Nanomaterials Technology: Convergence between Nanotechnology and Materials Science and Engineering

Michael Fredholm

This chapter will describe the implications for security forces of the convergence between nanotechnology and materials science and engineering. It will aim to investigate what can be expected in the medium term, until 2025, by examining U.S. and Russian efforts in nanomaterials, with a focus on security forces applications. It will also suggest a few scenarios in which nanomaterials are likely to be misused against individuals or societies, states, and their security apparatuses. What are the challenges? What should we expect in this field in the medium term, that is, by 2025?

This chapter will not cover the convergence of nano/bio/info technology or robotic/cognition/info technology, since these will be described elsewhere in this volume.

How will we predict the implications of future technology? We need to distinguish between Early Warning, Situational Awareness, and Forecasting. Which is our focus? Forecasting may be impossible, so Early Warning and, whenever possible, Situational Awareness with regard to new technology and its implications may be better options. Most studies extrapolate from the past, but this may not be enough.

The current trend in technology threat forecasting is to use tweets (and, for some, RSS feeds). However, tweet logs lag behind social media and real events but they do mirror them (RSS feeds also suffer from time lag). There is a more serious time lag as well, since open-source information appears later than real events. There are also time gaps, due to a limited availability of data. Algorithms can be used to address these problems, although the enthusiasm with regard to potential success seems bigger than the actual results.

The trend in horizon scanning for emerging technology is to scan open source scientific literature. Early indicators are likely to appear in open source specialised literature. Key discoveries are relevant for various scientific disciplines, therefore key scientific technical journals should be added to watch lists for emerging technologies. Analysis of publications, conference proceedings, and tweets can be also used to keep track of developments in science and technology.

However, this methodology will not work well for military technologies, since not all achievements are published. Automated data mining can reduce human 'blind spots' but will produce many false positives/false negatives. Data mining can find 'nearest neighbours' to known technologies, but no actual black swans. Besides, the current data mining trend is to rely on Google search for patents, which is insufficient since potentially adversarial countries do not publish their scientific results in this way.

For this reason, a qualitative rather than quantitative study is necessary. Furthermore, the study must be based in a broad understanding of not only the subject area but also of the wider societal and technological trends. For this reason, the present chapter will begin with an outline of the background of current and projected military and security applications of nanomaterials, then go on to focus especially on U.S. and Russian efforts, since these will illustrate the difficulties of solely relying on open-source specialised literature. Finally, a number of misuse scenarios will be described, again with an emphasis on those for which open-source information may be insufficient for forecasting.

Origins

The concepts that inspired nanotechnology were first discussed by physicist Richard P. Feynman in his lecture 1959 with the title "There's Plenty of Room at the Bottom", in which he described the possibility of synthesis via direct manipulation of atoms.[150] The term 'nanotechnology' was first used by Norio Taniguchi in a conference paper in 1974.[151] However, K. Eric Drexler made the term 'nanotechnology', which he used in his 1986 book *Engines of Creation: The Coming Era of Nanotechnology,* popular.[152] As a result of these works, nanotechnology emerged as a scientific field in the 1980s. Commercialisation of products based on advances in nanoscale technologies finally began in the 2000s.

Although nanotechnology is an emerging technology, defined as a technology which is not necessarily new but not widely used, it is likely to result in significantly more advanced science-based innovations in the near future. Moreover, it has the potential to create a new industry or transform an existing one, having already moved beyond the purely conceptual stage. In short, the defining characteristics of an emerging technology are neither commonplace science-based innovations or industrial usage nor concrete, as opposed to theoretic, application. Other characteristics of emerging technologies, as identified by Mohanad Halaweh, are uncertainty, network

---

150 Feynman, Richard P. 1959. Plenty of Room at the Bottom. Transcript. Pasadena: American Physical Society.
151 Taniguchi, Norio.1974. On the Basic Concept of 'Nano-Technology'. In: Proceedings of the International Conference on Production Engineering. Part II. Tokyo: Japan Society of Precision Engineering.
152 Drexler, K. Eric. 1986. Engines of Creation. The Coming Era of Nanotechnology. New York: Anchor Books.

effect, unseen social and ethical concerns, cost, limitation to particular countries, and a lack of investigation and research.[153]

The sub-field of nanomaterials technology is a converging technology. The term, which was introduced by Mihail C. Roco and William Sims Bainbridge, refers to the "synergistic combination of four major 'NBIC' (nano-bio-info-cogno) provinces of science and technology," that is, (a) nanoscience and nanotechnology; (b) biotechnology and biomedicine, including genetic engineering; (c) information technology, including advanced computing and communications; and (d) cognitive science, including cognitive neuroscience.[154] Nanomaterials are the result of the convergence between nanotechnology and materials science and engineering.

Materials science, also commonly known as materials science and engineering, is an interdisciplinary field which involves the discovery and design of new materials, with an emphasis on solids.[155] Intellectually, the origin of materials science was the Age of Enlightenment, when researchers began to use analytical thinking from chemistry, physics, and engineering to understand ancient, phenomenological observations in metallurgy and mineralogy. Materials science thus incorporates elements of chemistry, physics, and engineering.

Nanotechnology is the manipulation of matter resulting in the engineering of functional systems at the atomic, molecular, and supramolecular scale

---

153 Halaweh, Mohanad. 2013. Emerging Technology: What is it? In: Journal of Technology Management & Innovation 8(3):108-115.

154 Roco, Mihail C. & Bainbridge, William Sims 2002. Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation.1-2.

155 Science Journal of Chemistry, Research Topic #2, Materials chemistry; http://www.journalchemistry.org/index accessed on 04 December 2017.

and implies a projected ability to construct items from the bottom. Nanotechnology is not a single technological field but encompasses all types of research and technologies that deal with the special properties of matter below at a certain scale, which is usually interpreted between 1 and 100 nanometres.

Nanomaterials research takes a materials science-based approach to nanotechnology, in effect being a convergence between traditional materials science and the emerging potential of nanotechnology. In this way it is possible to create many new materials – nanomaterials – and devices with a vast range of applications, for example in medicine, electronics, biomaterials energy production, and consumer products. Materials whose structure can be found at the nanoscale often have unique optical, electronic, or mechanical properties. Many lend themselves to dual use application, for example, in construction materials, consumer products, and military/security equipment. At the same time, there is a significant potential for the abuse of consumer products that include nanomaterials.

The field of nanomaterials is, like the traditional field of chemistry, loosely grouped into organic (carbon-based) nanomaterials, such as fullerenes, and inorganic nanomaterials, based on other elements, such as silicon. Examples of nanomaterials include fullerenes, carbon nanotubes, nanocrystals etc.[156] Nanomaterials have an impact on metals, alloys, fibres, ceramics, and composites.

Major benefits of nanotechnology include improved manufacturing methods, leading, for instance, to vehicles, energy systems, and detoxification systems with a better performance. Purification and

---

156 Everipedia.org, Materials science, https://everipedia.org/wiki/Materials_science/, accessed on 11 December 2017.

environmental clean-up applications include the desalination of water, water filtration, waste-, and groundwater treatment. Future benefits may include better food production methods, nutrition, physical enhancement, nanomedicine, and eventually large-scale automated fabrication infrastructure. Due to the scale on which it operates, nanotechnology may allow for the automation of tasks that were previously impossible due to physical restrictions.

Our focus here will be on applications in technology and the security forces. In modern history, military needs have often pushed technology, particularly in situations when countries are faced with existential threats as, for example, during World Wars I and II as well as the Cold War. However, it will be shown that this is not necessarily the case with nanomaterials, since nanomaterials technology really only emerged in the early 21st century, when no existential military threat remained. Then, the focus was on low-intensity conflicts and counterterrorism in remote countries. This situation is unlikely to change in the short term.

Moreover, the implementation of nanotechnology will necessarily include an economic parameter, which is difficult to forecast. Will the gains produced be regarded as motivated by the higher costs? Furthermore, the organisational culture must be receptive to the adoption of new technology, even if it disrupts existing traditions and doctrine.

