BRIEFING No. 8

SECURITY

NANOTECHNOLOGIES FOR ANTI-COUNTERFEITING APPLICATIONS

Counterfeiting is a global phenomenon, affecting individuals and communities in small villages and major cities right up to big retail stores and pharmaceutical companies. The dual impact of globalization and growth of internet trade has made the problem considerably more acute. Counterfeit products circulate globally via unregulated channels but can also enter legitimate supply chains. In many cases it is very difficult to distinguish them from genuine products.

At present counterfeiters are able to copy most anti-counterfeiting technologies within 18 months. As a result an estimated 7-10% of all goods sold worldwide in 2007 were counterfeit at a cost of ca. €450 billion. Industry segments for which counterfeits are a significant problem include pharmaceuticals, airplane parts, auto parts, and designer clothing, among others. Recent developments in nanotechnology and nanomaterials have enabled significant improvement in the field of anti-counterfeiting measures. However, their implementation may require the development of new policy.

This BRIEFING outlines promising developments with strong potential to create new technology platforms for anti-counterfeiting applications, adding value to the growing demand to reduce citizens' health and security risks of using counterfeit products and industry aspiration to reduce revenue losses associated with counterfeiting activities.

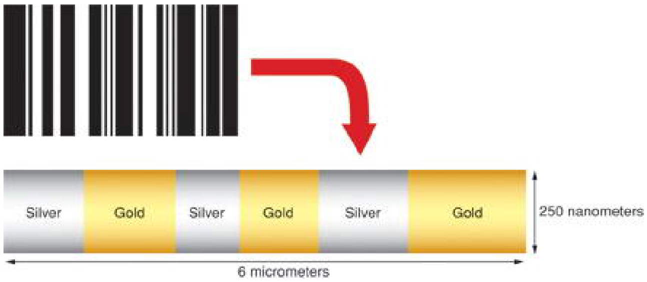

Illustration of a nano barcode for enhanced product protection against counterfeiting[1]

The counterfeiting challenge

Counterfeiting is a high-volume, high-profit business which poses health risks for citizens, lost revenue for businesses, brand damage and decreased public confidence. Several factors make this activity attractive to criminals:

- free trade zones, globalization and complex product supply chains make it easy to introduce counterfeits into legitimate supply channels, especially in areas with weak regulatory controls;
- it is a lucrative activity, especially for products that command high prices or are required in large volumes;
- technologies to make constituent ingredients and packaging are cheap and readily available;
- existing anti-counterfeiting technologies have significant limitations allowing counterfeiters to copy most anti-counterfeiting technologies within 18 months;
- current legislations and regulations do not provide a strong enough deterrent to discourage counterfeiters.

> **Information Box 1: Counterfeiting Definition**
>
> **Counterfeiting** encompasses any manufacturing of a product that imitates the appearance of the product of another to mislead a consumer. It also includes trademark infringing goods, copyright infringements as well as copying of packaging, labelling and any other significant features of the product.

Nano strengthens barriers to counterfeiting

By providing non-reproducible technological features, nanotechnology based developments are expected to offer a significant move forward in preventing illicit copying intellectual properties and products. Ultimately, the implementation of the novel techniques will considerably reduce tax revenue losses through counterfeiting and improve citizens' safety and quality of life.

Holograms, tamper-evident closures, tags and markings and RFID labels are the most widely known anti-counterfeiting technologies. The key limitation of these methods is that they can be copied. Innovations exploiting the intrinsic nature of nanomaterials to give items complex and unique 'fingerprints' results both in the development of new approaches and improvement of existing techniques.

Holography - easily identifiable holograms, for example, showing the manufacturer's logo are primarily used as first level identification devices. Two dimensional nanoscale gratings, photopolymers and luminescent nanoparticles can be utilized to provide an additional level of security for the holograms[2].

Laser surface authentication - a laser is used to examine the surface roughness of an object. Complexity and uniqueness of the surface roughness code is similar to iris scans and fingerprints. The advantages of the technique is that surface roughness at nanoscale cannot be replicated. Therefore, a much higher level of security is offered to products as compared to holograms and watermarks[3].

