposes without adaptation (Group of Personalities, 2003). They do not seem to consider the possibility that such dual use technologies can also be applied by criminals and terrorists, or regimes which do not respect human rights (as is the case in many countries in the world today). Currently, there is no European regulation of classified information used or originating from European funded research (see section 5.2.1 above). This implies that either the security research programme does not lead to results which are particularly useful for the security sector, or there is an acute risk that the published results end up in the wrong hands, thereby undermining the security of European citizens even more.

On a more fundamental level, the disappearance of the boundary between military and civilian technologies also infringes on academic freedom. Especially in the case of life sciences, the scientific community is put increasingly under political pressure to limit openness and take responsibility not only for its own research and the safety and security of its results, but also to take measures to restrict access to materials and knowledge by others who may use it for hostile purposes (IAP, 2005). The further integration of civil and security research may lead to expansion of such precautions and restrictions of academic freedom, to the detriment of scientific discovery and technological progress for the benefit of society in areas like nanomedicine, nanoelectronics, energy and environmental technologies.

Similarly, the existing export restrictions for strategic goods may be expanded to cover more and more civilian technologies with a potential dual use. This could jeopardise international trade and world peace and stability.

According to a recent publication of the Rathenau Institute in the Netherlands (Vedder et al, 2007), in the new millennium, governments in Europe as well as North America have been establishing regulatory and technological systems aimed at improving security in their territories man-made disruption to population, infrastructure, environment and food and water supply. This trend was already set in motion before the terrorist attack of 11 September 2001, but has been intensified since that. As a result, the privacy of citizens has been eroded further without proper discussion of how privacy and security should be balanced. The motivation behind the necessity of these measures is mostly lacking. There is a need for political and public debate, taking into account:

- the cumulative effect of intelligence and security measures;
- advancing digitisation of data files;
- efficacy of security measures;
- greater transparency of national and European procedures for adopting new security measures.

The closed circles where the debate takes place must be opened up to the general public (Vedder et al, 2007).

The Rathenau report is playing a role in the political and public debate in the Netherlands. Some commentators find it too pessimistic regarding the impacts of security policies and technologies. Also, a large majority of the Dutch public is more concerned about security than about privacy (Comité 4 en 5 mei, 2007). A similar trend in public opinion can be observed in other European countries, as discussed below (section 5.4).

### 5.3.2 Impacts of RFID and related technologies

The EC's work on better implementation of the Data protection directive 95/46/EC also includes technological aspects. In 2003 and 2004 the Commission worked on a Communication on Privacy Enhancing Technologies (PET). At present, "RFID devices raise fundamental issues on the scope of the data protection rules and the concept of personal data. The combination of sound and image data with automatic recognition imposes particular care when applying the principles of the directive." However, the Commission believes the rules are still valid. The Directive is technologically neutral, and sufficiently general to accommodate new technologies, although particular guidelines may have to be adapted (European Commission, 2007). The European Parliament is also discussing the implications of RFID chips and how to regulate them. The Scientific and Technological Options Assessment unit (STOA) of the European Parliament is engaged in a project on RFID and Identity Management. The final report was announced for April 2007 but had not been published yet in June. (van 't Hof, forthcoming)

Philips' chief privacy officer Jeroen Terstegge criticised the focus on "personal data protection" by the EU in the discussion on RFID chips. He believes that the focus of legal protection should be "digital footprints", and whether or not these footprints can strictly be classified as personal data. The point is not that the use of RFIDs chips and data storage will infringe on personal data protection (Seminar RFID & Opsporing (Tracing), ECP.NL, Rathenau Institute, RFID platform Nederland, Den Haag, 4 April 2007).[27]

**Box 1: Case study on Dutch transport RFID chip card**

Dutch public transport companies will introduce RFID chip card technology to pay for tickets in 2009. Two types of tickets are available, anonymous and personalised. The railway company NS is pushing for the personalised card, by only offering a price reduction on personalised cards and sending current subscription holders the personalised card. The Committee on Secure Personal Data (CBP) and the passenger association ROVER have complained that NS is violating privacy and personal data protection legislation. A public debate in Parliament and the media started in April 2007, stimulated by the Rathenau Institute.

