



Economic Analysis of Nanotechnology for Security Applications

Table of Contents

Executive Summary.....	4
1. Methodology.....	5
1.1. Definition	5
1.2. Methodology for Preparing the Report	5
1.3. Methodology for Quantitative Assessment.....	5
2. General Market Description	6
2.1. Brief Market Description	6
2.2. Nanotechnology Impact	8
2.3. Drivers and Barriers to Innovation.....	9
2.3.1. Drivers of Innovation.....	9
2.3.2. Barriers to Innovation	10
2.4. Relevant Sector Segmentation and Applications	11
2.5. Possible Future Products and Time Range.....	11
3. Application Profiles.....	13
3.1. Detection of Chemical, Biological, Radiological, Nuclear, Explosives (CNRNE)	13
3.1.1. Short application description	13
3.1.2. Functional requirements	15
3.1.3. Boundary conditions.....	16
3.1.4. Product examples.....	16
3.1.5. Economic Information and Analysis	17
3.1.6. Selected Key Companies Profiles.....	17
3.2. Anti-counterfeiting and Authentication	19
3.2.1. Short application description	19
3.2.2. Functional requirements	20

3.2.3.	Boundary conditions.....	22
3.2.4.	Product examples.....	22
3.2.5.	Economic Information and Analysis	22
3.2.6.	Selected Key Companies Profiles.....	23
3.3.	Forensic Analysis (Fingerprint Detection).....	24
3.3.1.	Short application description	24
3.3.2.	Functional requirements	24
3.3.3.	Boundary conditions.....	24
3.3.4.	Product examples.....	24
3.3.5.	Economic Information and Analysis	25
3.3.6.	Selected Key Companies Profiles.....	25
4.	References	26

Executive Summary

This report looks at the economic impact of nanotechnology for ‘homeland’ or civil security applications, excluding military applications. Three applications are considered in more detail; Detection of Chemical, Biological, Radiological, Nuclear, Explosives (CBRNE),

Estimates of the size of the global security market range from €30bn to €50bn. Drivers to innovation include new security threats - particularly terrorism - public procurement, and a high research intensity of security firms. This report uses the ESRAB security framework, considering missions (border control, protection against terrorism and organised crime, critical infrastructure protection, and restoring security in case of crisis) and capabilities. Nanotechnology could potentially impact several capabilities; CBRNE detection, stand-off scanning, materials for blast and impact protection, and marking, tracking and tracing of components.

Nanotechnology applications in detection of CBRNE include conductive polymers for chemical detection, vertically aligned carbon nanotube arrays functionalised to react to the presence of biological substances, and scintillators for detection of radioactive materials. Functional requirements of detection technologies include reliability, sensitivity, stability and cost. Existing products include portable chemical detectors which employ a Field Asymmetric Ion Mobility Spectrometry (FAIMS) chip, produced by Owlstone Nanotech. Other companies working in this area include Xintek, Kromek, ICx Technologies and Nanōmix.

Anti-counterfeiting and authentication technologies are intended to ensure that a physical product is genuine. Nanotechnology-based approaches to this need include laser surface authentication and magnetically patterned tags, which are capable of satisfying the functional requirements of uniqueness, replicability, and appropriate total cost. Companies developing products in this space in SingularID, Ingenia, DataDot Technology, and Oxonica Security.

Technologies with an impact on forensic analysis are currently at a very early stage of development, though a UK-based company has developed a method which uses nanoparticles to bind to the chemical residues that compose a latent fingerprint. These can be used to both enhance the quality of the recovered fingerprint pattern, and to derive additional information – such the presence of narcotics in the bloodstream of the fingerprint owner. This work is still at a development stage, and there are believed to currently be no commercially available nanotechnology-based solutions in this area.

1. Methodology

1.1. Definition

For the purposes of this report, nanotechnology is defined as “the study of phenomena and fine-tuning of materials at atomic, molecular and macromolecular scales, where properties differ significantly from those at a larger scale.”¹

The specific focus of this report is on applications of nanotechnology in security, including identification, detection and protection. This report does not cover uses of nanotechnology in weaponry or other offensive military applications.

