



Ethical and Societal Aspects of Nanotechnology Enabled ICT and Security Technologies

WP4, Ethical and Societal Aspects, Annual Report 3

Ineke Malsch and Anne Mette Frøelund Andersen, 20-04-2011, postbus@malsch.demon.nl

Abstract

The third annual report on Ethical and Societal Aspects of Nanotechnology of the ObservatoryNano project focuses on ethical and societal aspects of Nanotechnology, ICT and Security. These issues are either raised by new technological trends or currently discussed in policy or stakeholder debates or in ethical, philosophical or social science literature. In this general domain, three main areas can be distinguished:

- 1) Ethical and societal aspects of nanoelectronics and ICT,
- 2) Ethical and societal aspects of nano-enabled civil security, and
- 3) Civil / military dual use of nanotechnology.

For each of these three areas, the following four key questions are examined:

- a) Which ethical and societal issues are raised by current technical and economic trends in nanoelectronics and nanotechnology for security applications?
- b) Which relevant issues are currently being debated by policy makers and stakeholders? Which issues apparent from the technical and economic trends are not discussed sufficiently?
- c) What are the issues discussed by ethicists and social scientists writing about nanotechnology? Which new insights do they have to offer for the policy and stakeholder debate?
- d) What are new issues for the debate and who could do what?

It turns out that trends in nanoelectronics and nanotechnology for ICT and security applications have contributed to new issues for the debate related to research ethics, value sensitive design and ubiquitous computing. Specifically in relation to security applications of nanotechnology, surveillance, security and privacy enhancing design of security technologies are issues under discussion. Four general current debates on civil-military dual use may also be relevant to governance of dual use nanotechnology: on the relation between civil and military R&D, on definitions of dual use, on non-proliferation of dual use goods and technologies, and on military robots.

Table of contents

Ethical and Societal Aspects of Nanotechnology Enabled ICT and Security Technologies	1
WP4, Ethical and Societal Aspects, Annual Report 3.....	1
Abstract	1
Table of contents	2
Executive Summary	3
1. Introduction	5
2. Ethical and societal aspects of nanoelectronics and ICT	6
2.1 Which ethical and societal issues are raised by current technical and economic trends in nanoelectronics and ICT?.....	6
2.2 Which relevant issues are currently being debated by policy makers and stakeholders? Which issues apparent from the technical and economic trends are not discussed sufficiently?.....	9
2.3 What are the issues discussed by ethicists and social scientists writing about nanotechnology? Which new insights do they have to offer for the policy and stakeholder debate?.....	14
2.4 What are new issues for the debate and who could do what?	17
3 Ethical and societal aspects of nano-enabled civil security	19
3.1 Which ethical and societal issues are raised by current technical and economic trends in nanotechnology for civil security applications?.....	19
3.2 Which relevant issues are currently being debated by policy makers and stakeholders? Which issues apparent from the technical and economic trends are not discussed sufficiently?.....	20
3.3 What are the issues discussed by ethicists and social scientists writing about nanotechnology? Which new insights do they have to offer for the policy and stakeholder debate?.....	22
3.4 What are new issues for the debate and who could do what?	25
4 Civil / military dual use of nanotechnology	26
4.1 Which ethical and societal issues are raised by current technical and economic trends in nanotechnology for dual use applications?	26
4.2 Which relevant issues are currently being debated by policy makers and stakeholders? Which issues apparent from the technical and economic trends are not discussed sufficiently?.....	27
4.2.1 Relation civil-military security R&D	28
4.2.2 Weapons and Materials of Mass Destruction.....	28
4.3 What are the issues discussed by ethicists and social scientists writing about nanotechnology? Which new insights do they have to offer for the policy and stakeholder debate?.....	33
4.4 What are new issues for the debate and who could do what?	36
Acknowledgement.....	38
References	38
Annex 1: list of issues identified in technical and economic reports by ObservatoryNano, Nov 2008, May 2009, Dec 2009	44
Annex 2: relevant issues in policy / stakeholder debate.....	46

Executive Summary

In this report, public debates and literature on ethical and societal aspects of nanotechnology in ICT and security, and civil-military dual use aspects of nanotechnology are discussed. The main aim is to identify new or persistent issues in these debates that merit the attention of policy makers responsible for nanotechnology in Europe. Another aim is to raise awareness of these issues among the partners in the ObservatoryNano project responsible for reports on technical and economic trends in two of the ten technology sectors covered by the ObservatoryNano: ICT and security.

In general, there is a wide gap between the world of policy makers and stakeholders in nanotechnology and the worlds of policy makers and stakeholders, and ethicists and social scientists concerned with ICT, privacy, security and dual use issues. Many ethical and societal issues related to ICT, civil security technology and military technology date back to before nanotechnology started to be applied there. Even when issues are relatively recent, they tend to be related more to software, services or political aspects than to technological developments of hardware. When nanotechnology enters debates or literature on ethical or societal aspects, it is mostly in a rather superficial way. Applications of nanotechnology are mentioned that could give rise to new issues or that could make existing issues more pressing. One example is nanobiotechnology as a potential new biosecurity threat. Another example is communicating nanochips implanted in the human body as the ultimate Big Brother technology bringing all citizens under constant surveillance by a dictatorial regime. The likelihood of such nano-threats is usually not explored in any depth. There is a potential that such speculations when left unaddressed could lead to public backlash against nanotechnology as a whole. Therefore it might be wise to analyse the likelihood and existing regulations and other mechanisms to prevent such horror-scenarios in a multidisciplinary project or expert workshop.