The Public Prosecutor Harm Brouwer would also like to be able to use the data collected with RFID and other chip technologies. He sees opportunities for identifying criminals and collecting evidence, including their travel by public transport and car (after introducing road pricing). He discussed these opportunities during a seminar organised by the Rathenau Institute, RFID Platform Nederland and ECP.nl on 4 April 2007.[28]

Proponents for the use of private databases for police and national security purposes, like Mr Brouwer (see box 1), do not appear to make a rational assessment of the main current bottlenecks in crime fighting, and identify the optimal use of the public budget for the police and justice department. Instead they seem to be attempting an increase in the public budget by imposing legal requirements for storing data on private companies, without paying for it. This leads to an increase in taxes "in kind" on these companies, which may lead to higher prices for consumers. The quality of the debate would improve if all the costs, expected benefits and risks of each technical and non-technical security option were made available.

In the Nanoforum workshop on Nanotechnology and Security several new ethical aspects of nanotechnology were discussed, relating to the implications of invisible distributed wireless sensor networks (possibly mobile). For example, how can informed consent of the observed persons be guaranteed? Can the devices be turned off after use or by

[27] http://www.rathenau.nl/showpageproject.asp?steID=1&ID=2029

[28] http://www.rathenau.nl/showpage.asp?steID=1&item=2132

people who do not want to be observed by them? Should the devices be biodegradable after use? (Morrison, 2007).

The Dutch ministry of Justice sent an evaluation of the personal data protection law to the Parliament on 24 May 2007. The authors are concerned that the existing legislation is inadequate to handle privacy aspects of new technologies including biometrics and nanotechnology. (Zwenne et al, 2007)

The innovation observatory of MadrI+D in Madrid, has published a report comparing the policy and technological aspects of novel biometric or electronic National Identity Cards in a number of European countries and the USA. They found that "privacy issues raised by the new identification systems are an important concern in several countries." In Belgium and Austria, privacy considerations have been taken into account in the design of the cards. There is an intensive public debate on it in France and the UK. France has postponed introduction of the new national ID card until 2008, and the UK foresees it in 2010. ID cards or passports with RFID chips are a particular concern, as the personal and biometric data can be read without direct contact. In Germany, the Federal Office for Information Security BSI has studied RFID security and biometric recognition techniques (Vázquez Gallo & Sánchez Ávila, 2007).

Research on the ethical and social implications of biometrics under the EU project BITE, also reveals similar issues of balancing privacy and security. The risk of "function creep" or the unforeseen and unauthorised re-use of stored personal data is a key issue for technologies used in biometrics as well as nano-based security technologies. DNA-based identification technologies especially may make available not only information allowing the identification of an individual, but also his or her genetic make-up which may then potentially be abused for illegitimate purposes (Mordini & Petrini, 2007). As mentioned in chapter 2 and 4, nanotechnology can also be applied in DNA sensor technologies.

### 5.3.3 Conclusions on impacts on ethics and human rights

At present, the potential impacts of nanotechnology based security technologies are still unclear. The expected impacts of such research in general are to improve security for the European citizen. However, the demand from end users for security technologies has not been clearly articulated. In addition, the boundary between civil and military research is eroding, and this may lead to unexpected security risks if new dual use technologies end up in the wrong hands. Also, academic freedom and free trade may be further restricted, even for traditional non-military technologies. RFID chips and other technologies may not respect privacy and personal data protection legislation. This may be overcome by introducing privacy enhancing technologies (PET). However, justice departments and police forces are interested to use collected data for fighting crime and terrorism. These issues have started a debate in the last few years in Europe and its Member States, however the quality of the debate may be improved by providing complete information on costs, expected benefits and risks, and discussing technical as well as non-technical solutions to concrete security risks.

## 5.4 Public perception

The regular Eurobarometer surveys give an insight to European public opinion on security, privacy and nanotechnology, and current public opinion seems to be more concerned with security than with privacy or freedom.

According to a recent Special Eurobarometer survey on "The role of the European Union in Justice, Freedom and Security policy areas" (European Commission, 2007), 56% of respondents in the 25 EU member states[29] considered the "fight against organized crime and trafficking" among the three priorities for the European Union in the Justice, Freedom and Security Areas. This was immediately followed by 55% in favour of the

[29] The survey was held in June – July 2006, before the accession of Bulgaria and Romania.

"fight against terrorism". "Promoting and protecting fundamental rights" was seen as a top priority by 24%; and "Quality of Justice" by 21%. Many people seem to trust their government and the EU more than their fellow citizens. This is also reflected in the latest General Eurobarometer survey held in autumn 2006. In this survey, 75% of respondents favour a common European Security and Defence Policy; 85% believe criminals must be punished more severely; and 64% want more equality and justice than individual freedom (European Commission, 2006).

Still, crime and terrorism are not the biggest concerns for European citizens. According to the General Eurobarometer survey held in autumn 2005 (European Commission, 2005), unemployment (44%) and the economic situation (26%) are the most important problems respondent's countries were facing, followed by crime (24%). Terrorism (14%) ranked seventh out of ten.