1.2. Methodology for Preparing the Report

The development of this report has been a three stage process. Desk research using publicly available sources of information was used to produce a first version of this report. Input and feedback is then sought from experts, via questionnaires, interviews and discussions, and from the ObservatoryNano symposium which takes place in March 2009. A final report is then produced, which synthesises the desk research and external expert input.

1.3. Methodology for Quantitative Assessment

Quantitative assessments of market size, growth rates, and the current market shares of nanotechnology enabled products are developed using external data sources such as market research providers, industry groups, and individual experts. Estimates and market size projections that are made by the authors of this report are clearly marked as such.

All forward looking estimates are necessarily a projection, and are therefore subject to error within the market models themselves, as well as to unforeseen external events. In particular, the current economic crisis has forced countries and companies to significantly adjust their growth forecasts – in most cases, this will not have been taken into account in projections which date from before 2008.

¹ Introduction to Nanotechnology, http://ec.europa.eu/nanotechnology/index_en.html

2. General Market Description

2.1. Brief Market Description

From the European Security Research Agenda²:

Since the end of the Cold War, the threat of large-scale military aggression has subsided and been substituted by new threats which are multifaceted, interrelated, complex and increasingly transnational in their impact. These were laid out in the European security strategy to include organised crime, terrorism, state failure, regional conflicts and proliferation of weapons of mass destruction.

This array of new security threats has re-shaped the security industry, essentially unifying previously disparate elements such as customs and border control, policing, emergency response, and critical infrastructure protection under the name ‘civil’ or ‘homeland’ security. The ESRAB report groups these elements by mission³, which include:

- Border Control
- Protection against terrorism and organised crime
- Critical Infrastructure Protection
- Restoring Security in Case of Crisis

Civil security also represents a market for a wide range of technologies and services, from detection of harmful substances to forensic investigation.

Estimates of the size of the security market range from €30bn to €50bn. The CEO of Thales is quoted as saying that it is believed to be between 30 and 35 billion Euros, of which 25% (€7.5bn - €8.75bn) is in Europe⁴. This equates to roughly 0.07% of European GDP. Epoc Messe Frankfurt

² Meeting the challenge: A European Security Research Agenda, Report from the European Security Research Advisory Board, September 2006

³ Meeting the challenge: A European Security Research Agenda, Report from the European Security Research Advisory Board, September 2006

⁴ http://uk.reuters.com/article/UK_SMALLCAPSRPT/idUKN1451503520080514?sp=true

GmbH (organisers of the Intersec conference), project that homeland security revenues will reach \$178bn (€142bn) by 2015. This projection places the current global market value at nearer €47bn.

The German Ministry for Education and Research, in its Research for Civil Security programme, has placed the value of the German market for security technology and services at “€10bn in 2005, with growth rates of 7%-8%⁵.” The variation in market size estimates is likely due to the difficulties in drawing the boundaries of this market; the US definition of homeland security only includes activities like policing and fire services in so far as they come under ‘disaster response’.

Reliable estimates of the number of people employed in the security industry in Europe are similarly varied. In terms of direct employment impact, Thales, for example, one of the largest European security industry firms, has 19 323 employees in its security business in 2007, of which well over half were based in the European Union.

The security industry is also an area in which Europe-headquartered companies play an important role, with leading industrial players including EADS, BAE Systems, Finnmechanica and Thales.

⁵ Research for Civil Security, Programme of the German Federal Government, 2007, http://www.bmbf.de/pub/research_for_civil_security_.pdf

2.2. Nanotechnology Impact

Nanotechnology has the potential to impact a number of security applications. ESRAB looked at technology development in terms of the capabilities required to perform specific missions. Taking protection against terrorism and organised crime as an example, the capabilities required include:

1. Detection, Identification and Authentication
 - a. Drugs, Explosive, CBRN (Chemical, Biological, Radioactive, Nuclear) detection
 - b. Stand-off scanning
2. Information Management
3. Risk Assessment, Modelling, Impact Reduction
 - a. Develop ballistic, blast, impact reducing measures for existing infrastructure
 - b. Develop protection against contaminants in buildings
4. Positioning and Location
 - a. Observation through walls, metal, etc.
 - b. Marking, tracking, tracing of components for substance production
5. Situation Awareness and Assessment

Note that this is an abbreviated list. There are over 30 capabilities required for this mission – this list highlights those most affected by developments in nanotechnology. A number of these capabilities also apply to other missions; CBRNE detection is also a capability required for a border control mission, for example.