Trends in nanoelectronics and nanotechnology for ICT have contributed to new issues for the debate related to research ethics, value sensitive design and ubiquitous computing. Experts and policy makers have called for accompanying ICT research with research in ethical, legal and social aspects and for targeting research to societal needs. The second recommendation appears to have been implemented more than the first. This illustrates a general trend that the distance between technological developments and research and debate on ethical and societal issues is considerably larger in ICT than in the life sciences. The European Commission could adapt the guidelines for ICT research ethics and call for integration of ELSA in EU funded ICT research. The EU funded PRISE project mentioned in paragraph 3.3 could serve as an example. Researchers and companies could include ELSA boards in their networks and technology platforms. Among engineers and companies engaged in nanoelectronics and ICT, value sensitive design is becoming increasingly popular. However, ethicists have pinpointed dilemmas including which values would be acceptable in design and who should decide on this. There is a lack of interaction between engineers and ethicists and a lack of public debate. The European Commission could organise workshops bringing together engineers and ethicists to discuss value sensitive design and initiate public dialogue projects. Regulatory and privacy issues related to RFID and the internet of things have entered the political agenda in Europe. However, there may be a need for broadening this to encompass more general societal trends influenced by ubiquitous computing. Parliamentary Technology Assessment organisations could organise public discussions on ubiquitous computing.

Security applications of nanotechnology have given rise to more or less the same concerns as ICT applications. In addition, surveillance, security and privacy enhancing design of security technologies are issues under discussion. Policy makers could take suggestions for interpretations of the concept of privacy and guidelines for research ethics by ethicists and social scientists into account in their

deliberations on new policies and regulations. The research community could take both into account in their efforts towards privacy enhancing design of security technologies.

Dual use aspects of nanotechnology should primarily be addressed by policy makers and politicians. Researchers and companies can only play subsidiary roles including respecting the law, raising awareness of legal requirements and ethical norms among students and voluntarily taking responsibility for new emerging threats by informing authorities or starting public debates. There are four general current debates that may also be relevant to governance of dual use nanotechnology: on the relation between civil and military R&D, on definitions of dual use, on non-proliferation of dual use goods and technologies, and on military robots. Regarding the changing relation between civil and military R&D in future European research, policy makers could open up consultations to a wider audience including civil society, the research community and industry. Other actors could actively engage themselves in this debate. The European Group on Ethics could take this discussion of definitions of dual use into account in their requested opinion on ethics of security research. In relation to non-proliferation, policy makers could install a monitoring body to assess progress in relevant technologies on a regular basis, as proposed by scientists for life sciences relevant to the BTWC convention. Awareness of dual use aspects of nano-enabled miniaturisation of robotics could be raised among researchers and policy makers by tabling discussions in relevant conferences.

1. Introduction

This report examines current trends in the co-evolution of nanotechnology and society related to nanotechnology, ICT, privacy and security. The aim of the report is to highlight new or persistent issues currently in debate that merit the attention of politicians and policy makers engaged in decision making on nanotechnology for information and communication and for security. The report is not intended to present a new vision of the ObservatoryNano project on these issues, but to identify significant issues and views discussed by others.

The sectors covered in this report are two of the ten technology sectors where nanotechnology is being applied which are analysed in the ObservatoryNano project. The other sectors are Aerospace, Automotive & Transport, Chemistry & Materials, Construction, Energy, Environment, Health, Medicine & Biotechnology, Agrifood and Textiles. Some of these areas have given rise to specific ethical or societal issues discussed by policy makers and stakeholders or in the philosophical and social science literature. These include the topics of this year's annual report on Ethical and Societal Aspects of Nanotechnology for ICT and Security.¹ Last year's report focused on Ethical and Societal Aspects of Nanotechnology for Health, Medicine and Biotechnology and for Agrifood. The other reports in this series on ethical and societal aspects of nanotechnology focus on more general issues including responsible development of nanotechnology (1st annual report) and communicating nanoethics (4th annual report). The report will be made available to European policy makers on nanotechnology and others via the website www.observatorynano.org.

The authors of this report choose to discuss Ethical and Societal Aspects of Nanotechnology, ICT and Security, including civil security and dual use applications of nanotechnology from the point of view of a technical perspective. This is because the role of the ObservatoryNano is primarily to make information on (non-military) technological and economical trends in nanotechnology and their broader implications available to policy makers. It should be noted that this is one particular methodological approach. In an equally valid approach, one could choose to take the ethical and social consequences of R&D of nanotechnology as starting point, leading to a completely different classification (e.g. military, monopoly, concentration of wealth, labour qualification, etc.) The European Union does not fund military research under the Framework Programme for RTD and therefore also no research into societal aspects of purely military research. Research into societal aspects of dual use technologies is permitted under the Framework Programme. Military research is the responsibility of the EU Member States and the European Defence Agency (EDA).