Public perception of problems and threats seems to be relatively unstable and related to actual incidents. According to an earlier Eurobarometer survey (European Commission, 2002), over 80% of respondents feared international terrorism, about 78% feared organized crime, about 76% proliferation of Weapons of Mass Destruction and about 75% nuclear accidents. This was just after the attack on the World Trade Centre in New York.

In these polls, no technical or non-technical questions were asked about solutions to the main problems. There is a pressing need for balanced information to the public before any conclusions can be drawn on whether they would accept security technologies or measures.

European public awareness and opinions of different technologies including nanotechnology have been investigated in other Eurobarometer surveys. Public awareness of nanotechnology is gradually developing. According to the latest Eurobarometer study on Biotechnology, held in 2005, 42% of respondents did not know if nanotechnology would have positive or negative impacts on their lives. 40% thought it would have a positive effect, 13% expected no change, and 5% believed nanotechnology would lead to a deterioration in their quality of life. However, only 44% said they had heard of nanotechnology before participating in the Eurobarometer survey. Nanotechnology is considered morally acceptable, useful and not risky, and most respondents believe it should be encouraged. A total of 55% of respondents support nanotechnology, including both people who knew about it before and those who heard about nanotechnology for the first time (European Commission, 2006).

Other studies on the public perception of nanotechnology indicate that health, safety and environment risks of engineered nanomaterials appear to be the main concern for societal groups. The public debate focuses on occupational safety and applications of nanoparticles in cosmetics, washing machines and food.

Other NGO's are worried about privacy aspects of ambient intelligence; focusing mainly on RFID chips, cameras, internet, and data collection and storage technologies. The Consumentenbond (Dutch Consumers Union) and Meldpunt Misbruik Identificatieplicht (clearinghouse for abuse of identification legislation) attended the seminar of RFID and tracing organised by ECP.NL, Rathenau Institute and RFID platform Nederland on 4 April 2007. The latter NGO especially, is very concerned about the privacy implications of RFID and other security technologies and measures. The NGO European Digital Rights (EDRI) is an association of 25 European privacy and civil rights organisations, which campaigns for civil rights in the Information Society.[30] Amnesty International has a campaign on the Internet and Human Rights, fighting censorship and human rights violations by governments aided by Internet providers.[31] So far, none of them has published a statement on nanotechnology as such, although RFID chips and other security

[30] http://www.edri.org/

[31] http://irrepressible.info/

technologies have been commented on. Peace movements such as Pax Christi International focus more on human rights, mediation and reconciliation in conflicts. Technological aspects are addressed in their advocacy work on disarmament and arms control. Such peace movements tend to focus on military technologies including Weapons of Mass Destruction, conventional weapons (cluster ammunition, small arms, etc.) and sometimes non-lethal weapons.[32]

The UK based NGO, Privacy International, has issued a map of leading surveillance societies in the EU and around the world. According to it, Germany is the best of the European countries, offering significant protection and safeguards for the privacy of its citizens. Belgium, Austria and Greece offer adequate safeguards against abuse. Some safeguards but weakened protection is offered by Portugal, France, Italy, Cyprus, Hungary, Poland, Latvia, Estonia and Finland. Ireland, Spain, the Netherlands, Denmark, Czech Republic, Slovenia, Lithuania and Sweden systematically fail to uphold safeguards. The UK is one of five global, endemic surveillance societies, offering the worst protection (Privacy International, 2006). Privacy International has included nanotechnology as a potential future concern for privacy in its annual reports in 2004 and 2005 (PHR 2004, PHR 2005).

## 5.5 Key societal and ethical issues

Key societal and ethical issues related to security technologies and to nanotechnologies have been identified from several sources. These are discussed below.

The European Security Research Advisory Board (ESRAB) has developed a strategic research agenda for European security research, including technical and non-technical aspects (ESRAB, 2006). ESRAB highlights the need for regulating governance, including national authorities and improving EU regulations on classified information. The programme's guiding principle is respect for privacy and civil liberties. This is of course a requirement for all EU funded research. The research agenda aims to integrate research and technology development with research into political, social and human sciences in five areas:

- citizens and security;
- understanding organizational structures and cultures of public users;
- foresight scenarios and security as an evolving concept;
- economics of security;
- ethics and justice.