Perhaps, for this reason, results have so far been incremental. It will be shown that existing nanomaterials technology provides gradual, not revolutionary advantages. Underlying the age of nanotechnology from the beginning was the belief in the revolution in military affairs (RMA) hypothesis, which claimed that new technology would enable radically new military hardware and operational concepts, making high technology the key arbiter on the battlefield of the future. Information processing, communications, robotics, and other advances in technology would lead to major advances in military affairs. Sensors would develop until the battlefield essentially became transparent, and the fog of war would become a problem of the past. Vehicles of all kinds would become lighter, faster, and stealthier. Finally, new types of weapons would emerge, among them advanced biological agents and directed energy beams. However, sceptics such as Michael O'Hanlon argued that although advances in information processing and communications were real, the other projected developments were at least overstated by their proponents, and the RMA hypothesis was unconvincing, at least in the near future. Environments such as forests and cities would remain significant obstacles to high-technology warfare. Most trends in military technology were not as impressive as RMA proponents argued. While new tools and weapons would change tactics, they would not change the basic nature of armed conflict. In 2000, O'Hanlon concluded that "even if a contemporary revolution in military affairs may eventually be possible, it does not appear within reach today."[157]

Almost two decades later, the RMA hypothesis still appears to be beyond our reach, despite the limited benefits for military hardware provided by developments in nanotechnology. As for the incremental advances provided by nanomaterials, most are indeed visible in consumer goods.

Current consumer applications

Several products that contain nanomaterials are already in use. Nanomaterials may be found in a variety of items, which people are not aware of since they cannot be seen with the naked eye. At present, simple nanoparticles are the most widely used nanomaterials, used in coatings, paints, sensors, chemical catalysts, and food packaging.

---

[157] O'Hanlon, Michael. 2000. Technological Change and the Future of Warfare. Washington, DC: Brookings Institution Press. 193.

Nanomaterials are already common in products, especially in the field of cosmetics, pharmaceuticals and consumer chemicals. For example, a sunscreen based on mineral nanoparticles such as titanium oxide offers several advantages, including higher radiation resistance than conventional sunscreen. Zinc oxide nanoparticles let light of some wavelengths through while blocking the rest, which makes them useful for certain sunscreen products. Silver nanoparticles with antimicrobial properties are added to laundry detergents. The use of engineered nanofibers in textiles enables wrinkle-resistant and water- and stain-repellent clothing, and such textiles need to be washed less frequently and at lower temperatures. Silver nanoparticles with antimicrobial properties are added to washing powder. They can also be woven into socks, where they kill bacteria. Nanotechnology also allows the introduction of full-surface protection from electrostatic charges by the integration of carbon particle membrane in fabrics. It may also be applied in food packaging. Clay nanoparticles improve barrier properties and are used in some plastic food packaging to increase shelf life, for instance in glass packaging for drinks. Perhaps most importantly at present, the use of nanomaterials enables lighter and stronger products. Clay nanoparticles are used to make lighter, stronger, and more elastic composites, and therefore are used in some car bumpers and composite bicycle frames. They also make cell phones lighter in weight and enable the production of harder synthetic bones. Even balls for various sports are made more durable. Recent generations of semiconductors can also be included in the field of nanotechnology.[158]

Nanotechnology thus already provides existing types of consumer products with incrementally better, but not revolutionary, functions. Nanomaterials can be used to produce more lightweight products. Surfaces and coatings

[158] Manyika, James et al. 2013. Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy. McKinsey Global Institute. 114, 118.

on ceramics and glasses become easier to clean or even self-cleaning, and more scratch-resistant.

Nanotechnology also has applications in heavy industry, particularly in construction. Lighter and stronger materials enable the construction of vehicles that are faster and safer. This is particularly useful for aircraft manufacturers, since it leads to significantly increased performance. Such materials also reduce the size of equipment thereby reducing fuel consumption. Existing types of combustion engines benefit from parts that are more heat-resistant and hard-wearing.

Projected consumer applications

The dilemma is that many types of nanomaterials are already available, but a high production price makes them uncompetitive. Graphene, which is composed of one-atom-thick sheets of graphite – carbon hexagons – is already being produced but the cost remains high compared to other materials and thus uncompetitive. Being one sixth the weight of steel per unit of volume and more than a hundred times as strong, it has huge potential. It can also be compressed without fracturing and has 35 per cent less electrical resistance than copper and ten times the conductivity of copper and aluminium, and thus would be an excellent choice for electrical circuits. Nanotubes (tubular graphene) are perhaps best known and show great potential, if production processes can be scaled up cost-effectively.[159]

Projected consumer applications include 'smart' materials, nanosensors, and miniature power generation.

Smart materials are any kind of material designed and engineered at the nanoscale for a specific task. This includes a wide variety of possible

---

[159] Ibid.118.

commercial applications. Clothes could become 'smart' through embedded wearable electronics. Fabrics and other materials could be designed to respond differently to various molecules. Artificial drugs could recognize and render inert specific viruses. Self-healing structures could naturally repair small tears in a surface in the same way as self-sealing tires or human skin.

A nanosensor would resemble a smart material in that it that would react to its environment and change in a fundamental, intentional way. A photo-sensor might passively measure incident light and discharge its absorbed energy as electricity when the light passes above or below a specified threshold, in effect sending a signal to another and larger machine. Such a sensor would likely cost less and use less power than a conventional sensor, yet function in the same applications.

Miniature power generation systems would generate the energy needed to power other miniature systems through the wearer's normal body movements. Improvements in battery and solar power technology and increased energy efficiency will also enhance the use of energy.

While nanomaterials can be expected to result in many improvements in existing products, nanomaterials are not generally believed to be a disruptive technology, that is, one which will have major implications for individuals and societies. Yet, this field will result in new products and services. It will result in changes in quality of life, health, and the environment, but it will likely not change patterns of consumption, the nature of work, or bring changes in the organisational structures of corporations or states.[160]

---

[160] Ibid. 20.

Current and projected military and security applications

Certain military products too have appeared with incrementally better, but no revolutionary, functions. However, comparatively few have entered service. Far more are projected. These can be grouped into communications and sensor applications, defensive applications, and offensive applications, in roughly this order of apparent importance. Applications for homeland security and policing would be a fourth category, even though it would overlap with the others in significant ways.

Communications and sensor applications

The use of nanomaterials will enable high-performance information technology with a performance improved by several orders of magnitude as compared to present technology. Small but powerful computers will be built into weapons, uniforms, and vehicles. Batteries and similar power sources will have an improved efficiency as compared to conventional technology, since nanoenergetic materials can store more energy than conventional energetic materials. The produced goods will be smaller, lighter, cheaper, and more efficient.

Nanomaterials allow the replacement of several present-time bulky and energy-intensive sensors with far smaller ones with far lower energy requirements. An example would be a cheap array of microsensors with the ability to detect chemical and biological warfare agents on a single chip or flexible, textile-embeddable, nanofiber-based sensors capable of being mounted on more solid garment or used in a pocket as a wearable sensor. Cheap miniature sensor systems could be scattered in high numbers, including miniature drones, some of which may be very small, perhaps centimetres, later millimetres, and even below. Low-cost miniature satellites can be built for low- orbit deployment, for the collection of data emitted by unattended ground sensors, such as GPS beacons, cameras, microphones, vibration detectors, or other sensors. Such technology has already been announced by several U.S. firms.[161]

Communications between soldiers can be improved by the use of nanoparticles to create coated polymer threads woven into soldiers' uniforms, allowing protected communication between the soldiers. The system of threads in the uniforms could be set to different light wavelengths, eliminating the ability for anyone else to listen in.[162]

The use of nanomaterials will also enable further miniaturisation of the technology used for unmanned vehicles including combat vehicles – drones. Unmanned Aerial Vehicles (UAVs) will have greater range and endurance, due to the lighter payload and smaller size. Unmanned Underwater Vehicles (UUVs) will have better performance characteristics, due to the miniaturisation of navigation and guidance electronics.

Despite the advantages, a challenge for miniature UAVs will be survivability in an electronic warfare environment. Enemy jamming is likely to be an efficient countermeasure, since, due to its small size, a miniature UAV close to the enemy is unlikely to have sufficient inherent power to transmit through enemy jamming without losing its communications line. It must then be completely autonomous and, if designed as a sensor platform, able to return home or at least to report within communications range of a swarm of other miniature UAV sensor platforms.