CBRNE detection is one of the capabilities which may be enhanced with nanotechnology. This is covered in more detail in chapter 3.1 but briefly, developments in chemical sensing are likely to include optical fibres, cantilever-based sensors, chemresistors using carbon nanotubes, and chemicapacitive sensors, to mention just a few. These will enable more accurate detection, smaller devices, lower cost production, and ultimately single platform detection of multiple substances.

2.3. Drivers and Barriers to Innovation

2.3.1. Drivers of Innovation

New Security Threats

As previously stated, the emergence of new or increased security threats has significantly changed the security landscape. To take one example, the risk that weapons of mass destruction fall into the hands of terrorists or criminal gangs will only be solved on a policy level – increasing international cooperation and information sharing – but the risk can be mitigated to some extent by new technology. The ability to scan every vehicle at a border crossing would allow the interception of this material, but to avoid disproportionate economic costs, this would require high-throughput screening, high accuracy with low false positive rates, and a reasonable total cost of deployment and use.

The Role of Government

The mechanism by which these new security threats drive innovation highlights the role of government. New security market needs are often a direct result of government policy; new regulations for airport security or quality standards for the national water supply necessitate the development of new scanning equipment and monitoring tools.

Government also creates security markets through public procurement. The UK's e-Borders project, which has a budget of GBP 1.2bn, aims to join up the various UK border control systems in order to provide 'an intelligence led approach to operating border controls'.⁶ A substantial element of this project for the development of these information systems was awarded to the Trusted Borders consortium, led by Raytheon. This in turn requires the development of technologies for collecting and record biometric data from UK residents and visitors.

Military procurement also drives the development of technologies for civil security. A number of the technologies in this domain are dual use; a chemical weapons detector developed for the military could also have applications in detection of harmful substances in the civilian sphere.

⁶ http://www.trustedborders.com/press_release_14_11_07.shtml

Research Intensity of Firms

The 'Aerospace and Defence' industry (which is not the same as the security industry, but has significant overlaps) spends an average of 4.9% of its turnover on research and development. Whilst this is behind healthcare (13.4%) and electronics (7%), it is substantially ahead of the automotive industry, general industrials, consumer goods, chemicals and energy.

The historical reason for this is that the industry was expected to generate a military advantage for its customer by developing technology which was substantially more capable than alternatives. In terms of civil security, it is still the case the products are likely to be developed to the specifications of particular customers. Governments often understand that the technologies that they are procuring are not 'off-the-shelf' and require development

2.3.2. Barriers to Innovation

Fragmented Market

The corollary to the centrality of governments is that this renders the security market highly fragmented. The bulk of security policy and procurement is still handled by national governments, which are likely to generate different requirements, to have differing budgets, and generally render it difficult to scale security technology. Whilst some large players can be identified (such as the FBI, Border Control or Custom agencies) for the most part this market is divided into local or regional emergency services, ports and airports, and public transport systems.

Preservation of Civil Liberties

As Industry Commissioner Günter Verheugen states, "We must enhance security but we must also avoid 'big brother is watching you' solutions."⁷ There is a very understandable concern amongst civil society about the development of security technologies, particularly those which are perceived to be more invasive. This category includes sensing and scanning technologies which are capable of passively scanning a crowd or area – without someone necessarily knowing that they are being observed.

⁷ <http://www.euractiv.com/en/science/eu-security-research-seeks-respect-civil-liberties/article-175851>

Societal acceptance can be improved if the technology can demonstrate effectiveness in proportion to the threat posed; people are willing to sacrifice a degree of privacy if they can be convinced that it is necessary (and allowed to make an informed choice).