The programme furthermore includes innovation support measures. Not all political, social and human research is relevant to nanotechnology applied to security. Most are more closely related to the implications of security policy for civil rights, and are targeted to policy issues. The recommended research topics 'ethical aspects of security technologies' and a 'review of existing codes of conduct, best practices, etc. as to the ethical use of security technologies and to develop new ones where shortfalls exist' are relevant to security applications of nanotechnology (ESRAB, 2006, p 60).

As part of the review of codes of conduct etc proposed by ESRAB, there is a pressing need to develop new European regulations for handling classified information in EU funded projects. These new regulations should include "clarification on the dual use of nano-derived technological devices for security purposes and full respect of human dignity and integrity" (Morrison, 2007). Furthermore, the concept of 'security technology' should be limited as much as possible, to avoid unnecessary restrictions to academic and trade freedom.

[32] www.paxchristi.net

The EU discussion and work in progress to regulate and develop privacy enhancing technologies must make good progress. There is a "need to incorporate ethical design from the start. This requires a multidisciplinary approach that involves not only scientists and technologists, but social scientists. For security RTD this is particularly important. … (There is a need for) the introduction of features in ubiquitous sensor networks to facilitate their removal when no longer required, and the enforcement of a minimum size" (Morrison, 2007).

The real demand for new security technologies (whether nanotechnology based or not) and non-technical options must be articulated in a public stakeholder debate. In such a debate, there is a need "to effectively discriminate between measured security and perceived security" (Morrison, 2007).

Care must be taken that new nanotechnology based security technologies respect existing legislation and civil rights. There is a "need to respect the autonomy of citizens and obtain consent with regard to protection of privacy, collection of data and its share for security purposes (anti-terrorism, judicial use, etc)" (Morrison, 2007).

## 5.6 Conclusions

In this chapter on societal implications of nanotechnology based security technologies, four questions have been discussed:

1. What is the existing regulatory and ethical framework relevant to nanotechnology based security technologies?

The Charter of Fundamental Rights of the European Union, several European directives, guidelines and international declarations cover legal and ethical aspects of nanotechnology based security technologies.

The main issue currently in debate is a proper balance between the rights to liberty and to security. Legislation and ethical guidelines for the protection of private and family life, home and communications; personal data protection; and equality and non-discrimination must be taken into account.

For some applications, the right to physical and mental integrity; and prohibition of degrading or inhuman treatment are valid.

All products must respect legislation aimed at protecting and enhancing environmental quality and consumer protection.

Research must balance academic freedom with responsible science and technology development. This includes a new balance between openness and handling classified information for security technologies.

2. What impact on ethics and human rights is expected from new nanotechnology based security technologies?

At present, potential impacts of nanotechnology based security technologies are still unclear. Proponents of security research expect security improvements for the European citizen, but they do not give evidence to corroborate this expectation. The eroding boundary between civil and military research may lead to unexpected security risks. Academic freedom and free trade may be restricted progressively. Some security technologies may not respect privacy and personal data protection legislation.

3. What is known about European public opinion of nanotechnology and of justice, freedom and security policies?

Many Europeans are more concerned with security than with privacy and freedom, according to a number of Eurobarometer surveys, however public awareness of security measures, security technologies and nanotechnology is low. This means that no conclusions can be drawn from opinion poles about the acceptance of the security policies or technologies used or under development.

Some NGO's have expressed concern about health, safety and environmental aspects of engineered nanomaterials and applications in sensitive consumer products such as cosmetics, washing machines and food. Other NGO's are concerned about privacy and human rights aspects of the information society, or with (military) arms control and disarmament. No NGO appears to have taken a position explicitly mentioning nanotechnology based security technologies.

4. What are the key issues for further research in social sciences and humanities, public debate and political decision making based on the analysis in this chapter?

ESRAB (2006) recommends research into 'ethical aspects of security technologies' and a 'review of existing codes of conduct, best practices, etc. as to the ethical use of security technologies and to develop new ones where shortfalls exist'. These are relevant to security applications of nanotechnology.

Research in social sciences and humanities must also contribute to the development of new Privacy Enhancing Technologies, and on criteria for assessing if new technologies respect citizens' rights and current legislation. Such research must also enable early identification of a need for new or adapted legislation.

Public debate must be organized to articulate public acceptance of security measures, technologies and nanotechnologies.

Political decision-making must focus on developing new European regulations for handling classified information in EU funded projects, and for regulating and standardising Privacy Enhancing Technologies. There is a need for a more fundamental debate about the right balance between civil and security research and technologies, in order to avoid unnecessary constraints on academic and trade freedom.