¹ It has been suggested to include also aerospace applications of nanotechnology in the present report, but the relevant nanotechnological trends identified by ObservatoryNano are more related to general transport and automotive applications, and not related to discussions of dual use of aerospace technologies. Therefore the discussion on civil / military dual use in this report is more general including trends in nanotechnology for aerospace applications and other technologies.

2. Ethical and societal aspects of nanoelectronics and ICT

The discussions on ethical and societal aspects of nanoelectronics and ICT tend to focus on how ambient intelligence, also called ubiquitous computing, changes the organisation of society and how people communicate and interact with each other. Fiedeler² (Austrian Institute for Technology Assessment ITA) remarks that these issues are not new and have been discussed since several years in the “Begleitforschung” (accompanying research) of ICT. Nevertheless there are two strong relations to nanotechnology. First, nanotechnology will enhance the miniaturisation of electronic devices and second some people are concerned about nanotechnology and that it will lead to similar problems as other Information and Communication Technologies.

Key issues on the political and stakeholder agenda are privacy and data protection. The emerging ‘internet of things’ has also given rise to new policy issues. This term refers to the increasing integration of electronic chips in ordinary objects that enable connecting these objects to the internet. E.g. fridges that can order milk automatically or RFID chips or other (nano)electronics in textiles, cardboard or other products that enable tracking the user who is not aware of this. More in general, computer ethics and how human rights and human dignity are affected by ICT are also relevant to the discussion on nanoelectronics.

2.1 Which ethical and societal issues are raised by current technical and economic trends in nanoelectronics and ICT?

As this chapter focuses on the ethical and societal aspects of applications of nanotechnology in ICT, this section gives an overview of the expectations expressed by a variety of actors of future implications of current trends in nanoelectronics and nano-enabled ICT. The underlying technical and economic trends are presented in General Sector Reports and Briefings on Nanotechnology for Information and Communication (ObservatoryNano, 2009b) Because of the indirect relationship between technological trends in nanoelectronics and ethical and societal implications of ICT systems and applications, it is not very useful to discuss the technological trends by themselves in the present report. In stead, the expert views on potential ethical and societal issues are taken as starting point. The downside is that this gives room for speculation.³

The field of nanoelectronics is dominated by the same technology push dynamics as the general area of information and communication technologies. This technology push trend in nanoelectronics transforms society on a macroscopic scale and promises to solve societal problems defined by the proponents of the technology rather than by a wider community of societal stakeholders. Several general trends have given rise to ethical and societal issues and debates for the past decades. These issues remain valid when nano-electronics is applied in the same or similar products and systems. These traditional issues include ubiquitous computing applications including RFID tags that raise privacy issues. (ObservatoryNano, Roco 2010) Other more general controversy relates to human-machine interactions, especially where sensors are placed inside the human body, and robotics. Regarding applications of nanotechnology and other technologies in neuro-implants, Fiedeler (2008) has critically examined the state of the art of such implants in order to distinguish likely scenarios from hype. Especially progress in deep brain stimulation would merit more research into ethical and societal issues. (Fiedeler, 2008)

² Personal communication, March 2011

³ A body of literature criticises “speculative ethics” (e.g. Nordmann & Rip 2009, Fiedeler 2008a), but discussing this goes beyond the scope of this report.

Life cycle analysis of the environmental impacts of electronics products and the interpretation of the precautionary principle are even more general issues. Below, the issues in the current discussions of relevant nanotechnologies are first explored. Subsequently, more background is given in a brief historical overview of expectations of societal impacts of nanoelectronics in the last decade.

Recent trends in nanoelectronics and applications of nanotechnology in ICT that may give rise to new or more severe ethical and societal issues include quantum computing and sensing nanoinformatics, nanophotonics and plasmonics (incl biosensing, magnetic recording, cancer treatment, etc.) and carbon electronics. (Roco 2010) Converging ICT and cognitive sciences in new research aimed at bioinspired and biomimetic assembly (Roco, 2010 p 80) or more in particular mimicking the brain or engineering the brain/body/biology (van Est et al. 2010) are also the topic of more recent policy and stakeholder debates.

Bio-ICT (cell level) requiring major advances in interfacing ICT with biological systems at the micro-nanoscale was recommended as a priority for Future and Emerging Technologies (FET) Pro-active research under the EU IST programme 2009-2013. In addition, other controversial topics such as embodied ICT (system level, call in 2011) and neuro-ICT (call in 2009/10) were recommended by the ISTAG advisory group 2008-2009. Societal awareness should be raised about the potential benefits of the new technologies; the report did not mention taking into account societal or ethical concerns in proposed research. (ISTAG, 2009) A related new area of research is biophotonics, utilizing light based technologies in medicine and life sciences. The EU funded project Photonics4Life (P4L) includes an ethics board that explores regulatory and ethical issues related to the research and maintains contacts with patients groups. (P4L, 2010)

The European Commission (EC, 2009) published a Communication on the FET strategy (research strategy for Future and Emerging Technologies). This included a proposed call for major scientific challenges for cooperation across disciplines. Disciplines could include biology, chemistry, nanoscience, neuro- and cognitive science, ethology, social science, economy and arts and humanities. Recent projects include Virtual Physiological Human (VPH) and Blue Brain, that were discussed critically by Technology Assessment specialists (van Est et al., 2010).