Developments in nanomaterials will of course also benefit manned flight. The use of nanomaterials may eventually lead to integrated health-

---

161 n.a. 2014. Nano-Satellites, the Future of Interception. Intelligence Online. Issue 726.
162 Everyipedia.org, Industrial applications of nanotechnology, https://everipedia.org/wiki/Industrial_applications_of_nanotechnology/, accessed on 11 December 2017.

monitoring systems for airframe and engine, and advanced sensors that would allow fully integrated exterior-interior flow control and continuously deformable wings constructed of nanomaterials for better aerodynamic characteristics, manoeuvrability, and range.[163]

Finally, nanotechnology could be used for implants in soldiers' bodies in the form of neuron contacts, small computers, bio-compatible materials, and power supplies, which would be used for monitoring, communication, expanded senses, or drug release. However, this capacity would reach beyond that of nanomaterials and enter other fields of convergent technologies.

Even so, there seems to be a key threshold that needs to be overcome. This particularly concerns information technology and is indeed exemplified by software complexity. Moore's well-known law suggests a doubling of computer power every 18 months, and indeed computer power has hitherto increased exponentially. However, this doubling of computer power has not automatically led to a doubling of human capacity to write significantly more complex software. Jordan Pollack has observed that "faster and faster computers seem to encourage software companies to write less and less efficient code for the same essential functionality" which suggests that there are limits to the complexity of achievable design.[164] The human cognitive ability to remember, not to mention improve, millions of lines of code remains limited. When nanotechnology enables the self-

---

[163] Venneri, S. & Hirschbein, M. & Dastoor M. 2002. A Vision for the Aircraft of the 21st Century. In: Roco, Mihail C. & Bainbridge, William Sims. Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation. 313-317.

[164] Pollack, Jordan (Brandeis University). 2002. Breaking the Limits on Design Complexity. In: Roco, Mihail C. & Bainbridge, William Sims. Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation. 161-164.

replication and indeed self-improvement of design, that is, evolutionary design, a true breakthrough will take place. But this seems increasingly unlikely to happen in the medium term.

Defensive applications

The use of nanomaterials will reduce the volume and weight of the combat equipment carried in the field. This characteristic can in itself be regarded as a defensive application. But there are others, which may prove even more important.

For instance, uniform fabrics can include high-performance fibres in which special nanoparticles group together when something strikes the fabric, in order to stiffen the area of impact. This stiffness helps lessen the impact of blunt force. By reducing the force of the impact, the nanoparticles protect the soldier from injury. One such development is the so-called liquid armour, which consists of several layers, with a thick fluid between each layer. Upon impact, the fluid solidifies, thus absorbing the impact over a wider area.[165] Nanoparticles functioning as ballistic resistance also make the fabrics flame-retardant. This will shield soldiers from both kinetic energy and high temperatures. Moreover, the fabrics become more durable. The latter can also be made to shield soldiers from chemicals and biological warfare agents. Selectively permeable membranes could provide an outer layer for uniforms that would prevent aerosols and liquids from penetrating. Integrated decontamination activity and cooling or heat-resistant properties are feasible too.

---

[165] By an odd coincidence, this function corresponds to the protection provided by a legendary suit of living chain-mail armor in Georgia, worn by the hero Torgva. When hit by a sword, arrow, or bullet, all the loops of the chain-mail gathered and piled up in that very spot, protecting its wearer. (cf. Hunt, David. Legends of the Caucasus. London: Saqi.159.).

Surfaces of many different military items including uniforms and vehicles can be designed so electromagnetic radiation reduces the infrared signatures of the object's surface. This will improve stealth in the form of thermal camouflage, protecting soldiers from being seen with night vision devices and enabling better protection from infrared guided weapons or infrared surveillance sensors. Indeed, surfaces with locally variable colour – for example, through the use of phase-change materials, such as mobile pigment nanoparticles injected into the material – can be used for camouflage, enabling uniforms to change its colour according to the surroundings. By combining these methods dynamic multispectral camouflage can be created to protect against visual, infrared, and eventually radar observation.

Beyond the field of mere nanomaterials, converging technologies that include nano-scale applications can reach yet further.

Nanotechnology makes a biomedical, health-monitoring system worn by soldiers possible, able to watch over health and stress levels. Such systems would use sensors for vital signs, stress hormones, and physical activity, and could sense the state of health of the wearer. They would react by releasing drugs or, using smart materials, by compressing wounds until further medical treatment can be applied. This would reduce casualties, due to heat stress and dehydration, performance failure due to sleep deprivation (sleep time being determined by the lack of motion of the sensor), certain wounds, and combat stress. Detecting chemical and biological warfare agents, through the appropriate sensors would be also possible.

The system would also be able to release drugs into the soldiers' bodies, such as pain killers in case of injuries. The system would be able to inform the medics of the base of the soldiers' health status whenever they are wearing the system and are within communications range. The energy needed would be generated through the soldiers' normal body movements.

Yet another development could consist in improving human performance, including compensation for sleep deprivation and enhancement of survivability in case of physical injury.

Offensive applications

In nanomaterials, there is a higher focus on communications, sensor, and defensive applications than on offensive ones. However, better sensors and higher performance in weapons systems is a characteristic that in itself may be regarded as an offensive application. Besides, weapons can of course be improved as other forms of industrial applications. So far, most attention has been on explosives. Fast-release explosives, and incidentally slow-release propellants as well, must have high energy density while retaining stability, and nanoenergetic materials show greater power density than those in conventional explosives, thus can store more energy than conventional energetic materials.[166]

Nano-sized thermic materials could be used for new types of bombs several times more powerful than conventional explosives. A thermobaric weapon is a type of explosive that utilizes oxygen from the surrounding air to generate an intense, high-temperature explosion. The fuel-air bomb is one of the most well-known types of thermobaric weapons.

Nano-sized materials would also enable miniature munitions, including missiles that could be equipped with guidance systems, even though their explosive power may not reach that of conventional missiles.

---

166 Lau, Clifford 2002. Nanotechnology and the Department of Defense. In: Roco, Mihail C. & Bainbridge, William Sims. Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation. 349-351.

For clandestine special operations, nanofiber composites could enable metal-free small arms and ammunition.

Unmanned Combat Aerial Vehicles (UCAVs), that is, armed drones, will have greater aerial combat capabilities, in part for the same reasons as UAVs (lighter payload and smaller size) but also because there is no pilot on board, there will be no g-force limitations and no need for life support, armour, or evacuation systems. Again, even more can conceivably be achieved through other converging technologies, including fully autonomous systems, known as Lethal Autonomous Weapons Systems (LAWS). If the latter remain unfeasible, it may be possible to modify or implant the desired systems in small animals such as rats or even insect.

Genetic engineering enables targeted chemical and biological warfare agents, including through nanotechnology. The development of biological agents that will not be detected or affected by known countermeasures can be expected. An inorganic nanomaterial would then be used to mask a biological material, for instance, the anthrax toxin could be bound to a nanoparticle that is used to transport the toxin across the cell membrane. Current vaccines would then not function. Second, nanotechnology could be used to disrupt the immune system, through either suppression or overstimulation, and prevent it from functioning. Certain nanoparticles can trigger an immune response, and delivery enabled by nanotechnology can again be used to overcome existing medical countermeasures.[167]

---

[167] Kosal, Margaret E. 2014. Anticipating the Biological Proliferation Threat of Nanotechnology: Challenges for International Arms Control Regimes. In: Nasu, Hitoshi &McLaughlin, Robert (eds.): New Technologies and the Law of Armed Conflict. The Hague: Asser Press.159-174.

Homeland security applications and policing

The terrorism threat that heralded the 21st century also brought home the potential for nanotechnology in homeland security, specifically sensors for chemical/biological/radiological /explosive detection. Sensor systems can be expected to be installed in all sorts of facilities, including but not limited to transportation nodes (airports, railway and subway stations, and others), border crossing points, government offices, public water supplies, chemical industries, and schools.[168]

Nano-materials also present significant opportunities for policing. Again there will be an emphasis on sensors, but this time used in police investigations. For law enforcement agencies, a key benefit of the improved sensory capacities of scientific instruments would be the ability and the speed with which forensic scientists will be able to examine crime scenes and traces left by criminals. Nanotechnology is expected to allow for faster DNA analysis and an improved examination of fingerprints and blood samples.[169]

Nano-materials may also play a major role in the use for the policing purposes of Big Data and, soon, the Internet of Things (IoT). Devices such as telephones and personal computers are already used by law enforcement to determine the whereabouts of individuals. With the increasing connectivity of a wide range of goods, such as clothes, jewellery, and footwear to the nearest wireless network, for commercial or entertainment purposes, it will become easier to pinpoint the whereabouts of a person at a

[168] Murday, James. 2002. NBIC For Homeland Defense: Chemical/Biological/Radiological/Explosive (CBRE) Detection/protection. In: Roco, Mihail C. & Bainbridge, William Sims. Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation. 341ff.
[169] Europol. 2015. Exploring Tomorrow's Organised Crime. The Hague. 22.

certain time and in fact investigate the movement patterns of a suspect. If such data becomes available – and privacy concerns will no doubt form obstacles to the imminent use of these methods – Big Data analytics will facilitate predictive policing.