## 5.7 References


Comité 4 en 5 mei, "Nationaal Vrijheidsonderzoek 2007," (National Freedom Survey), http://www.4en5mei.nl/4en5mei/vrijheidsonderzoek/_rp_kolom2_2_elementId/1_110423

Commissie Criminaliteit en Technologie, "Technologie en Misdaad; kansen en bedreigingen van technologie bij de beheersing van criminaliteit", Commissie Criminaliteit en Technologie, Den Haag, January 2005, (Technology and Crime; opportunities and threats of technology in controlling crime) http://ejure.cust.iu.nl/downloads/dossier_id=246/id=215/show.html

Cordis FP7 webpages, "Getting through ethics review," 2007, http://cordis.europa.eu/fp7/ethics_en.html

Council of Europe, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe of 1 January 1981," www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm

EC Science & Society, "Ethics in EU projects," 2005, http://ec.europa.eu/research/science-society/page_en.cfm?id=3205

ESRAB, "Meeting the challenge: the European security research agenda; a report from the European Security Research Advisory Board, September 2006, European Commission, DG Enterprise, http://ec.europa.eu/enterprise/security/doc/esrab_report_en.pdf

EU, "Directive 95/46/EC of the European Parliament and of the Council of the European Union of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," Official Journal L281 23 November 1995, p 31-50, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:01995L0046-20031120:EN:NOT

EU, "Charter of fundamental rights of the European Union", 2000/C 364/01, Official Journal of the European Communities, Brussels, 2000, http://ec.europa.eu/research/science-society/page_en.cfm?id=3203

EU, "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector," http://eur-lex.europa.eu/LexUriServ/site/en/consleg/2002/L/02002L0058-20060503-en.pdf

EU, "A Secure Europe in a Better World; European Security Strategy" – presented by Javier Solana, EU High Representative for CFSP, adopted by the Heads of State and Government at the European Council on 12 December 2003

EU regulation on classified information

European Commission, "Eurobarometer 58.1," Oct/Nov 2002, http://ec.europa.eu/public_opinion/archives/eb/eb58/eb58_en.htm

European Commission, "Eurobarometer 64," Oct/Nov 2005, http://ec.europa.eu/public_opinion/archives/eb/eb64/eb64_en.htm

European Commission, "Eurobarometer 66," Oct/Nov 2006, http://ec.europa.eu/public_opinion/archives/eb/eb66/eb66_en.htm

European Commission, "Special Eurobarometer 244b: "Europeans and Biotechnology in 2005: Patterns and Trends",

European Commission, "Special Eurobarometer 266: The role of the European Union in Justice, Freedom and Security Policy Areas", DG Communication at the request of DG

Justice, Freedom and Security, Brussels, February 2007, http://ec.europa.eu/public_opinion/archives/ebs/ebs_264_en.pdf

European Commission, "Communication from the Commission to the European Parliament and the Council on the follow-up of the Work programme for better implementation of the Data Protection Directive," European Commission, Brussels, 7 march 2007, http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/com_2007_87_f_en.pdf

European Group on Ethics, "Ethical aspects of ICT implants in the human body", opinion no. 20, 16 March 2005, European Commission, http://ec.europa.eu/european_group_ethics/index_en.htm

European Parliament, "Resolution on security research – the next steps (2004/2171 (INI))," P6_TA(2005)0259, http://www.europarl.europa.eu/registre/seance_pleniere/textes_adoptes/definitif/2005/06-23/0259/P6_TA(2005)0259_EN.pdf

Group of Personalities in the Field of Security Research, "Research for a Secure Europe", European Commission, Luxembourg, 2003, http://ec.europa.eu/enterprise/security/doc/gop_en.pdf

Hof, C. van 't, "RFID & Identity management in the everyday life of European citizens: balancing convenience, control and choice in a new dimension of the digital public space," European Parliament, Brussels, expected in April 2007.

IAP, "IAP Statement on Biosecurity", Inter-Academies Panel, 2005, http://www.knaw.nl/nieuws/pers_pdf/IAP_Biosecurity_statement.pdf

Mordini, Emilio & Petrini, Carlo (eds), "Ethical and Social Implications of biometric identification technology," in Anali of the Instituto Superiore di Sanita, Vol 43, No. 1, 2007, http://www.iss.it/publ/annl/cont.php?id=2066&lang=1&tipo=3&anno=2007

Morrison, "Proceedings from the Nanotechnology and Security Workshop", Nanoforum, March 2007, www.nanoforum.org > Nanoforum reports

Netherlands' Government, "Actieprogramma Maatschappelijke sectoren en ICT (2005-2009)", (action programme societal sectors and ICT), http://www.e-overheid.nl/data/files/e-overheid/actieprogramma-maatschappelijke-sectoren-ict.pdf