Radio frequency identification (RFID) - is a form of automatic identification and data capture technology where data stored on a tag is transferred via a radio frequency link. An RFID reader is used to extract this data from tags. New developments exploit nanoscale variations, naturally produced during the manufacturing process of RFIDs that are unique to individual integrated circuits , which can be verified during data transfer[4]. This is known as the Physically Uncloneable Function (PUF).

Nano barcodes - three dimensional polymer patterns on the order of tens of nanometres can be made on silicon substrates to provide 3D nanoscale data encryption key, similar to barcodes. The advantages over conventional barcode/marking are difficulty of detecting presence (covert marking) and duplication. These can be applied to banknotes, security papers, art, jewellery and gem stones[5].

SERS and quantum dots tags – metal nanoparticles produce unique electromagnetic spectra (known as surface enhanced raman scattering) while certain semiconductor nanoparticles (known as quantum dots) have different fluorescence based on size and chemical composition. Both can be exploited as identification tools. They offer difficulty in reproducing due to infinite combinations, covert security feature, non-toxicity and multi-functionality. These nanoscaled tags can be applied in inks, adhesives, laminates, paper, packaging, textiles, glass, and others[6].

Nanocomposite tags consist of a materials-based pattern (with magnetic and/or optical features) that forms part of a label, tag or embedded portion of an item. The nanometre sized magnetic and optical features are generated randomly during manufacturing, constituting a unique 'fingerprint' that is read and stored in a central database . The result is a secure identity for an individual item that is prohibitively expensive and difficult to copy. This technology can be applied in the pharmaceutical, spare parts, fashion and food and beverage industries[7]. Incorporating encapsulated and functionalized (e.g. thermochromic) nanoparticles in labels is another promising solution based on the use of nanocomposites.

Impacts

Economic/Industry

The pharmaceutical industry is the most heavily affected by counterfeiting (estimated at €10.5 billion per year in Europe), with the market size of anti-counterfeiting technologies estimated at €324 million in 2009, which includes a range of technologies from barcodes to RFID. The accessible market for nanotechnology-based approaches is likely to be limited initially to higher cost items where the loss to counterfeiting exceeds the cost of investing in new technologies[8].

More robust anti-counterfeiting may also protect the position and margins of Europe's pharmaceutical, food and manufacturing firms.

Nanotechnology may also have a more tangential impact on anti-counterfeiting. The second most common approach to product identification after barcodes is RFID. Developments in printed electronics, such as nanomaterials for conductive inks are likely to enable roll-to-roll processing of RFID tags and therefore decrease their price. This will enable more items to be tagged at unit rather than pallet-level, and enable improved tracking of items throughout the supply chain.

Societal/Impact on European Citizen

Industry world-wide loses large amounts to counterfeiters. However, the ultimate victims of counterfeiting are society and consumers. They receive poor-quality goods at an excessive price and are in many cases exposed to health and safety dangers. Approximately 2.5 million jobs have been lost due to counterfeiting and piracy across the G20 economies[9].

The adoption of improved anti-counterfeiting techniques, such as highlighted above, would result in:

- a dramatic reduction in financial costs associated with purchase and use of counterfeited goods;
- fewer job losses due to unfair competition caused by counterfeiting;
- a significant rise in customer goodwill and confidence in products and services;

- a reduction in tax revenue losses to government;
- reduced costs to protect and enforce intellectual property rights.

Technology readiness levels (TRL)