In the framework of the above-mentioned VPH project, the Action-Grid project reports the emergence of a new sub-area of nanotechnology: nano-informatics, which extends biomedical informatics to nanomedicine. "Nano-informatics refers to the use of informatics techniques for analysing and processing information about the structure and physico-chemical characteristics of nano-particles, their interactions with their biological environments, and their applications." Five scientific grand challenges are distinguished:

- data and knowledge storage and management incl. new bio-nano repositories for standardisation
- nano-ontologies and semantic search & interoperability, providing new infrastructure and methods for integrating nano-related data and information systems
- extension of the scope of VPH including modelling and simulation at nanolevel, e.g. nanoparticles in the human body
- inclusion of a new area: "translational nano-informatics"
- extension of traditional electronic health records to include nano-related information for diagnosis, therapy and analysis of potential toxic effects of nanoparticles

The first nano-informatics meeting was organised by NSF in Virginia, USA in 2007. (Action-Grid, 2010 p 59, 62)

After a call for pilot projects for FET Flagships end of 2010 (to prepare future large public-private research programmes each worth €100 million), 6 pilot projects are expected to be launched in May

2011. This should result in the selection of 2 Flagships in 2013. The 6 pilots are FuturICT⁴, Graphene-CA, Guardian Angels, HBP-PS (Human Brain Project-Preparatory Study), ITFoM (Medicine of the Future: Molecular Modelling in Medicine, Aging and Drug Safety) and CA-RoboCom (robot companions for citizens). In addition, a horizontal FLEET project studies ethical aspects.⁵

Recent history of expectations of societal impacts of nanoelectronics

Since the beginning of the 21st century, foresight exercises of developments in nanoelectronics and its applications have highlighted several ethical and societal issues that could be raised by these trends. The feasibility of the expectations has not been examined. They are presented here because the expectations play a role in decision making on research strategies, independent from their feasibility.

In 2001, the IST Advisory Group (ISTAG) to the European Commission proposed four “scenarios for ambient intelligence in 2010” in preparation of the EU FP5 IST programme. Among the required enabling technological developments was very unobtrusive hardware including fully optical networks, nano-micro electronics, power and display technologies. Several foreseen social aspects of Ambient Intelligence were deemed to “require precautionary research, particularly in the areas of privacy, control and social cohesion. In addition, encouragement may be needed to develop forms of Ambient Intelligence that are sensitive and adaptive to societal development and the diversity of European social, political and cultural life.” (Ducatel et al, 2001, p 9) These issues have been taken into account in later EU IST policies according to Aarts & Grotenhuis (2010).

An NSF sponsored expert conference held in 2003 in the United States concluded that nanoelectronics applications including smart dust sensors, bacteria-size microprocessors, high density data storage and high speed data communications could contribute to “the ultimate interconnected environment”, and give rise to new or enhanced privacy issues. The opportunities created to store almost unlimited amounts of data gives rise to new issues including ownership of the data and restrictions on use. (Roco & Bainbridge, 2003)

In 2006, a similar study by the European Science Foundation (ESF, 2006) foresaw long term impacts of applications of nanoscience in Information Technology on everyday life. Nanoscience could play a role in several trends, including not only miniaturisation, but also power supply for nomadic or embedded systems enabling ambient intelligence, increasing complexity and links with biology / convergence such as understanding the brain, the interface between the central nervous system and IT, and the creation of ‘intelligent’ machines mimicking the brain. Nanoscience was deemed to be a crucial enabler of new market paradigms like ‘objects as virtual consumers’ (beyond 2020). Potential societal impacts include safety and security of data and ethical issues such as privacy, impacts of new use, the social role of intelligent systems replacing experts, bioethics issues and economic impacts. ESF recommended accompanying ICT research with social science research to investigate the human factor including implications of new products. In addition, long term societal aims for ICT programmes should be formulated including health, safety, culture, e-democracy, helping disabled people etc. Communication, trust building and anticipation of potential consequences were also deemed necessary. (ESF, 2006)

A few years later, an expert workshop on nanoelectronics (EC, 2009) highlighted a change in the dynamics in the field. In the early stages, drivers for nanoelectronics used to be miniaturisation and cost reduction. From about 2009, the main trends were expected to be ultra low power nanoelectronics with novel functionalities, energy efficient design, miniaturisation and reliability, and

⁴ The FuturICT project will include an ethics board, according to project coordinator Stephen Bishop.