The potential role of Big Data, or better, Big Data Analytics, in policing and other types of intelligence collection is not yet properly understood. Big Data represents information assets characterised by high Volume (quantity), Variety (type of content), Velocity (speed at which the data is generated), and Variability (inconsistency of the data and its accuracy). Big Data Analytics can be defined as the specific technology and analytical methods for its transformation into Value. This working definition of Big Data is derived from its various characteristics, which has been referred to as the four Vs:[170]

Volume: The amount of data in datasets is very large, requiring multiple petabytes of storage.

Variety: Data is generated and collected from a number of distinct sources and more than one dataset is integrated and analysed.

Velocity: Data is being added to, deleted from, and/or transferred into datasets at different speeds and times depending on the type of data and collection methods.

---

170 AAAS-FBI-UNICRI. 2014. National and Transnational Security Implications of Big Data in the Life Sciences. Washington, DC: American Association for the Advancement of Science. 21. Cf. also Kosal, Margaret E.& Preston, Thomas. 18-21 February 2015. Contagion: The Peril and Promise of Big Data Analytics and Technological Advances in the Life Sciences for Biological Security. Paper prepared for International Studies Association Meeting. New Orleans. 5.

Variability: Datasets are incomplete, imperfect, and error-prone, and the data collected in these repositories is not standardised (also referred to as the veracity of data).

Big Data represents the information assets, while Big Data Analytics constitute the specific technology and analytical methods for the transformation of these assets into value, that is, intelligence products.[171] Such products will no doubt be increasingly common in a variety of situations in which intelligence is needed.

However, a major difficulty in implementing Big Data Analytics is the likely result of spurious correlations, that is, correlations without causal connection. Big Data Analytics will not reduce the need for experienced intelligence analysts in the loop.

A particular application of Big Data Analytics will no doubt be opinion mining, which could be used as a means to identify and prevent emerging riots and public unrest. If the data is made available to law enforcement, this would enable a potential revolution in policing and fighting serious and organized crime. Its adoption would allow law enforcement agents to prioritise their efforts and engage in truly intelligence-led policing. Big Data analytics would then reveal patterns in criminal activity and identify links between ostensibly unconnected events or criminal actors to an extent currently difficult or impossible, especially with regard to decentralised criminal networks and online networks.[172] It is indeed envisaged that accelerated developments in machine learning, algorithms, and sensors that track individuals, for instance through IoT, eventually will enable datasets,

---

171 De Mauro, Andrea & Greco, Marco & Grimaldi, Michele. 2015. What is big data? A consensual definition and a review of key research topics. http://dx.doi.org/10.1063/1.49 07823, accessed on 29 September 2017.
172 Europol. 2015. Exploring Tomorrow's Organised Crime. The Hague. 43.

at first used for marketing purposes, that can be used to create profoundly powerful models capable of predicting human behaviour, including individual behaviour. If used for policing purposes, this would greatly increase capabilities for crime prevention.[173]

Case Study: U.S. efforts in nanomaterials

Nanotechnology in the United States

The U.S. Department of Defense has stated that it began to sponsor research in nanoscience already in the early 1980s, since that was the time when research in this field began. It soon identified nanoscience and nanotechnology as one of six strategically important research areas. Several federal agencies, including the Department of Defense, joined the Interagency Working Group on Nanotechnology to evaluate and support research, and defence funding was organised to focus on three areas of nanotechnology deemed to be of critical importance: nanomaterials by design, nanoelectronics/magnetics/optoelectronics, and nano-bio devices. From a defence viewpoint, the Department of Defense regarded the areas of nanoelectronics, chemistry, and materials as most important to enhance warfighting capabilities.[174]

In 2000, the U.S. National Nanotechnology Initiative (NII) was launched by President Bill Clinton as an interagency programme to coordinate federal nanoscale science, engineering, and technology research and development (R&D) activities and related efforts among participating

---

173 Center for Long-Term Cybersecurity. 2016. Cybersecurity Futures 2020. Berkeley: University of California. 29-34.

174 Lau, Clifford . 2002. Nanotechnology and the Department of Defense. In: Roco, Mihail C. & Bainbridge, William Sims. Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation. 349-351.

agencies.[175] From FY2001 through FY2014, Congress appropriated approximately $19.4 billion for nanotechnology R&D. President Barack Obama proposed $1.5 billion in NNI funding for FY2015.[176] The NII was formed as a broad-based programme in nanoscience. It was intended to couple that programme with information technology and biotechnology. As a result, the coordinating offices for both the NII and the U.S. Information Technology Initiative (ITI) were co-located in order to encourage collaboration. The NII aimed to support progress in key areas of research, yet the funding depended on congressional decisions and was generally regarded as insecure.[177]

In fact, in the United States, commercial actors are the principal ones in nanotechnology. As a result, most developments so far have taken place regarding civilian applications and consumer products. However, some have dual-use applications.

When the NII was launched, it was envisioned that in twenty to thirty years' time, nano-bio-info-cogno (NBIC) technology would mature. Several Department of Defense programmes were then envisioned to integrate biomedical status monitoring technology, among them the ambitious 1991 Land Warrior programme.[178] In addition, NBIC technology would enable

175 Interagency Working Group on Nanoscience, Engineering and Technology, National Nanotechnology Initiative. February 2000. Leading to the Next Industrial Revolution. Washington, D.C.: Committee on Technology, National Science and Technology Council.
176 Sargent, John F. Jr. 16 December 2014. The National Nanotechnology Initiative. Overview, Reauthorization, and Appropriations Issues. Congressional Research Service, Report RL34401. 1, 7.
177 Murday, James. 2002. NBIC For Homeland Defense: Chemical/Biological/Radiologi cal/Explosive (CBRE) Detection/protection. In: Roco, Mihail C. & Bainbridge, William Sims. Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation. 352-355.
178 Etter, Delores M. 2002. Cognitive Readiness: An Important Research Focus For National Security. In: Roco, Mihail C. & Bainbridge, William Sims. Converging

the replacement of fighter pilots, either by autonomous systems or with the pilot-in-the-loop.[179] And indeed, drone technology has already changed the nature of low-intensity air power. The use of nanomaterials is very likely to continue the trend of the miniaturisation of sensors, electronics, information processors, and computers. This will reduce the weight, size, and power of UAVs. Since removing the pilot from combat aircraft will not only reduce the risk of death or injury but also further reduce weight, since devices, such as oxygen system, ejection system, or personal armour, will become unnecessary. Furthermore, combat UAVs will become more manoeuvrable and capable of more extended missions as well, and tasks, such as take-off and landing, navigation, and target identification, will be done autonomously. An autonomous situation awareness capability may become possible too. Of course, surface warships, submarines, tanks, and other combat vehicles may experience similar development. However, despite advances so far, there is still a long way to go for all these developments to take place.

State-of-the-art technology

Although nanotechnology deals with very small structures, nanomaterials can and will perhaps most often be employed in the construction of large, and indeed very large, platforms. Already at the beginning of the 21st century, the U.S. military services were looking into the use of nanoparticles in high-performance platforms and weapons. The idea was to

---

Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation. 330-337.

179 Lau, Clifford. 2002. Nano-Bio-Info-Cogno as Enabling Technology for Uninhabited Combat Vehicles. In: Roco, Mihail C. & Bainbridge, William Sims. Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation. 359-360.

embed small structures consisting of nanomaterials with special properties into larger structures, that is, warships, combat aircraft, and combat vehicles. Nanotechnology would thus enable combat equipment of greater stealth, higher strength, and lighter-weight structural materials. In addition to enabling higher performance, the use of nanomaterials would provide higher reliability and lower life-cycle cost.