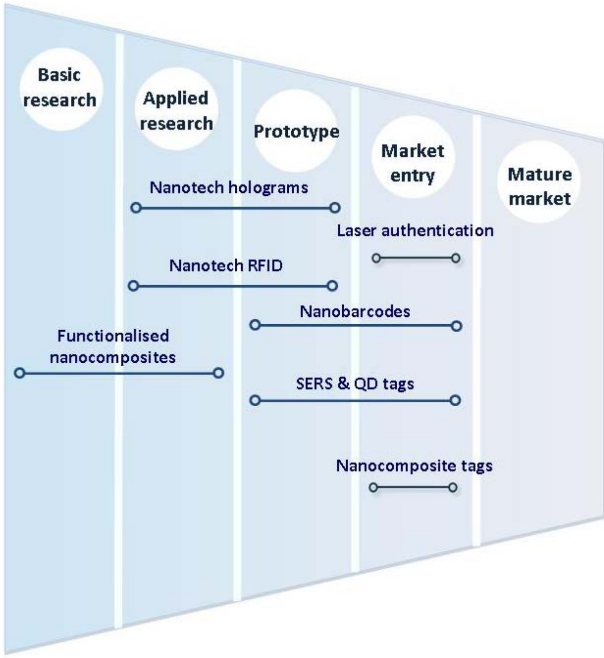

Figure 1: *TRL for a number of nano-enabled anti-counterfeiting applications*

Challenges

Economic barriers

The total cost is important, compared to both existing solutions and the likely savings from using more sophisticated anti-counterfeiting strategies. For tagging-based solutions the cost per tag is an important factor and will limit the products with which they can be used cost-effectively. For sensing approaches, cost is a factor of the equipment required plus any changes to existing production processes. A further barrier is the requirement to adopt these technologies throughout the supply chain, deploying detection equipment with wholesalers and end-users, as well as at production sites.

Technological challenge

While new nano-enabled techniques can generate unique features that cannot be reproduced even by the manufacturer, the problem of fast and secure reading of these features and exchange of the information between producer and end-user remains mainly unresolved.

The anti-counterfeit industry is saturated with covert features; however, it lacks feasible and cost efficient overt methods of product authentication.

ELSA issues

As with any other technological development, anti-counterfeiting methods utilizing nanotechnologies should be developed in a responsible, sustainable way, and efforts are needed to let those in developing countries share the benefits. In preparation of this briefing, no information has been identified that the developments highlighted give rise to specific ethical or societal issues.

A number of international organizations have been established to work with government officials and industry groups across the globe to educate the public on the danger of counterfeit and measures to combat it. For example, the Counterfeiting Intelligence Bureau (CIB) set up the live counterfeiting seizure map and database of seizure reports enabling everyone to see the details of recent anti-counterfeiting operations[10]. However, experts recommend that more actions should be undertaken to raise public awareness of the risks of illegal goods and counterfeits, and the availability of advanced anti-counterfeiting technologies.

Health & Safety

A range of nanomaterials are used in advanced anti-counterfeiting technologies[11]. These materials are expected to have a negligible effect on the health of end users and the environment, since they are typically incorporated into a substrate material (e.g. polymer, metals, or glass). Once integrated in a substrate, the nanoparticles are not likely to be released in an amount that would cause a risk to humans or the environment. However, while the amounts of nanomaterials used in anti-counterfeiting applications are usually very small, the possible handling of free nanoparticles during the manufacture of devices or components requires suitable procedures to be followed to limit workers' exposure. Given the potential scale and ubiquity of these new technologies, investigation of the whole life-cycle of these nano-enabled products (from manufacturing stage through use and to disposal) should be performed.

EU Competitive Position

Analysis of patent applications shows strong growth of activities in the field of anti-counterfeiting technologies since 2000 (***Figure 2a***). At present North America (mainly USA) leads the process of IPR protection closely followed by EU countries (***Figure 2b***).

Several European start-ups have been founded in recent years to exploit nanotechnologies for anti-counterfeiting (including Ingenia Technology and Scriba Nanotech). Whilst current market share and employment is low, the companies have been successful in attracting external investment.

SECURITY: NANOTECHNOLOGIES FOR ANTI-COUNTERFEITING APPLICATIONS

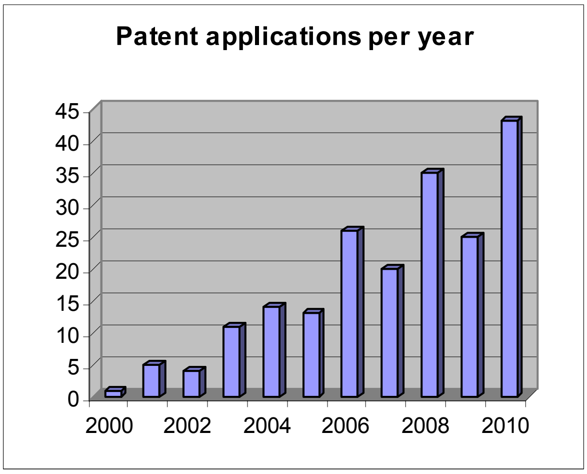

Figure 2a: Patent applications per year (2000-2010).