⁵ http://cordis.europa.eu/fp7/ict/programme/fet/flagship/home_en.html

cost. According to the participants, nanoelectronics should contribute to societal challenges in these fields: healthcare and wellness (address the needs of an ageing society), transport and mobility, energy and environment, communication and infotainment, and security and safety. The report included the following application scenarios focusing on some key opportunities and dilemmas: Guardian Angel for aged people (J.P. Colinge), autonomous robots (Rainer Waser), ubiquitous powering (Adrian Ionescu), all-in-one devices (Reinhard Mahnkopf) and autonomous city mobility environment (Livio Baldi). (EC, 2009)

In a comprehensive analysis of results of the first ten years of the US National Nanotechnology Initiative and foresight of the next ten years, progress in (especially energy efficient) nanoelectronics was expected to contribute to High Performance Computing (HPC). HPC had already been driving scientific and technological progress in the last decade in a wide range of fields including energy, materials science, engineering, life sciences, climate and environment and defence and security. Indirectly, it had thus been driving many societal impacts of new technologies. Sensitive future applications and impacts mentioned include sensors implanted in the human body for health monitoring, mobile electronic devices and ubiquitous access to information, new social definitions of “private” and “public”, and new cultural norms of acceptable interactions. A possible high impact application could be real-time natural language translation enabling international cooperation and networking. Challenges were foreseen for business models of corporations and national economies. (Roco, 2010, p 300-301)

More recently, the EU funded FESTOS project discussed security implications of new technologies including a scenario “At the flea market” where intelligent nanotechnology-based products can be set to self-destruct with a wireless signal, leading to an economic collapse and scarcity of old products. (FESTOS, 2011)

To conclude, current trends in nanoelectronics are expected to give rise to major impacts on society, including potential benefits as well as disruptions. Most relevant foresight exercises in the last decade have called for targeting research towards societal benefits and raising public awareness of potential benefits. Raising awareness of potential risks and disadvantages is mostly not an issue in these reports. In general, critical research on Ethical, Legal and Societal Aspects (ELSA) of nanoelectronics and ICT is not called for by research policy makers and academic and industrial experts engaged in such foresight studies. This is a remarkable difference compared to research in nanomedicine and nanobiotechnology, the topic of last year’s ObservatoryNano Annual Report on Ethical and Societal Aspects of Nanotechnology. (Malsch & Hvidtfelt-Nielsen, 2010) In the following section 2.2, it will become clear whether such a different relation between ethics and research represents a broader consensus among stakeholders.

2.2 Which relevant issues are currently being debated by policy makers and stakeholders? Which issues apparent from the technical and economic trends are not discussed sufficiently?

Recent debates among policy makers, politicians and stakeholders on ethical and societal aspects of nanoelectronics and ICT have focused on some key issues. These issues are not exclusive for nanoelectronics but more related to general trends in ICT where nanotechnology may play a role including miniaturisation and convergence. These include research ethics (in particular related to converging technologies), ubiquitous computing/ambient intelligence (in particular RFID and internet of things), privacy and data protection, and precaution.

Research ethics

Even if ICT in general and nanoelectronics in particular is a technology push area, this does not mean that researchers are free to do what they like, at least not in Europe. The European Commission's "**Ethical Guidelines** for undertaking ICT Research in FP7" oblige proposers to comply with fundamental ethical principles and to actively identify potential ethical issues related to their research. ICT research should take a responsible approach, respect privacy and informed consent and comply with ethical regulations for animal testing. The guidelines explicitly mention some sensitive areas including ICT implants and wearable computing, eHealth and genetics, and ICT and bio/nanoelectronics. The latter has a strong potential for misuse. Researchers engaged in bio/nanoelectronics should respect guidance for ICT implants and wearable computing which generally prescribes development of the least invasive alternative. These researchers should also take into account implications for privacy and data protection and ethical guidance for other relevant disciplines such as biology. (Cordis, 2010)

There is some debate about the effectiveness of the current guidelines for excluding controversial research proposals. They only take into account research ethics issues such as informed consent of the persons involved in the research and animal testing, not expected ethical and societal issues which may result in the future from the technologies and systems developed in the project.⁶ Furthermore, the current checklist for ethics in research leads to ethical compliance rather than ethical reflectivity. It is deemed necessary albeit insufficient to include an ethics work package in ICT research. Emerging ICT will throw up complex ethical issues which will have to be addressed. (Rogerson, 2011) It is necessary to create more time for ethical reflection already during technology development and pilot phases. (Hustinx, 2011) Alma Whitten (Google) pleads for research *and development* ethics. For Google, there is no distinction between the research phase and the development phase.⁷ The European Science Foundation has published a European code of conduct for research integrity in all areas not just ICT. (ESF, 2010)

Similarly, a group of experts of the Rathenau Institute remarked that "There already is a strong awareness within the European Commission that developments in biotechnology and nanotechnology can lead to controversial political and regulatory issues. The European Commission seems to pay less attention to the governance of information technologies and their convergence with cognitive sciences. The fact that science and society issues are treated differently for different fields seems to relate to the fact that the research in these fields is commissioned by different DGs. For example, DG Research has a special directorate Science in Society... which explicitly focuses on the governance of emerging technologies. DG Information Society and Media, which very actively stimulates the convergence of neuroscience and information technology, needs to pay more attention to the ethical, legal and social aspects of information technology. For this, it is crucial to acknowledge that the benefits to society of information technology can not automatically be taken for granted. Such awareness is already growing within the IT industry. ..." (van Est et al, 2010 p 187) According to Bart Walhout⁸, also from the Rathenau Institute, the difference between institutionalisation of ethical reflection in the IT domain compared to the life sciences could also be explained by the more private character of practises: whereas ethical issues in life sciences often relate to confined situations (research lab, medical), electronics cross-cut many more areas with a less public character. As the relation between NT developments and issues at stake also is often indirect this hampers straightforward ethical analysis. He considers the influence of NT enabled ICT