The U.S. Department of Defense regards coatings, thin films, and advanced surfaces as particularly important aspects of systems, devices, and technologies critical to the services' warfighting mission.[180] Already in the early 2000s, the U.S. Navy was in the process of testing the use of nanostructured coatings in warships that were expected to dramatically reduce friction and wear. At the time, the U.S. Navy also was testing nanocomposites in which clay nanoparticles were embedded in polymer matrices for shipboard use, since such composites had been shown to have greater fire resistance.[181]

New coatings were also developed for the Air Force. By 2015, a plasma electrolytic oxidation (PEO) nanoceramic coating that provided an at least tenfold improvement of corrosion and wear resistance in missile launchers had been introduced following research by IBC Materials and Technologies Inc., who were under contract with the Air Force Research Laboratory's Materials and Manufacturing Directorate. The coating also resulted in a 27-percent improvement compared to current coatings concerning fatigue, and was announced to utilise green technology contrary to the current

---

[180] McQuade, Tyler. 2016. Local Control of Materials Synthesis (LoCo). Defense Advanced Research Projects Agency (DARPA). In: https://www.darpa.mil/, accessed on 29 March 2016.

[181] Lau, Clifford. 2002. Nanotechnology and the Department of Defense. In: Roco, Mihail C. & Bainbridge, William Sims. Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation. 349-351.

coating scheme, which includes anodisation, a primer, and a solid film lubricant (anodising has been the standard protective coating for aluminium and other light alloys but uses chromic and sulfuric acid, which produces hazardous byproducts, such as sulfuric acid fumes and aluminium hydroxide). Using only water-based, low-concentration electrolytes, which produce a significantly harder, denser and lower-friction ceramic coating with high corrosion resistance, the PEO coating was not only environmentally better but allowed for higher performance. The PEO coatings were thus qualified for the LAU-12X Advanced Medium Range Air-to-Air Missile (AMRAAM) missile launchers on F-15, F-16, F-18 and other combat aircraft platforms.[182]

Already in 2011, Lockheed Martin announced that its F-35 fighter jets will use carbon nanotube composite plastics – nanocomposites – in some structural parts, beginning with wingtip fairings.[183] Since then, nanocomposites are being increasingly used. Silicon carbide particulate-reinforced aluminium is used for F-16 ventral fins and as fan exit guide vanes for large turbofan engines on the 777 commercial aircraft. In situ metal matrix composites are used for the compressor inner shroud of the F-22 fighter's engine. Advanced super alloy materials are used in the engine of the F-15 and F-16 aircraft. Precision, high-performance ceramic bearings are used in gyros for F-18, AV-8, F-16, several helicopters, and in the bearings for IR seekers for the Navy Missile Homing Improvement Programme. The use of armour plates made of nanomaterials is also increasingly common. Ceramic composite armour was used to protect

182 Air Force Office of Scientific Research (AFOSR). 2015. Wright-Patterson Air Force Base. Press release of 20 April. In: www.wpafb.af.mil/news/story.asp?id=123445595, accessed on 29 March 2016.
183 Trimble, Stephen. 2011. Lockheed Martin reveals F-35 to feature nanocomposite structures. In: Flight Global, 26 May (www.flightglobal.com/news/articles/lockheed-martin-reveals-f-35-to-feature-nanocomposite-357223/), accessed on 29 March 2016.

flight crews in C-141 transport aircraft in Bosnia against small arms fire and, on the ground, for light armoured vehicles.[184]

A new battle dress was expected to be launched in 2015. It is based on Second Skin (a responsive uniform made of new fabrics, with aerosol protection and self-detoxifying characteristics), but has been delayed and therefore will be postponed for several years. The project was started with high ambitions. In addition to Second Skin, the new battle dress was to have chemical and biological (CB) protection with reduced thermal burden, to be based on multifunctional materials for protection, and to have integrated protection characteristics with active cooling and physiological monitoring.[185]

Another key project underway is the Uniform Integrated Protection Ensemble (UIPE), which concerns CB protective garments. Its objective is the transition to new fabrics and garment designs. This will include improved aerosol protection, a reduction in the logistical burden, and the increase in the physical and cognitive performance of the war fighter in Mission Oriented Protective Posture (MOPP) gear, that is, protective gear used in toxic environments. The plan encompasses characteristics, such as liquid shedding fabric to reduce agent load, self-detoxifying materials to minimise risks from agent residuals, and high-performance selective permeable membranes and absorption layers.[186]

---

184 Defense Advanced Research Projects Agency (DARPA). 2015. Materials Science: Advancing the Next Revolution of 'Stuff'. In: www.darpa.mil/news-events/2015-08-14, accessed on 29 March 2016.

185 Cf. Presentation of Robert Botto, Chief, Physical Sciences and Technology, DTRA, at the 2015 Chemical & Biological Defense Science and Technology Conference, St. Louis, Missouri 12 May 2015.

186 Ibid.

Yet another key project underway is Enhanced CB Survivability Coatings. Its objective is to develop an improved acceptance standard for chemical agent resistance, investigate new and more resistant, potentially reactive coatings, and develop a coating for aircraft with improved capabilities. The plan encompassed an update of the Chemical Agent Resistant Coating (CARC), a paint commonly applied to military vehicles to provide protection against chemical and biological agents, to a relevant acceptance standard for chemical resistance and the development of permanent or at least more durable coatings that also have reactive moieties to reduce residual risk.[187]

By 2015, there still remained doubts on when these projects would mature. Besides, ambitions remained high, possibly too high for easy implementation. Half serious, half in jest, a representative of the USAF concluded that, despite the high hopes for Second Skin, what the U.S. military really needed was the fictitious suit of the animated movie superhero, Mr. Incredible. That is, a bulletproof and flame-resistant protective suit that can be worn indefinitely under any climatic conditions.[188]

With such high ambitions, the possibility remains that research and development programme specifications and requirements are set unrealistically high. Scientists and the military have perhaps felt free to add too many improvements to the original needs. This is a well-known dilemma; one can always find new ways to improve the original plan, but as a result, the project is repeatedly delayed and takes years to mature. Besides, a personal observation is that, in the United States, cooperation between the Defense Threat Reduction Agency (DTRA) and the services, and

[187] Ibid.
[188] Cf. Presentation of Billy Mullins (USAF) at the 2015 Chemical & Biological Defense Science and Technology Conference, St. Louis, Missouri 12 May 2015.

between DTRA and the intelligence community, remains limited.[189] This is also a factor that keeps U.S. research and development from achieving its full potential in military and security applications based on nanomaterials.

In addition, scientists have observed that methods that enable atomic through millimetre-scale control over structure and properties of materials deposited on surfaces remain underdeveloped.[190] Furthermore and as a result, many of the expected improvements have not yet matured, despite a belief in the early 21st century that they would be in use by now (that is, within 10 to 20 years from 2001). For instance, in 2001 one such forecast assessed that, by now, national security would be "greatly strengthened by lightweight, information-rich war fighting systems, capable unmanned combat vehicles, adaptable smart materials, invulnerable data networks, superior intelligence-gathering systems, and effective measures against biological, chemical, radiological, and nuclear attacks."[191] While superior intelligence-gathering systems have emerged, in particular for counterterrorism, the rest still remains a forecast only.

Outlook for the year 2025: research and development potential and challenges for security forces

Although an early leader in nanotechnology, when it comes to practical applications, the United States – perhaps surprisingly – lags behind its own projections.

---

189 Roundtable on Threat Forecasting, Technology Watching, and Horizon Scanning. 2015 Chemical & Biological Defense Science and Technology Conference, St. Louis, Missouri 13 May 2015.

190 McQuade, Tyler. 2016. Local Control of Materials Synthesis (LoCo). In: https://www.darpa.mil/ Defense Advanced Research Projects Agency (DARPA). accessed on 29 March 2016.