OECD, "Guidelines on the protection of privacy and transborder flows of personal data," Paris, 23 September 1980, http://www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html

OECD, "Ministerial Declaration on the Protection of Privacy", Ottawa, Canada, 13 November 1998, http://www.oecd.org/dataoecd/39/13/1840065.pdf

PHR 2004, Threats to privacy, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-82586

PHR 2005, Threats to privacy, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-543674#_ftn835

Privacy International, "Leading Surveillance Societies in the EU and the World," in Daily Telegraph, 2 November 2006, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-545269

TWA Netwerk, "Security Technology Trends in the Netherlands", Ministry of Economic Affairs, Den Haag, 2007, http://www.twanetwerk.nl/upl_documents/TWA_Security_Engels.pdf

Vázquez Gallo, Enrique, Sánchez Ávila, Carmen, "Sistemas nacionales de identificación electrónica en el entorno europeo y norteamericano" [National systems of electronic identification in Europe and North America, with executive summary in English], Informe

de Vigilancia MadrI+D, Madrid, 2007, downloads 4.1 and 4.2 on http://www.madrimasd.org/tic/Informes/default.aspx

Vedder, A (et al), "Van privacyparadijs tot controlestaat", Rathenau Instituut, 2007, http://www.rathenau.nl/showpage.asp?item=2099

Wils, Jean Pierre, "Würde", in Düwell, Marcus, Hübenthal, Christoph, Werner, Micha H. "Handbuch Ethik. 2. Auglage", Metzler Verlag, Stuttgart, Weimar, 2007, pp 558-563

Wikipedia, "Human dignity", 2007, http://en.wikipedia.org/wiki/Human_dignity

WSIS, "Geneva Declaration of Principles," World Summit on the Information Society, Geneva, 2003, www.itu.int/wsis

Zhang, G.Q, Begeer, R, Hartman, R.A, "Point-One Strategic Research Agenda – Version 1 of detailed information on technology contents of Orange book," Point One, Eindhoven, 18 April 2007, www.point-one.nl

Zwenne, Gert-Jan, Duthler, Anne-Wil, Groothuis, Marga, Kielman, Hugo, Koelewijn, Wouter, Mommers, Laurens, "Eerste fase evaluation wet bescherming persoonsgegevens; literatuuronderzoek en knelpuntenanalyse," (1st phase evaluation personal dataprotection law) WODC, Ministry of Justice, Den Haag, 24 may 2007, http://parlando.sdu.nl/cgi/login/anonymous > search "nanotechnologie"

# 6 Conclusions

This report has described nanotechnology applications in civil security in three broad categories: detection, protection, and identification. In addition, it has described some of the ethical and societal concerns surrounding these applications and the organizations that are involved in this debate.

Civil security issues are becoming more important to governments across the globe, and the EU is no exception. The EC sees security research as an important policy objective, which started in 2001 with a Preparatory Action on Security Research (PASR) and now is the 10th Theme of the Collaboration programme of FP7. The Commission sees three important strands to security research enabling an increase in: industrial competitiveness; scientific research capabilities; and security for society. Although many of the technological advances described in this report were not originally designed for security purposes, they have demonstrated clear adaptation to such applications.

Civil security covers both physical and virtual aspects. Physical risks include the protection of individuals, property and critical infrastructure (such as emergency services, power and water supplies) from both intentional and natural damage and disruption. This can take the form of biological or chemical agents, projectiles, explosives, or other interference such as electromagnetic pulses. Applications can be at the level of detection (through various types of sensor, and surveillance equipment, as described in chapter 2), verification of identity (through biometrics for example) and protection such as filters, shielding and other forms of barrier (e.g. bullet-proof vests, as described in chapter 3). Identification and anti-counterfeiting measures (such as nano barcodes, chapter 4), support virtual security aspects such as identity and financial theft, and help prevent unauthorised access to systems and physical sites. Cryptography measures based on quantum effects are expected to massively increase the security of data transfer (chapter 4).

Civil security, however, is an area that raises many ethical and societal issues. The balance to be achieved by governments is between a secure environment for citizens where the risk from intentional or natural damage is minimised, and ensuring that personal freedom and civil rights are not compromised. Although many of the ethical and societal issues are not specific to nanotechnology applications, some will be heightened as a result of such developments (for example the development of ambient sensor systems). These issues were discussed in chapter 5.