2.4. Relevant Sector Segmentation and Applications

The first year economic report looks at three applications of nanotechnology for civil security:

- CBRNE Detection
- Anti-Counterfeiting and Authentication
- Forensics (Fingerprint Analysis)

These broad application categories have been chosen as the most appropriate point at which to describe the impact, requirements and current products that are enabled by nanotechnology. Each of these areas has more specific end user applications: e.g. CBRNE detection for ports. These may be considered in more detail in future years.

2.5. Possible Future Products and Time Range

Application	Commercially Available	1-3 years	3-5 years	5+ years
CBRNE Detection	A number of products which use Raman or Field Asymmetric Ion Mobility Spectrometry (FAIMS) are currently available.	Explosive sensors using conductive polymers	Cantilever-based explosive sensors	Integrated single platform detection.
Anti-Counterfeiting and Authentication	SingularID's tags are commercially available. Laser Surface Authentication is believed to be commercially available.		Material for identification documents (it is not clear how actively this research is being pursued)	
Forensics (Fingerprint)		Trials of functionalised nanoparticles as		

Analysis)		fingerprint powder replacements are currently underway		
------------------	--	--	--	--

3. Application Profiles

3.1. Detection of Chemical, Biological, Radiological, Nuclear, Explosives (CNRNE)

3.1.1. Short application description

This application area specific considers approaches to the detection of harmful substances associated with a security threat, such as a chemical or biological agent.

Current solutions to this involve a range of machines and technologies. Detection of explosives residue is typically carried out by swabbing the item to analysed, and then processing this sample with an ion mobility spectrometer. This can be configured to not only detect explosives, but also traces of narcotics⁸. Explosives detection trace portals (or ‘puffers’) use a non-contact method, blowing particles which are then analysed using ion mobility spectrometers. These are currently produced by Smiths Detection and GE Infrastructure, and can be found at a number of airports and other high profile locations.

Identification of chemical agents (whether chemical weapons or toxic chemicals) typically requires another device. The detection mechanism may be IMS or Fourier Transform Infrared Spectroscopy. Devices in a variety of forms are available, from handheld units for first responders, to units which are intended for continuous monitoring of a given location. The technology used for detection of biological agents often uses Polymerase Chain Reaction (PCR) and is also available in portable forms.

This is an area of high interest, particularly for governments, and there is a wide range of research work being carried out this area. Nanotechnology offers the possibility to make smaller, more sensitive and integrated detection platforms for each of these substances. These could typically be used in transit points like airports, train stations, seaports and borders to prevent the transport of CBRNE material.

Chemical Detection

A very wide array of technologies are being considered for detection of chemicals, including conductance sensors and conductive polymers, field effect transistors, piezoelectric sensors, field

⁸ http://www.smithsdetection.com/eng/IONSCAN_400B.php

effect transistors, piezoelectric sensors, surface acoustic wave sensors, flexural plate wave sensors, sensor arrays, optical fibres, cantilever mechanism, chemiresistive sensors, chemicapacitive sensing and spectroscopic methods. For more detailed descriptions of these approaches, please go to <http://www.observatorynano.eu/project/document/890/>.

Detection of Biological Substances

Work being carried out in the healthcare industry on the detection of pathogens, toxins and other substances has applications in civil security. One of the primary events triggering concern about the weaponization of biological substances were the anthrax attacks of 2001, in which anthrax spores were sent by mail to US media outlets and senators, resulting in the deaths of five people.

Nanotechnology-enabled detection methods include the use of metallic nanowires, to which are attached antibodies corresponding to specific pathogens. Fluorescent antibodies are then added, which bind to any pathogens which are present. Measurement of the fluorescence then indicates the presence and concentration of pathogens.