191 Roco, Mihail C. & Bainbridge, William Sims. 2002. Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation. 4-5.

For instance, the United States had expected to launch its new battle dress in 2015. Based on Second Skin (a responsive uniform made of new fabrics, with aerosol protection, self-detoxifying characteristics, and so on), and for this reason presumably far more advanced than the equivalent new Russian battle dress (see below), it has been delayed and will have to be postponed several years.[192]

The United States has fallen behind in capability because since 2001 or 2003, depending on whether Afghanistan or Iraq is taken as starting point, the security focus was on counterinsurgency in these two countries and elsewhere. Thus, there was no necessity for a plan to fight in a contaminated environment or against a high-technology opponent.[193]

Some in the United States now believe that Early Warning technology for contaminated environments will have matured by 2020. Self-contained and wearable and/or disposable diagnostic systems, with no need for calibration or maintenance, will then be available to all personnel. However, others do not agree and believe that the introduction of mature warning technology will be postponed several years beyond this date.[194]

Concluding, in the short term (until 2020), applications of nanotechnology for security forces will remain incremental. However, in the medium term (until 2025), it is possible that one or more ground-breaking developments will have taken place, in particular with regard to operations in contaminated environments. In addition, nanotechnology will lead to

[192] Presentation of Robert Botto, Chief, Physical Sciences and Technology, DTRA, at the 2015 Chemical & Biological Defense Science and Technology Conference, St. Louis, Missouri 12 May 2015.
[193] Special Panel: Science and Technology (S&T) Meets the Warfighter. 2015 Chemical & Biological Defense Science and Technology Conference, St. Louis, Missouri 12 May 2015.
[194] Presentation of Rich Schoske on Diagnostic Detection Diseases at the 2015 Chemical & Biological Defense Science and Technology Conference, St. Louis, Missouri 12 May 2015.

improvements in firepower, protection, mobility, sensors, and command and control. Even so, it seems unlikely that the emergence of completely new systems will have an impact on security forces before 2025).

Case Study: Russia's efforts in nanomaterials

Nanotechnology in Russia

It was late that Russia became a major actor in nanotechnology, and then because of top-down initiative. Russia's President Vladimir Putin and especially Prime Minister Dmitry Medvedev, known for his great interest in nanotechnology, singlehandedly began the process. On 24 April 2007, President Putin presented a strategy for the development of nanoindustry.[195] In his annual address to the Federal Assembly two days later, Putin singled out nanotechnology as the locomotive of Russia's scientific and technological development strategy.[196]

The Russian Corporation of Nanotechnologies (Rusnano) was established in July 2007 by federal law to improve Russia's science and industry in the field of nanotechnology.[197] Rusnano invests in nanotechnology inventions and also helps them become commercial enterprises. In 2008, President Putin stated that nanotechnology could lead to revolutionary changes in weapons systems.[198] While this was only one, and not a major, part of his

195 Президентская инициатива – Стратегия развития наноиндустрии, № Пр-688, 24 April 2007.
196 Putin, Vladimir. 2007. Послание Федеральному Собранию Российской Федерации. In: http://archive.kremlin.ru/appears/2007/04/26/1156_type63372type63374type82634_125339.shtml, accessed on 29 March 2016.
197 Федеральный закон Российской Федерации от 19 июля 2007 г. N 139-ФЗ "О Российской корпорации нанотехнологий".
198 Putin, Vladimir. 2008. Выступление на расширенном заседании Государственного совета «О стратегии развития России до 2020 года», 8 February. In: http://archive.kremlin.ru/text/appears/2008/02/159528.shtml, accessed on 29 March 2016.

speech, it shows that the military potential of nanotechnology had not been forgotten.

However, the 2008-2009 global financial crisis had a severe impact on the Russian state budget. Besides, the sanctions imposed against Russia in 2014 and the falling oil price made it difficult to acquire international funding for major projects.

State institutions have remained the principal actors in Russian nanotechnology.[199] The dominant subject area of Russian nanoscience is physics, followed by chemistry and materials.[200] This is hardly surprising, since fundamental research and applicable science were strongly supported in the Soviet period. Besides, the generation of nanoparticles and nanostructured materials has a long tradition in the country, which makes this field an important part of current Russian nanotechnology programmes.[201] The Soviet Union also witnessed rapid development in the field of biotechnology,[202] including that of military applications. However, following the end of the Cold War, Russia's then President Boris Yeltsin (1991-1999) privatised the national biotechnology industry, which almost resulted in a near-collapse of the support for research and development and in the emigration of many leading scientists.[203] Moreover, Russian

---

199 Westerlund, Fredrik. 2011. Russian Nanotechnology R&D: Thinking Big about Small Scale Science. Stockholm: FOI. 13.
Karaulova, Maria et. al. 2014. Nanotechnology Research and Innovation in Russia: A Bibliometric Analysis. Project on Emerging Technologies, Trajectories and Implications of Next Generation Innovation Systems Development in China and Russia. Manchester Institute of Innovation Research, University of Manchester: Working Paper 2014.
200 Ibid. 23.
201 Swiss Business Hub Russia: Russia Nanotechnology. OSEC Business Network Switzerland, Moscow 2011.
202 "'Biotechnology' means any technological application that uses biological systems, living organisms, or derivatives thereof, to make or modify products or processes for specific use." UN Convention on Biological Diversity, Art. 2 (1992).
203 Roffey, Roger. 2010. Biotechnology in Russia: Why Is It Not a Success Story?

investments in nanotechnologies remained below those of the United States even before sanctions were imposed.[204]

By 2011, examples of Rusnano projects included Connector Optics, which was expected be a base for high-speed fibre optics production in Russia, producing fibre with a capacity of 80 gigabytes per second; Sitronics-Nano, which would produce 90-nanometer chips which, although not a world record, was the norm for microchips used in most modern electronic devices; Pruzhina, which produced springs far superior to others currently produced in Russia and with a projected lifespan close to 30 years, first intended for use in railway carriages where present springs had a lifespan of a few years only; and Danaflex, which would produce food packaging film with a coating that reduced the amount of air and moisture that could penetrate through the film, helping to preserve the food longer.[205]

State-of-the-art technology

The influence of nanotechnology on Russian military technology has, so far, been incremental. Besides, there is some doubt whether all of the announced projects in fact make use of nanotechnology.

Already in 2007, only months after President Putin had presented the strategy for the development of nanoindustry, Russia introduced and demonstrated the 'father of all bombs', claimed to be the world's most

---

Stockholm: FOI. 7.

204 Harper, Tim. 2011. Global Funding of Nanotechnologies & Its Impact. Cientifica (July). 3-4.

205 Dulnev, Nikita. 2011. Rusnano's big nanotechnology secrets revealed. In: http://rbth.com/articles/2011/08/03/rusnanos_big_nanotechnology_secrets_revealed_13216.html, accessed on 29 March 2016.

powerful thermobaric bomb, with a reported power equivalent to 44 metric tons of TNT. It was claimed that nanotechnology was a key element.[206]

Yet there were without doubt real results. For instance, at the Oboronekspo-2014 defense technology exhibition, RT-Khimkompozit, owned by the state corporation Rostekh, announced a cockpit window coating made of nanomaterials that would improve visibility by reducing disturbing light reflections, thus enabling better vision for the pilot; moreover it would reduce UV radiation, and thus cockpit temperature.[207]

Another example, which was Ukrainian but which was noted by Russian media, was an armoured fighting vehicle of the type BTR-3E1, which in 2014 was advertised as having a coating of nanomaterials that protect it from corrosion.[208] Military technology research and development until recently followed the same trajectories in Russia and Ukraine, with many cooperative efforts.

The new Russian multifunctional battle dress Ratnik ('combatant') was expected to be the standard from 2015 onwards. The Ratnik system is reported to incorporate improved Russian military/tactical 6B43 model ceramic hard armour plates (to chest and back) and tactical armour plate carriers (tactical vests). The 6B43 model plates are reportedly a titanium/boron carbide ceramic composite. Ratnik was already used in the

---

206 Reuters. 2007. Самая мощная в мире вакуумная бомба: российские испытания. In: www.1tv.ru/news/techno/67699, accessed on 29 March 2016.

207 На ОБОРОНЭКСПО-2014: РТ-Химкомпозит" представит новые уникальные разработки. In: http://vpk.name/news/115381_na_oboronekspo2014_rthimkompozit_predstavit_novyie_unikalnyie_razrabotki.html, accessed on 29 March 2016.

208 Харьковские ученые разработали нанопокрытие, благодаря которому БТР не "съест" коррозия. 2014. In: http://vpk.name/news/118088_harkovskie_uchenyie_razrabotali_nanopokryitie_blagodarya_kotoromu_btr_ne_sest_korroziya.html, accessed on 29 March 2016.