⁶ Emilio Mordini, intervention during RISE/HIDE conference, 9-10 December 2010

⁷ intervention at ETICA-EGAIS-STOA workshop on IT for a Better Future, European Parliament, 31 March 2011, <http://www.etica-project.eu/>

⁸ personal communication, March 2011

to have much impact on individual identity and autonomy (as suggested by ambient intelligence concepts etc).

In addition, some neuroscientists are also beginning to show concerns for the societal implications of their research. In 2010, an initiative was taken for a voluntary code of conduct for neuroscientists. (Bell, 2010) This initiative is not gratuitous but appears to be a response to a fundamental new dynamics in the neurosciences. According to van Est et al (2010), in particular in regard to engineering the brain, there is a new approach of neural engineering in addition to traditional observation and theory building. Neural engineering implies that scientists construct a computer model of the brain or introduce implants into the brain without a pre-existing theory and learn from the unforeseen effects and unpredicted behaviour. This combination of experimental, converging behavioural engineering gives rise to new ethical, legal and social issues making traditional bioethics issues more profound such as mental integrity, informed consent, liability, regulating safety, privacy, bodily integrity and remote control issues. The EU is currently not funding any large ELSA projects in the neurosciences or neural engineering. (van Est et al, 2010, p 119)

In the light of this discussion, President Barroso of the European Commission has requested an opinion from the European Group on Ethics in Science and Technology (EGE) on the Ethical Implications of Information Communication Technology (ICT).⁹

Ubiquitous computing/ambient intelligence

Recent stakeholders debates related to ubiquitous computing or ambient intelligence have been sparked by the use of RFID chips as tags in increasing numbers of products including consumer goods as well as passports, public transport cards and implants in the human body. This debate has broadened to a discussion on the “internet of things” and linked up to prior debates on more general aspects of ambient intelligence.

By 2007, RFID was already used for identity management in everyday life, without many issues. In subsequent years, several challenges were foreseen in a project by the Dutch Rathenau Institute:

- “RFID users need to know what maintainers can and are allowed to do with RFID data
- RFID users should play a role in developing new RFID environments
- If personal data from different RFID settings are merged it should remain clear who is responsible for handling these data
- The privacy guidelines and the concepts of personal data and informational self-determination need to be reconsidered in the light of an increasingly interactive environment
- Governments should take a clear stance on whether RFID bulk data will be mined for investigative purposes.” (Hof, 2007)

In a later Dutch public debate on the vaccination campaign for H1N1 influenza in 2009, some expressed the fear that the government might use this campaign to implant nanochips into the bodies of citizens. Experts responded that they considered this highly unlikely, but found it difficult to address such concerns adequately.¹⁰

⁹ On 22 march 2011: http://ec.europa.eu/european_group_ethics/index_en.htm

¹⁰ On the Internet this discussion can be found on several sites. It also surfaced in other countries in that period, e.g. <http://ppjg.wordpress.com/2009/10/04/nano-chips-in-needles-chipping-humans-with-vaccine-needles/> Dutch newspapers also reported on this discussion, e.g. Trouw: <http://www.trouw.nl/tr/nl/4324/Nieuws/article/detail/1177074/2009/12/28/rsquo-RIVM-stand-er-te-vaak-alleen-voor-rsquo.dhtml> and HP/De Tijd, <http://test.hpdetijd.nl/2009-11-09/zeven-vragen-over-de-mexicaanse-griep>

In France, CNIL (National Commission on Informatics and Liberties) included RFID chips as one of the new technologies of concern. CNIL discussed how RFID could threaten privacy and data protection and how the citizens' liberties should be protected by adapting legislation. CNIL keeps monitoring technology development in this field. Other related concerns include biometrics and video surveillance. (CNIL website)

CNIL also participated in the French national dialogue on nanotechnology. The main concern CNIL brought into that debate was how to avoid 'hyper-traceability' of persons and goods through RFID-chips that could compromise the freedom of movement and the right to anonymity. Nanotechnology was expected to cause a revolution comparable to or bigger than the Internet. Invisible communicating RFID chips and difficult to detect nanochips may already be implanted in the human body. A major challenge for CNIL was how to control what is invisible. CNIL considered it its duty to ensure proportionality of applications of personal data processing by nano-objects and to exercise its authority as it is already doing for biometrics. For this, CNIL may need more resources. The president of CNIL was also concerned about human enhancement which is not just a matter of degree, but of nature. It may be necessary to ban certain applications such as communicating implants. (CDPD, 2010)