A sensor developed by NASA uses an array of vertically aligned carbon nanotubes, each tipped with a probe molecule. When the probe molecule comes into contact with a target substance, an electrical impulse is generated. A variety of different probing molecules can be used, enabling a single array to detect multiple substances.⁹

Detection of Radioactive and Nuclear Material

A detection technology which nanotechnology may improve is the use of scintillators; materials which emit photons when exposed to radiation. Materials including zinc oxide nanoparticles may work as scintillators but demonstrate improved energy resolution.¹⁰

Detection of Explosives

Explosive detection can be achieved with ion mobility or Raman spectroscopy. A group led by Anja Boisen at DTU Nanotech is developing explosive sensors which use a range of detection methods, including SERS, cantilever sensors, micro calorimetric sensors and colorimetric sensor

⁹ <http://www.usmedicine.com/dailyNews.cfm?dailyID=399>

¹⁰ <http://www.azonano.com/news.asp?newsID=1771>

arrays¹¹. The cantilever sensors measure changes in surface stress, temperature or mass to detect gases (as well as antibodies and proteins). Timothy Swager at MIT has developed methods to identify TNT using electronic polymers; this technology is being commercialised by Nomadics.

3.1.2. Functional requirements

The specific functional requirements of the detection of CBRNE substances depend heavily on the specific substance being targeted, and the environment in which sensing will be carried out. However, these general functional requirements are common to almost all applications.

Reliability

The reliability of a detection device describes the extent to which it generates false positive or false negative results. Whilst the consequences of a false negative result can be very severe, it is important to note that excessive false positives also have a cost, requiring investigation and response.

Sensitivity

The sensitivity of a device is often expressed as the quantity of a substance required to generate a detection result. This is measured in parts per million (PPM) or parts per billion (PPB). The target sensitivity depends on the substance being detected; in the case of anthrax, a single spore can be deadly, and so this should be the target sensitivity threshold.

Stability

Stability relates to the consistency of detection performance in a range of environmental conditions – such as differing temperatures, vibrations, shocks.

¹¹ http://www2.imm.dtu.dk/pubdb/views/edoc_download.php/5643/pdf/imm5643.pdf

Cost

The cost of a detection device, in relation to its lifetime and effectiveness, is a critical factor. An explosive detection sensor for an airport is likely to be in constant use, and thus a higher cost can be amortised over a longer time period and a greater number of operations. A node in a distributed sensor network, which may need to be replaced more regularly, should typically have a lower per piece cost.

Response Speed

The speed with which a detector operates is an important factor in many applications. If a harmful substance is present, it should be detected in time to mitigate its effects; to order an evacuation, or to stop a vehicle carrying dangerous material.

Power Consumption

Devices which are not connected to mains supply, such as portable detectors, also require low power consumption.

3.1.3. Boundary conditions

Most of the detection applications described in this chapter occur outdoors, and so the detection technology must withstand a range of environmental conditions, including high and low temperatures, direct sunlight, wind and rain.

3.1.4. Product examples

Early Warning Biohazard Water Analyzer

This device uses the nanotube detection technology developed by NASA and described in section 3.1. Due for release in April 2009, the Analyzer will detect waterborne microorganisms, including E.coli and Cryptosporidium.

P.Eye Explosives Detector

Launched in February 2009, the P.Eye detector is designed by Portendo. The device utilises Raman spectroscopy to identify explosive substances, and is designed for 'stand-off' use, in which a laser beam is used to detect substances from some distance away.

Nexsense C

The Nexsense C¹², produced by Selex Galileo, is a portable chemical detector which uses Field Asymmetric Ion Mobility Spectrometry (FAIMS). The FAIMS detector is produced by Owlstone Nanotech.

Fido[®] Explosives Detector

The Fido[®] detector is sold by ICx Technologies, and uses amplifying fluorescence polymers (AFP) to detect explosives in concentrations of parts per quadrillion (ppq). This technology is developed from Timothy Swager's work at MIT. The device itself weighs 3 pounds (1.5 kg), making it highly portable. (The device is named as a nod to the explosives sniffer dogs, which have a comparable sensitivity to explosive traces).

3.1.5. Economic Information and Analysis

Taking a limited definition of nanotechnology-enhanced detection for security applications, the value of current products is likely to be rather small, in the range € 1- 20 million. This is difficult to establish definitively; no market studies have been carried out, and few of the companies report their revenues publicly.