2014 annexation of Crimea.[209] The exact details of Ratnik remain unknown, but fabrics and composite materials would seem to be in part based on nanotechnology. Ceramic armour plates, manufactured by using boron carbide powder, and already used in the United States, were announced in 2013 by NEVZ-Soyuz, based in Novosibirsk. The company claims that the effectiveness of protection is five to six times higher, and the weight four times less than that of existing armour. Production costs are reportedly lower as well. Indeed, the same type of ceramic armour plates might be used to ensure anti-bullet protection on combat transport helicopters without sufficient original armour protection and combat vehicles.[210]

NEVZ-Soyuz is also reportedly developing ceramic bullets that would cost a fraction of lead-based ones. Ceramic bullets would also be ten times stronger than steal.[211]

Russian scientists claim to have developed highly durable materials, including liquid armour, which is developed by, among others, OAO NII Stali in Zelenograd.[212] Further developments using nano-materials are regularly reported as well in specialist forums.[213]

---

[209] Crane, David. 2014. Russian Nano-Armor Coming in 2015 for Future Soldier 'Warrior Suit', and Russian Spetsnaz (Military Special Forces) Already Running Improved 6B43 Composite Hard Armor Plates, New Plate Carriers and Combat Helmets, AK Rifle/Carbines, GM-94 Grenade Launchers and other Tactical Gear in Crimea, Ukraine. In: www.defensereview.com/russian-nano-armor-coming-in-2015-and-russian-spetsnaz-military-special-forces-already-running-improved-6b43-composite-hard-armor-plates-new-plate-carriers-ak-riflecarbines-gm-94-grenade-launch/, accessed on 29 March 2016.

[210] RIA-Novosti. 13 August 2013. Defense Review. 23 April 2014. In: www.defensereview.com. NEVZ-Soyuz Website. www.ru.nevz.ru

[211] DefenseReview. 23 April 2014.

[212] Разработки XXI века: "жидкая" броня. 2013. In: https://wf.mail.ru/news/407640.html, accessed on 29 March 2016.

[213] See, e.g., Новости ВПК. In: http://vpk.name/news/nano/new_dev/, accessed on 29 March 2016.

Outlook for the year 2025: Research and development potential and challenges for security forces

Despite great hopes, when it comes to practical applications in nanomaterials, Russia has not yet caught up with its competitors, nor lived up to its own projections. Even so, there have been some developments. For instance, the new Russian multifunctional battledress Ratnik became standard from 2015 onwards. While a less ambitious project than its U.S. counterpart, it had entered service already by 2014.

State institutions have remained the principal actors in Russian nanotechnology. As a result, Russia has lagged behind because of an emphasis on state-funded nanotechnology research programmes and financial difficulties directly caused by the Russian state's economic and other policies.

Concluding, in the short term (until 2020), Russian applications of nanotechnology in the Russian security forces will remain incremental, as will American applications. However, in the medium term (until 2025), it is possible that one or more ground-breaking developments will have taken place, again, in particular with regard to operations in contaminated environments. In addition, nanotechnology will lead to improvements in firepower, protection, mobility, sensors, and command and control. Even so, it seems unlikely that the emergence of completely new systems will impact security forces before 2025).

Scenarios regarding the misuse of nanomaterials technology against individuals or societies, states, and their security apparatuses

Toxic nanomaterials accidentally released during armed conflicts

There is no provision in current nanomaterials technology for self-replication, so there is little opportunity for misuse that would actually entail disruptive consequences.

However, some nanomaterials are highly toxic. They could thus cause environmental damage, in particular during battlefield usage or after being decommissioned. Products that contain nanomaterials may accordingly require special end-of-life recycling procedures.[214] It has also been noted that nanomaterial coatings containing nanoparticles release a certain amount of the latter over time. However, the volume released depends on the type of nanoparticle. While, for example, only a very small amount of titanium dioxide nanoparticles would be released, as much as 30 per cent of silver nanoparticles may be lost, in comparison. The release follows from normal usage. For instance, nanoparticles in textiles are released through washing.[215] It follows that special cleaning and detoxification procedures will have to be conducted. However, it cannot be taken for granted that the armed forces of great powers would see this as an imperative in times of emergency.

Moreover, under the conditions of armed conflict, the imperative will always be on winning the conflict and saving the lives of friendly soldiers.

---

[214] Manyika, James et. al. 2013. Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy. McKinsey Global Institute.122.

[215] Part, Florian & Greßler, Sabine & Huber-Humer, Marion & Gazsó, André. 2015. Umweltrelevante Aspekte von Nanomaterialien am Ende der Nutzungsphase – Teil I: Abwässer und Klärschlamm. NanoTrust-Dossiers 43.1-6.

As a consequence, there will be less emphasis on recycling procedures, and toxic materials will be lost, abandoned, or dumped.

This is a 'known known' scenario and assessed as very likely.

Opportunistic use of nanomaterials by groups of organised crime

In the same way military and law enforcement benefit from applications which include nanomaterials, it must be expected that groups that are part of organised crime will also find ways to take advantage of them. As in all types of emerging technologies, the technology barrier will gradually be eroded, as deskilling takes place. Deskilling is the process by which skilled labour within an industry is eliminated by the introduction of technologies operated by semiskilled or unskilled workers. Within organised crime, deskilling can be said to take place when technology allows semiskilled members of the group to carry out work which formerly could only be handled by highly skilled personnel, such as laboratory technicians.

Currently a number of territories exist in which organised crime has access to advanced technology and communications networks as well as sufficient freedom of action to make full use of technological advances. Contested parts of the industrialised regions of Central Asia and the Caucasus come to mind, as well as the tri-border region of Argentina, Brazil and Paraguay, major parts of Pakistan, including urban areas with advanced research institutes, and Ukraine, a country which until recently shared a military nanotechnology base with Russia.

Organised crime will no doubt find numerous uses for nanomaterials. First, it can be expected that nanomaterials will be used to develop or alter drugs and psychoactive substances. Second, organised crime groups can be expected to take advantage of the developing market in nanotechnologies to produce counterfeit versions of legal pharmaceuticals and devices.[216] While designer drugs are likely to remain a lucrative market, the trade in counterfeit drugs and devices may become the more important criminal activity, since the trade is lucrative while the risk of prosecution and imprisonment is significantly lower.

But the key advantage of nanotechnology for groups of organised crime, compared with that of conventional technology, would be the possibility of committing complex and sophisticated identity frauds at a scope yet unprecedented.[217] A key cause is the increasing exploitation of Big Data and personal data for criminal purposes. There are already groups of cybercriminals that provide complete stolen identities to interested buyers, usually for the purpose of various kinds of fraud. In the future, it can be expected that such a data packages will consist of yet more comprehensive information, including the complete biography, personal details, photographs, credit card information, as well as the biometrical data of an individual.[218] In view of the expected developments in machine learning, algorithms, and sensors tracking individuals, for instance through IoT, models capable of predicting human behaviour, including individual behaviour, will be developed. Organised crime will find ways of using data to manipulate individual behaviour, for fraud, blackmailing, kidnapping, or other hostile purposes.[219] Terrorists would attempt to break or hack into IoT systems that handle traffic control or other critical infrastructure, in order to carry out spectacular attacks killing large numbers of people.[220]

---

[216] Europol. 2015. Exploring Tomorrow's Organised Crime. The Hague. 22.
[217] Ibid. 19.
[218] Ibid. 20.
[219] Center for Long-Term Cybersecurity. 2016. Cybersecurity Futures 2020. Berkeley: University of California. 29-34, 71-79.
[220] Ibid. 83-86.

Naturally, within the broader field of nanotechnology there are additional threats. The convergence between biotechnology and Big Data Analytics will present opportunities to terrorist groups and, perhaps more importantly, lone-actor terrorists, particularly in the form of disgruntled scientists.[221] There have already been cases of insider lone-actor terrorists who managed to shut down important government institutions, which highlight the potential of advanced materials for disrupting or halting government, military, or commercial activities.[222] New forms of high-end bioterrorism might come in many shapes, including antibiotic-resistant bacteria that would interfere with first line treatment. More advanced forms of bioterrorism might involve the introduction of immune system modifiers that block vaccine efficacy, targeted modifications of existing viruses, or even the reconstitution of formerly deadly viruses such as smallpox. By such means, the introduction of diseases such as anthrax and particularly influenza would be more plausible, more effective, and thus entail higher risk.