Recent political debate on RFIDs has resulted in broader concerns about the emerging "Internet of Things". The European Commission (EC, 2009a) published an action plan on it including not only general privacy and data protection rights but also the right to "silence of the chips". A dilemma is that incorporating a switch to turn the chip off might be expensive compared to the chip's other components such as sensors. Will the customer be willing to pay for privacy? And regulations are not enough to stop individual entrepreneurs developing new applications or hacking into existing systems.¹¹

Likewise, the German Parliamentary Technology Assessment Bureau of the Bundestag expected that ubiquitous computing (ambient intelligence according to the EU) may enable a lot of new services, but could also have implications for privacy and informational self-determination. TAB recommended:

- "adapting the data protection law to the opportunities offered by ubiquitous computing to monitor and obtain personal data even from otherwise uncritical data sources
- creation of a data protection law for employees
- societal discourse about the origin and use of data tracking in ubiquitous computing ...
- systematic monitoring of new technologies and evaluation of their impact on informational self-determination."

The societal compatibility of ubiquitous computing must also be investigated and discussed. This could be done by early consideration of user interest in the development process and creation of real choices by labelling and an opt-in model. (Friedewald et al, 2010)

Aarts & Grotenhuis (2010) have analysed 50 ambient intelligence projects carried out in Philips' ExperienceLab. Even though some were successful, many of these projects failed because they didn't fulfil their promise of user-centric design. To improve the chances of Ambient Intelligence to contribute to sustainable development, an "experience research" approach has been developed. This is tested in so-called living labs where public-private-civic partnerships contribute to the technology development. Applications of ambient intelligence should be assessed with a two-dimensional framework for stimulating "synergistic prosperity": body versus mind and society versus earth. Good products should contribute positively to all four aspects.

¹¹ Florent Frederix, Alan Freeland, interventions at ETICA-EGAIS-STOA workshop on IT for a Better Future, European Parliament, 31 March 2011, <http://www.etica-project.eu/>

Privacy and data protection

On a more abstract political and legal level, the 1995 European data protection directive is currently being revised under the influence of new and emerging technologies as well as geopolitical pressures promoting national security at the expense of citizen's freedom. (c.f. HIDE and RISE projects discussed in section 2.3) The policy and stakeholder debate in Europe focuses on the revision of the data protection directive and in particular on protecting civil rights of European citizens in international agreements on exchange of data including on airline passengers and financial transactions. Relations between the EU and USA and between the EU and emerging economies are of particular concern. Trends in nanotechnology are of minor importance in this more general political and legal debate. Other emerging technologies such as biometrics and RFID do play a role.

In this discussion, the European Organisation for Security EOS is lobbying on behalf of the European security industry. They ask for sufficiently precise and non-ambiguous privacy and data protection requirements and aim to contribute technological solutions to privacy and security enhanced design of security technologies. (EOS, 2010)

In the Netherlands, the new government intended to improve information security and protection of personal data in several ways:

- A time horizon and effectiveness test in proposed measures to store, link and process personal data
- Obligation to report data leaks of different kinds
- Monitoring introduction of large scale informatisation and automatisisation projects
- Integral approach to cybercrime (Opstelten, 2010)

Diana Whitehouse, chair of the International Federation for Information Processing (IFIP) pleads for taking into account the privacy of future generations and gender aspects. Public awareness should be raised about privacy aspects of converging technologies affecting the body, brain and being such as robotics, RFID and medical implants. (Whitehouse, 2011)

Precaution

The political controversy about the interpretation of the precautionary principle, in particular for engineered nanoparticles, has also spilled over into the nanoelectronics domain. In 2010, the European Parliament Environment Committee called for a ban on nanosilver and long multiwalled carbon nanotubes in electrical and electronic equipment. Other electrical and electronic material containing nanomaterials should be labelled, and the manufacturers should be obliged to provide safety data to the European Commission. They amended the EU Restriction of Hazardous Substances (RoHS) Directive accordingly in their vote on 2 June 2010. Eventually, political agreement was reached and the EP voted in favour of the final act on 24 November 2010. Reference to nanomaterials was included in rather general terms: "Review and amendment of the list of restricted substances in Annex II: as soon as scientific evidence is available, and taking into account the precautionary principle, the restriction of other hazardous substances, including any substances of very small size or internal or surface structure (nanomaterials) which may be hazardous due to properties relating to their size or structure, and their substitution by more environmentally friendly alternatives which ensure at least the same level of protection of consumers should be examined."¹²

To conclude, in recent European policy and stakeholder debates on ICT research ethics, a call has been made for ELSA research related to converging ICT and neuroscience on the nanometre scale. The discussion on ubiquitous computing/ambient intelligence has re-emerged, primarily triggered by

¹² <http://www.europarl.europa.eu/oeil/FindByProcnum.do?lang=2&procnum=COD/2008/0240>

applications of RFID. More recently this has broadened to include implanted communicating (nano)chips and the internet of things. Nanoelectronics are relevant primarily by contributing to miniaturizing sensors and RFID chips, making them even less visible. The political agenda is dominated by more general discussions on political and legal aspects of privacy and data protection, and precaution, where trends in nanoelectronics play an indirect and currently insignificant role. In section 2.3, contributions to the debates related to nanoelectronics in ethics and social science literature are explored. These contributions may help improve the understanding of the issues at stake.