3.1.6. Selected Key Companies Profiles

Owlstone Nanotech

Owlstone (<http://www.owlstonenanotech.com/site.php>) started life as a spin-off from the University of Cambridge, and is now a wholly-owned subsidiary of Advance Nanotech. The company has developed a Field Asymmetric Ion Mobility Spectrometry (FAIMS) detector which is created with a replicable silicon etching process. The FAIMS chip enables simultaneous detection of a range of substances.

¹² http://www.owlstonenanotech.com/PDF/NEXSENSE_C_Dsh55.pdf

Nanōmix

Nanomi (<http://www.nano.com/>) has developed a detection chip which employs a random network of CNTs, functionalised with specific analytes. The company's NanoTect™ environmental monitors claim to be able to detect low concentrations of gases. The main application is considered to be industrial use, rather than security. Nanomi received a grant totalling \$1.26 Million from the Department of Homeland Security in 2007.

ICx Technologies

ICx (<http://www.icxt.com/>) has also developed a detection chip which uses functionalised CNTs. One of its subsidiaries, Sensiq (<http://www.discoverensiq.com/products/sensiq/>) has developed a detector for liquid explosives (hydrogen peroxide and triacetoneperoxide) and a TNT detector which uses a semiconducting polymer film, developed by Timothy Swager¹³.

Xintek, Inc.

Xintek (<http://www.xintek.com/>) develops a variety of nanotech based field emission technologies, including a x-ray source. The company has a joint venture with Siemens for medical detection.

Kromek

Kromek (<http://www.kromek.com/>), formerly Durham Scientific Crystals (DSC), develops Cadmium Telluride based x-ray detectors. The company supplies material to the European Space Agency (ESA), and has evolved from CdTe materials to produce sub-assemblies and end-user products. The company had 38 staff in 2008.

¹³ A Better Liquid-Explosives Detector

http://www.technologyreview.com/read_article.aspx?id=17846&ch=nanotech&a=f

3.2. Anti-counterfeiting and Authentication

3.2.1. Short application description

Anti-counterfeiting and authentication technologies are intended to ensure that a physical product is genuine and not a copy. Fake goods have a substantial economic cost, in terms of lost sales of genuine clothing, music or films. In the case of engine parts or medicine, fakes may also be life-threatening.

Oxonica, which has a subsidiary working on authentication technologies, reported that counterfeiting led to lost revenues of €600bn in 2003. At a European level, the company claims that this led to a loss of €65bn, or the equivalent of 200,000 jobs¹⁴. (Note that the methodology used to reach these estimates is not wholly reliable; not every fake good sold represents the loss of a sale of a genuine good).

These technologies may also be used to identify as unique instances of an item, in addition to item classes. For example, a product may be able to be authenticated as being from a particular manufacturer or factory, but also as being a specific item produced at a certain time and date. Identifying a unique item could also involve identifying its location, as with RFID.

Laser Surface Authentication

One application of nanotechnology to this problem is laser surface authentication. This involves taking an image of the surface of an object and storing this pattern as a code. This leads to almost completely unique coding – the chances of two pieces of paper having the same surface features a 1×10^{72} .

Physical Unclonable Function

A technology developed by Philips Research, PUP involves the combination of information about a physical layer, cross referenced to a digital signature, with both required for successful authentication.

¹⁴ Oxonica, http://www.oxonica.com/security/security_intro.php

Magnetic Methods

Singular ID has developed a technology which involves integrating a random pattern of magnetic material into a tag – one of the benefits being that the tag itself could be made of a variety of materials such as plastic, metal or glass. The magnetic pattern, unique to each tag and with sufficient variability to enable identification of billions of items, can then be read using the giant magnetoresistance (GMR) effect, also employed in hard drive read heads.

Oxonica also employs a material which is capable of storing a unique magnetic pattern; in this case ‘striped’ magnetic rods of sub-micron lengths.