Finally, one should bear in mind that organised crime is opportunistic and often innovative. Some envisage a new dot-com bubble burst, with the advertising-driven business model for major Internet companies falling apart. This would result in a situation in which, as companies fail, employees at risk of losing employment would be increasingly tempted to steal valuable datasets, including those that pertain to privacy and financial services. It would not only be the datasets that would be of interest to organised crime; the dispossessed employees of the tech-industry would be

---

[221] Kosal, Margaret E.& Preston, Thomas: Contagion. 2015. The Peril and Promise of Big Data Analytics and Technological Advances in the Life Sciences for Biological Security. 2015. Paper prepared for the International Studies Association Meeting, 18-21 February 2015. New Orleans. 12-13.

[222] Fredholm, Michael. 2016. Understanding Lone Actor Terrorism: Past Experience, Future Outlook, and Response Strategies. New York: Routledge. 225-226.

of interest too, since they can be put to good use in criminal schemes.[223] For instance, it can be expected that increased dependence of the manufacturing and healthcare industries on robotics will create new vulnerabilities, which can be exploited by criminals, for instance via computer-based extortion. Even small, almost undetectable degradation along a product's supply chain may cause substantial damage to a company employing robotics. Since few individuals will have the requisite technical skills to enable such exploitation, this type of crime may be the result of a convergence between organised crime and terrorism, including lone actors with the necessary expertise and a grudge against a particular employer or society as a whole.[224]

When it comes to terrorism, any technology adopted for military use will eventually also be employed by terrorists. Terrorists have already begun experiments with unmanned drones, and the eventual use of nanomaterials, pilfered or otherwise derived from industries or security forces, will become part of their repertoire. What can be built, eventually will be built.

Off-the-shelf technology is not always so difficult to counter, and toxic effects are usually anticipated. However, security forces are often unprepared for the effects of new or improvised toxic materials. Existing sensors used to detect CB agents may not be correctly calibrated against new, improvised agents, since the properties of the latter have not yet been assessed.

This is a 'known unknown' scenario and assessed as very likely.

---

223 Center for Long-Term Cybersecurity. 2016. Cybersecurity Futures 2020. Berkeley: University of California. 51-7, 65-66.
224 Europol. 2015. Exploring Tomorrow's Organised Crime. The Hague. 21-22.

State programmes cut corners and accidentally release toxic nanomaterials

It cannot be assumed that state programmes for research into nanomaterials for military and security forces always will behave responsibly. In fact, large government administrations tend to handle their own operational security somewhat randomly, since they often consider themselves as not subject to petty regulation. Besides, national security is often believed to surpass operational and environmental security.

As a result, accidents happen, especially when corners are cut in the name of deadlines, budget restrictions, or the perception of urgency for national security. There tends to be no warning for this kind of incident. The accident or transgression may also be hushed up, so as not to reveal what went wrong.

This is an 'unknown unknown' scenario and assessed as likely.

The remaining enigma: Chinese nanotechnology

Not all developments within state-controlled military nanotechnology programmes are released to the public. There are always a certain number of 'black' or classified programmes. For this reason, tracking actual developments in U.S. and Russian military nanotechnology programmes is somewhat difficult. However, it is even harder, at least for researchers who lack Chinese language skills, to gain an insight into the applications of nanomaterials technology in China's armed forces. China is a major centre of nanotechnology research, and much of it is not made public in foreign languages. In 2011, China surpassed the United States as the largest funder of nanotechnology research in dollars. According to Tim Harper's estimates, in Purchasing Power Parity (PPP) terms China spends US$2.25 billion in nanotechnology research while the United States spends US$2.18

billion. However, Harper argued, in real dollar terms, adjusted for currency exchange rates, China was only spending about US$1.3 billion.[225]

Even so, Chinese investments are impressive, and it could be argued that China combines the funding policies of the United States and Russia. China makes substantial state investments, but its industry is simultaneously developing nanomaterials for the consumer market. This might bring benefits also for security applications. However, little seems to be published in Western languages on Chinese applications of nanomaterials technology in the security field.

This scenario is an 'unknown known' scenario and the potential for misuse is assessed as likely, since it involves state programmes.

Conclusions

Nanomaterials have brought incremental improvements in military technology and power projection and will lead to improvements in firepower, protection, mobility, sensors, and command and control. However, when it comes to the practical application of nanomaterials technology in the military field, both Russia and the United States lag behind their own projections.

State institutions remain the principal actors in Russian nanotechnology, while commercial actors are the principal ones in U.S. nanotechnology. As a result, most developments so far have taken place regarding civilian applications and consumer goods. However, some products involve dual-use application.

---

225 Harper, Tim. 2011. Global Funding of Nanotechnologies & Its Impact. In: http://cientifica.com/wp-content/uploads/downloads/2011/07/Global-Nanotechnology-Funding-Report-2011.pdf 3-4.

Russia has been lagging behind because of financial difficulties and an emphasis on state-funded nanotechnology research. The United States has fallen behind in capability because since 2001, the security focus has been on counterinsurgency in Iraq and Afghanistan and there was no real contingency plan to fight in a contaminated environment or against a high-tech opponent.

Some in the United States now believe that Early Warning technology for contaminated environments will have matured by 2020. Self-contained and wearable and/or disposable diagnostic systems with no need for calibration or maintenance will then be available to all personnel. However, others do not agree and believe that the introduction of sophisticated warning technology will be postponed several years beyond this date.

Concluding, in the short term (until 2020), the application of nanomaterials technology in the security forces will have an incremental impact on capabilities. However, in the medium term (until 2025), it is possible that one or more ground breaking developments will take place. Besides, the increased use of nanomaterials will likely lead to further improvements in firepower, protection, mobility, sensors, and command and control. In particular, developments can be expected with regard to operations in contaminated environments. Even so, it seems unlikely that the emergence of completely new systems will have an impact on security forces before 2025. There are no indications that any truly significant changes, such as a revolution in military affairs (RMA), will take place until several years beyond this date. Michael O'Hanlon's cautious forecast in 2000 that a revolution in military affairs does not appear within reach today remains essentially confirmed.

In modern history, military needs have often pushed technology, in particular in situations when countries are faced with existential threats, such as during the two World Wars and the Cold War. Moreover, the adoption of new military technologies can never be taken for granted, except in times of existential threat. First, the cost of the adoption of a new technology will have to be offset by cuts in another programme. Implementing nanotechnology will necessarily include an economic parameter, which is difficult to forecast. Will the gains produced be regarded as motivated by the higher costs? Second, the organisational culture must be receptive to the adoption of new technology, even if it disrupts existing traditions and doctrine.

Nanomaterials also present significant opportunities for policing. There will be an emphasis on sensors and forensics in police investigations, but nanomaterials may also play a major role in the use for policing purposes of Big Data and, in time, the IoT. Devices such as telephones and personal computers are already used by law enforcement to locate suspects, and the ability to do so will grow. Accelerated developments in machine learning, algorithms, and sensors that track individuals, for instance through IoT, will eventually enable datasets that will greatly increase capabilities in crime prevention.

When does converging technology in the form of nanomaterials applications represent a threat or a risk for individuals or the society of a small state, as well as for security forces in the defence of the state or first responders faced with hazardous threats? There are a number of potential scenarios for which Early Warning and Situational Awareness are mandatory and preparations needed. First, toxic nanomaterials are very likely to be released during armed conflicts. Second, groups of organised crime are very likely to make use of nanomaterials for a variety of criminal purposes whenever the opportunity arises. Third, state programmes are likely to transgress rules and accidentally release toxic nanomaterials. In addition to these threats, it should be borne in mind that little information on Chinese development efforts in nanomaterials in Western languages is currently available.

In particular, the threat from organised crime is often overlooked in the assessment of military and security technology. Currently, organised crime has access to advanced technology and communications networks as well as sufficient freedom of action to make full use of technological advances in a number of territories throughout the world, including contested parts of the industrialised regions of Central Asia and the Caucasus, the tri-border region of Argentina, Brazil and Paraguay, major parts of Pakistan, including urban areas with advanced research institutes, and the Ukraine, which until recently shared a military nanotechnology base with Russia. Organised crime is opportunistic and often innovative. There is also a threat from terrorism, including lone-actor terroristic acts carried out by insiders from nanotechnology research institutes. Any technology adopted for military use will in time also be employed by terrorists. What can be built, eventually will be built.