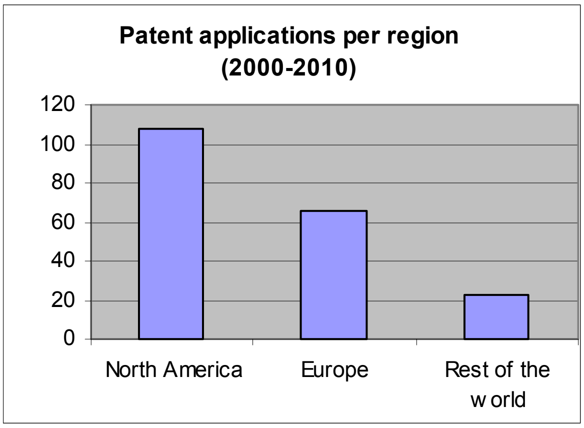

Figure 2b: Patent applications per region (2000-2010).

Summary

- A wide variety of counterfeit products circulate globally, both through legitimate and unauthorized channels (such as, for example, online trade) posing significant risks to public health and safety, lost revenue for businesses, brand damage and decreased public confidence.
- Recent nano-enabled developments in anti-counterfeiting technologies are expected to provide considerable progress in preventing illicit copying of intellectual property and products.
- These developments offer improved anti-counterfeiting performance, due to an almost infinite number of combinations (thus greater uniqueness), difficulty in reproduction and in detection.
- New approaches incur a direct cost – that of the security features and production equipment – and an indirect cost of equipping supply chain partners with devices to read these tags. For this reason, adoption is likely to occur in industry sectors where the goods being protected are high value.
- A successful technology should be simple and universal to be accepted by customs worldwide.
- Co-ordination and co-operation across industries and technology boundaries is essential to ensure effective industry specific options are devised. The EC should facilitate this process though introducing pan-European directives tackling affected industry sectors.
- Progress must be made to raise public awareness of the risks of illegal goods and counterfeits and availability of advanced anti-counterfeiting technologies.

Contact Information

Dr Sergey Gordeyev, Institute of Nanotechnology,
sergey.gordeyev@nano.org.uk

Tom Crawley, Spinverse,
tom.crawley@spinverse.com

References

[1] Image source: www.llnl.gov/str/Oct06/Krishnan.html

[2] Holographic nano-imaging realized with compact extreme ultraviolet lasers, Marconi M.C. et al. // Lasers and Electro-Optics Society, 2007. LEOS 2007. The 20th Annual Meeting of the IEEE
Volume holograms: www.smartholograms.com/productstech.html

[3] The LSA technology: www.ingeniatechnology.com/content/4/technology/1/

[4] PUF technology: http://www.verayo.com/product/pufrfid.html

[5] Nanobarcodes particles as covert security tags for documents and product security, S.G. Penn et al., Proceedings Vol. 5310 Optical Security and Counterfeit Deterrence Techniques V, Rudolf L. van Renesse, Editors, pp.337-340

[6] Surface-Enhanced Raman Scattering by Fran Adar, http://spectroscopyonline. findanalytichem.com

[7] Bilcare Technologies has developed and commercialized an anti-counterfeiting and security solution called nonClonableID ™ based on use of nanocomposites. http://www.bilcaretech.com/nonclonable/nonclonable.htm

[8] Pharmaceutical Anti-counterfeiting Strategies and Commercial Analysis 2010-2020, http://www.visiongain.com

[9] The Impact of Counterfeiting on Governments and Consumers. A REPORT COMMISSIONED BY BASCAP, May 2009

[10] Follow corresponding links at the CIB website of http://www.icc-ccs.org/index.php?option=com_content&view=article&id=29&Itemid=39

[11] Marie-Claire Toufektsian, ObservatoryNano report on Environmental, Health and Safety Impacts. Technology Sector Evaluation: Security, 2010, http://www.observatorynano.eu