The implications of nanotechnology developments for civil security were the theme of a recent workshop organized by Nanoforum in collaboration with the "Nano- Converging Sciences and Technologies" Unit of DG Research, and APRE (Agenzia per la Promozione della Ricerca Europea). Participants at the workshop discussed both the technological and societal issues surrounding research and its applications. A full report of the workshop is available from the Nanoforum website,[33] however the following specific recommendations were made:

**Technology issues**

- the creation of a repository of materials and research publications (particularly those arising from framework programmes) within the EU labelled by topic (e.g. "security"); in order to facilitate new research and continued development of existing materials by researchers. This could also include information regarding specific project deliverables; so that new research can take full account of what has been performed already (whether it has been published or patented or not,

[33] Proceedings from the Nanotechnology and Security Workshop http://www.nanoforum.org/nf06~modul~showmore~folder~99999~scid~452~.html?action=longview_publication&

and indeed whether it succeeded or not). This might take the form of a coordination or support action under the framework programme.

- the creation of an EU SME network to improve the fabrication of nanomaterials and devices relevant to security. For example the US and Japan have networks of academic centres and companies that facilitate access to materials and technology. This would support Europe's industrial competitiveness in the area of security RTD.
- research aimed at improving the basic analytical characteristics of bio-chemical sensing systems. Increasing sensitivity, overcoming interference (non-specific signals) and reducing response time are seen as critical features for improvement in sensor technologies, and their application in security, health and environmental areas.
- a systems-level approach to security research, integrating different projects and different expertise at each stage of the value chain.
- the development of easy-to-use devices and instruments for application in a variety of security scenarios. Here, of special interest are integrated systems (tailored for remote and embedded monitoring) with low power consumption that are capable of detecting a wide spectrum of agents and a wide range of concentrations with reduced probabilities of false or missed alarms.
- caution regarding patenting issues; as patents, particularly in this field, can be of limited usefulness.

**Societal issues**

- the need to incorporate ethical design from the start. This requires a multidisciplinary approach that involves not only scientists and technologists but social scientists. For security RTD this is particularly important.
- the need to effectively discriminate between measured security and perceived security.
- the introduction of features in ubiquitous sensor networks to facilitate their removal when no longer required, and the enforcement of a minimum size.
- the need to respect the autonomy of citizens and obtain consent with regard to protection of privacy, collection of data and its share for security purposes (anti-terrorism, judicial use, etc).
- clarification on the dual use of nano-derived technological devices for security purposes and full respect of human dignity and integrity.

It is clear that funding for security R&D will continue to grow (ESRAB has recommended that at least one billion euros be invested each year in specific security R&D within the EU, in addition to other research programmes which may produce applications for security). Nanotechnology developments have the potential to provide more sensitive, complete and rapid analysis of a variety of parameters that are important to maintaining a secure environment for citizens. These will not be achieved through conventional technologies. It can be expected therefore that the nanotechnology will contribute an increasing proportion of security R&D in the coming years.

# Appendix - EU organizations and projects

## Organizations

Amnesty International has a campaign on the Internet and Human Rights, fighting censorship and human rights violations by governments aided by Internet providers. (http://irrepressible.info/

Church of Scotland- Society, Religion and Technology Project. http://www.srtp.org.uk/nano01.htm

Consumentenbond, www.consumentenbond.nl

EDRI, European Digital Rights, is an association of 25 European privacy and civil rights organisations. They campaign for defending civil rights in the Information Society (http://www.edri.org/).

E-Jure, Knowledge Centre for ICT and Law, dossier nanotechnologies: http://ejure.cust.iu.nl/dossier_id=246/f_dossier/dossier.html

ENIAC, European Nanoelectronics Initiative Advisory Council, http://www.eniac.eu/index.php

ESRAB, European Security Research Advisory Board. Prepared the European Security Research Agenda, September 2006, http://ec.europa.eu/enterprise/security/doc/esrab_report_en.pdf

ESRIF, European Security Research and Innovation Forum, established during the European Security Research Conference, Berlin, 26-27 March 2007, http://cordis.europa.eu/fetch?CALLER=FP7_NEWS&ACTION=D&RCN=27387

EUROCONTROL, European Organisation for the Safety of Air Navigation. http://www.eurocontrol.int/corporate/public/subsite_homepage/index.html

Forum Internet: an online discussion forum on ICT and society in France. It organized a debate on the electronic national identity card in 2005. http://www.foruminternet.org/

Meldpunt Misbruik Identificatieplicht

Ministry of Justice, Innovatieplatform Technologie en Criminaliteitsbestrijding (Innovation platform technology and crimefighting), installed in 2006

Pax Christi International is an international Peace Movement lobbying for disarmament and arms control with the relevant UN and European organisations (www.paxchristi.net).