Surface Emission Raman Scattering (SERS)

Nanoplex, acquired by Oxonica in 2005, has developed biomarkers based on gold nanoparticles. These nanoparticles exhibit exponentially increased scattering efficiency, and when combined with reporter molecules adhered to their surface, can be designed to return a distinct SERS spectrum. These tags are nanometer-scale, robust, and are able to be read by handheld raman detectors¹⁵.

Document Materials

Another application of nanotechnology is to make materials for identification documents, which are hard to replicate and can be used to store additional material. A group at the University of Toronto had developed a three layer sandwich of polymer films (containing anthracene, NBD and Nile Blue), and were able to store an item of biometric data on each of the layers.

3.2.2. Functional requirements

Secrecy

As a safeguard against being compromised, the security competent should be as far as possible undetectable. In some cases it may be worthwhile to combine a visible security element as an obvious deterrent, whilst also including a hidden security component.

¹⁵ Going for the Gold: Multiplexed Optical Detection Tags Based on SERS-Active Gold Nanoparticles, http://www.oxonica.com/get_file.php?file=45_1_perspective_nb0207.pdf&cat=press_articles

Uniqueness

To identify a specific product, there must be a very low chance that the identifying element would occur in another tag or item. In practice this means that an identification element should have a less than a billion to one likelihood of appearing again by chance.

Replicability

To provide robust security, the identifying element should not be able to be recreated outside of the system that originally created it.

Systems Integration

Any system is only as secure as its most insecure point. Whilst the identifying methods themselves may be almost impossible to replicate, similar care must be taken to ensure that interrogation methods and identifier databases are equally as hard to compromise.

Cost

The expense of an authentication system is clearly an important factor, especially when considering goods which are made in quantities that reach hundreds of millions. From this perspective, technologies such as laser surface authentication that don't require adding anything to the product itself may be more cost effective. Costs may also be incurred by authentication methods which add extra steps or reduce the speed of a production process.

Privacy

Privacy considerations should also be taken into account. In general, only information which is needed to authenticate the product should be collected, and not information about the product in use.

Ease of Use

The difficulty of using the identification feature should be in proportion to the frequency with which it would need to be identified. Aircraft parts could conceivably require specialised identification equipment, but consumer goods would require an easy, portable solution.

Flexibility of Application

This chapter has already discussed a wide range of items which may need to be indentified, each of which has a variety of form factors and materials. A universal identification method would need to be able to be used in each of these applications.

3.2.3. Boundary conditions

A tracking system must return unique results, with sufficient variation to avoid repetition of codes and results.

3.2.4. Product examples

SingularID's Enxure

Enxure is a security system which includes tags with a random assortment of magnetic features, and a handheld scanner (which can be connected to a mobile phone or computer). The tags can be attached to a label or incorporated within a product itself.

Sol-ID™ by Oxonica Security

Sol-ID™ biomarkers are functionalised gold nanoparticles which provide distinct spectral signatures. Oxonica claims that the particles can be applied during normal printing methods.

3.2.5. Economic Information and Analysis

Current sales of nanotechnology-enabled products in the authentication market are likely to be around €10M. As a listed company, Oxonica is one of the few firms in this space that reveals its revenue. In 2007, the company's security division recorded sales of £490k (€550k – though note significant devaluation of the British Pound since 2007). The company additionally recorded orders valued at \$2.15M (€1,72M) for delivery in 2008¹⁶.

DataDotTechnology Limited recorded sales of AU\$ 5,301,564 (€2.7M) in 2008.

¹⁶ Oxonica Interim Result, 22/09/2008

<http://www.londonstockexchange.com/LSECWS/IFSPages/MarketNewsPopup.aspx?id=1964603&source=RNS>

3.2.6. Selected Key Companies Profiles

Singular ID

SingularID (<http://www.singular-id.com>) sells the Enxure security system, a combination of magnetically patterned tags and a scanner. The company was acquired by Bilcare on 7th January 2008 for 19,58M Singapore Dollars (approximately 10 M€)

Ingenia Technology Limited (ITL)

Ingenia (<http://www.ingeniatechnology.com>) develops Laser Surface Authentication (LSA) technology for product authentication. The company's technology is based on work carried out by Russell Cowburn at Imperial College London.

DataDot Technology Limited / Data Trace DNA

DataDot Technology (<http://www.datadotdna.com>) is listed on the Australian stock exchange with the ticker symbol DDT. DatatraceDNA is a joint venture between DataDot and CSIRO, and develops nanoparticles which can be added to a product during manufacture (or applied as a lacquer) and which then enable authentication of the substance.

Oxonica Security

Oxonica (http://www.oxonica.com/security/security_intro.php) develops SERS tags, which have applications as a biomarker and in brand protection systems.

3.3. Forensic Analysis (Fingerprint Detection)

3.3.1. Short application description

Incident support mainly involves requirements which occur after a security incident has taken place. These include forensic investigation, and neutralisation and decontamination following a chemical, biological, radioactive, nuclear or explosive (CBRNE) incident.

A specific application of nanotechnology is its use to improve fingerprint recovery. Latent fingerprints are formed by a chemical secretion from the fingertips. Nanoparticles or quantum dots could be designed to bind to these secretions, revealing the fingerprint in greater detail, and increasing the chance of matching it. A group in Sunderland in the UK has developed sol gel particles which use fluorescent dyes such as Texas red, increasing the quality of the recovered fingerprint.

3.3.2. Functional requirements

Functional requirements for forensic analysis include:

Ability to develop fingerprints. The substance used to capture latent fingerprints should be capable of binding to eccrine gland secretions, or acting as reagents to these substances to enable an image of the fingerprint to be taken.

Chemical analysis of fingerprint residue. The secretions left in a latent fingerprint can also convey information about the body of the owner, such as whether they have traces of narcotics in their bloodstream.

3.3.3. Boundary conditions

The method used should enable the capture of a fingerprint with as much ridge detail as possible, thus increasing the chances that the fingerprint owner will be identified. The capture method should also enable the reliability and validity of forensic testing, by providing consistent results.

3.3.4. Product examples

No commercial products are available at this time.

3.3.5. Economic Information and Analysis

No commercial products are available at this time.

3.3.6. Selected Key Companies Profiles

ROAR Particles

ROAR Particles (<http://www.roarparticles.com/>) technology was developed by Professor Frederic Rowell at the University of Sunderland. The company's products are a replacement for fingerprint dusting powders, enabling more accurate fingerprint definition, and identification of chemicals and metabolites in latent fingerprints.

The company appears to be working with Nanotechnology Victoria to pilot the use of these nanoparticles with Australian law enforcement agencies¹⁷.

¹⁷ Forensic Science in Australia, Nanotechnology Victoria,
http://www.nanovic.com.au/?a=industry_focus.forensics

4. References

Role of nanotechnology in brand protection

<http://profitthroughinnovation.com/packaging/role-of-nanotechnology-in-brand-protection.html>

Brand Protection through Nanotechnology

<http://www.brandauthen.com/20081028%20Brand%20Protection%20through%20Nanotechnology.ppt>

ESRAB Final Report

http://ec.europa.eu/enterprise/security/doc/esrab_report_en.pdf

European Security Research and Innovation in Support of European Security Policies,
Intermediate Report, September 2008, European Security Research and Innovation Forum,

http://www.esrif.eu/documents/intermediate_report.pdf

5. Appendix 1: Expert Engagement

The following people attended a session stream on nanotechnology for security at the ObservatoryNano workshop in Dusseldorf in March 2009:

Dr. EA McKigney (Los Alamos National Laboratory)

Professor Dr. Helmut Bachmayer (Biosecurity Consultant, ESRAB)

Dr Valerio Pagnotta (Teraeye Project)

Dr. Frank Schäfer (Fraunhofer EMI)

Dr. Christian Mittermayr (Lambda GmbH)

Dr. Gerhard Holl (WIWEB), Christian Stüble (Sirrix)

Dr Juergen Altmann (University of Dortmund)

Dr Michael Decker (ITAS)

Dr Mostafa Analoui (Livingston Group/Charlesson Pharmaceuticals)

Prof. Nikolas A. Chaniotakis (University of Crete)

Prof Jon Cooper (University of Glasgow),