Point-One, Pole de Competitivité Nanoelectronics www.point-one.nl

Privacy International: an NGO campaigning against intrusions of privacy worldwide. www.privacyinternational.org

Rathenau Institute, Screening Society project, www.rathenau.nl

TILT, Tilburg Institute for Law, Technology and Society, specialises in legal issues of new technology including nanotechnology, http://www.uvt.nl/faculteiten/frw/onderzoek/schoordijk/tilt/

TNO, Security and Safety department, http://www.tno.nl/groep.cfm?&context=markten&content=markt&laag1=194&item_id=194&Taal=2

## Projects

AMICOM: "Network of Excellence on RF MEMS and RF Microsystems". http://www.amicom.info/index.php

DINAMICS: "Diagnostic Nanotech and Microtech Sensors". Developing an exploitable lab-on-chip device for detection of pathogens in water supply systems. April 1st 2007 – March 31st 2011. Coordinator: Dr Christian Mittermayr, Lambda GmbH, Austria.

L-SURF: Design study for a large scale underground research facility on safety and security, SSA, 1 March 2005 – 29 February 2008, project leader Volker Wetzig, Hagerbach Test Gallery, Ltd, Switzerland, includes sensors based on nanotechnology, http://cordis.europa.eu/fetch?CALLER=FP6_PROJ&ACTION=D&DOC=1&CAT=PROJ&QUERY=1174651098303&RCN=74861

MOREPOWER: Compact direct (m)ethanol fuel cell for portable application, SUSTDEV, 1 February 2004 – 31 January 2007, project leader Suzana Pereira Nunes, Forschungszentrum Geesthacht, Germany, the fuel cells may be incorporated in a.o. security camera's, http://cordis.europa.eu/fetch?CALLER=FP6_PROJ&ACTION=D&DOC=11&CAT=PROJ&QUERY=1174651098303&RCN=73962

NANOS4: Nano-structured Solid Gas Sensors with superior performance, NMP, 1 January 2004 – 31 March 2007, project leader Giorgio Sberveglieri, INFM, Italy, new sensors for health, safety and security of people and the environment, http://cordis.europa.eu/fetch?CALLER=FP6_PROJ&ACTION=D&DOC=3&CAT=PROJ&QUERY=1174651098303&RCN=74321

NANOSECURE: "Advanced nanotechnological detection and detoxification of harmful airborne substances for improved public security". Developing systems that can be widely deployed for early warning and detoxification of harmful airborne substances with far higher efficiency than current methods. March 1st 2007 – February 28th 2011. Coordinator: Neil Wright, C-Tech Innovation Ltd, Chester, UK.

NEED: Nano-Engineering for Expertise and Development, developing R&D and strategies for Reactor and Nuclear Fuel Safety, Marie Curie action, 1 July 2004 – 30 June 2008, project leader Marek Szymonski, Jagiellonian University, Poland, http://cordis.europa.eu/fetch?CALLER=FP6_PROJ&ACTION=D&DOC=2&CAT=PROJ&QUERY=1174651098303&RCN=70968

PEARL: Privacy Enhanced security architecture for RFID labels, STW, period January 2006- October 2010, project leader S. Etalle, CTIT, University of Twente, Netherlands, http://www.onderzoekinformatie.nl/nl/oi/nod/onderzoek/OND1318897/

PHOREMOST: Nanophotonics to realise molecular scale technologies, IST, 28 September 2004 – 30 September 2008, project leader Clivia Sotomayor Torres, University College Cork, Ireland, potential applications include security, http://cordis.europa.eu/fetch?CALLER=FP6_PROJ&ACTION=D&DOC=13&CAT=PROJ&QUERY=1174651098303&RCN=71854

SELECTNANO: Development of Multifunctional Nanometallic Particles using a new process: sonoelectrochemistry, NMP, 1 March 2005 – 29 February 2008, project leader Aharon Gedanken, Bar Ilan University, Israel, potential industrial applications include security and anti-fraud labelling and authentication, http://cordis.europa.eu/fetch?CALLER=FP6_PROJ&ACTION=D&DOC=9&CAT=PROJ&QUERY=1174651098303&RCN=75845

TERAEYE: "a low cost and fully passive Terahertz inspection system based on nanotechnology for security application". Developing an innovative range of systems, based on Terahertz (THz) wave detection, to detect harmful materials for homeland security. Coordinator: Valerio Pagnotta, Comerint Engineering, Rome, Italy.