2.3 What are the issues discussed by ethicists and social scientists writing about nanotechnology? Which new insights do they have to offer for the policy and stakeholder debate?

There is still a lack of literature on the ethics of specific nano-related research in information and communication technology. However, reflections from computer ethics and information ethics are relevant to take into consideration since they are concerned with at least some of the same issues. A relation to nanotechnology is further miniaturisation in combination with smaller batteries. Small but versatile sensors that will enhance the existing problems and even enable new devices are also an expected contribution of nanotechnology in ICT. Other relevant philosophical debates where nanoelectronics is an emerging concern include implications of ICT for politics and the organisation of society, value sensitive design of ICT and again ambient intelligence.

Computer ethics

Developments in nano are part of a history of information science. A specialist who has been in the field of *computer ethics* as a philosophical field for many years is Herman Tavani. Tavani (2001) summarizes the development from around 1985 when computer ethics was defined at a time when computers were mainframes, machines that ‘chunched numbers’ up until now where computers are personal computers and many other things and are thought of as a communication *medium* or a *tool* essential for our lives. This new conception of computers penetrates deeply into our lives and is therefore highly relevant for an ethical analysis. However, it is often thought not to be as important as something like biotechnology where the ethical dilemmas are more obvious to everyone. Information technology is less controversial, but not less important for human life.

It has been discussed – analogously to the current discussion about nanotechnology - whether or not computer ethics could be seen as a part of general ethics or as raising new and unique questions. The veteran of raising awareness to ethics and computers is James Moor. In 1985 Moor wrote a classic article *What is Computer Ethics* in the journal *Metaphilosophy*. He later defined computer ethics as ‘the specialized field of identifying policy vacuums created by computers, clarifying conceptual confusions surrounding those issues, and then formulations and justifying new policies for those areas in which either there are no existing policies or where existing policies cannot be adequately extended’. (Tavani 2001)

Ethics of IT

Key issues in what is also called ‘the ethics of IT’ in a western tradition have centred on ethical principles such as *personal autonomy, privacy and property rights*. But attention is also called to the *global* challenge the complex interplay between information technology ethics and culture confronts us with by presenting other values and conceptions of what *the good life* is. Essentially this is what ethics is, to define what is good and right. Issues to be considered when many cultures are voiced are

the *digital divide*, *data privacy*, *intellectual property rights*, *democracy and autonomy in the information age*, *the globalist and consumerist attitudes*, and *the ecological impact of IT culture*. It is vital to be informed by different cultural inputs since silencing the voices of other cultures by not even letting them be heard conflicts with democratic western ideas of autonomy and competition. (Vallor 2008)

If such a concept as the *digital divide* is to be taken seriously its meaning must be spelled out, and concerns about those who are on each side of the gap must be considered. A divide split people in groups and is only problematic when the division becomes unfair (e.g. between rich and poor) or random. However, if resources that should be equally divided between all people end up in the hands of only one group, it is an unfair divide. The resources could be economic, mental, and physical and issues could be related to culture of IT and related to age. When measures are taken to ensure a fair divide or compensation to those who receive less, these are called issues of e-inclusion. (Mordini 2009)

Besides another question is raised: Have information and information technology become so important in our technology-dependent age that they have become constitutive of persons? That would imply that information is no longer limited to the moral status of an instrument, but has achieved a more substantial moral status. If so a moral claim can be made to the protection of personal data for its own sake. (Vallor 2008)

Capurro (2011) pleads for an ethical impact assessment and ethics observatory. ICT ethics should get the same weight as bioethics. An additional issue typical for ICT ethics is that people increasingly perceive the world through digital glasses. Gouijon notes that the current medical ethics practice does not fit ICT design but is still applied to it. If users are involved in ICT design, the researchers will have to comply with cumbersome ethics regulations. This is a disincentive against user centric design.¹³

Very few ethicists and social scientists explicitly address ethical issues related to nanoelectronics. However, in some (EU-funded) projects on ICT, privacy and security, possible new issues caused by nanoelectronics are discussed. Because nanoelectronics include miniaturisation of microelectronics and are expected to be applied in the same systems, current issues in the debate on microelectronics also apply to nanoelectronics.

Politics and organisation of society

Silvia Venier (2010) distinguished five major issues in the current policy and stakeholder debate on ICT, privacy and security. (1) The traditional trade-off model between privacy and security is under discussion. Privacy and respect for human physical and psychological dignity should be essential part of any security policy. (2) The cultural challenge posed by ICT is to reconstruct the boundary between the private and public spheres, because both have important different functions. (3) Technologies that impact the human body may conflict with fundamental rights. E.g. nanotechnologies that can improve cognitive abilities and analyse brain activity patterns. (4) New embedded technologies, ubiquitous surveillance or cloud computing have an impact on what is a cornerstone of the EU Data Protection Directive: the user's informed consent over the use of his personal data, another human right. Such technologies could affect the autonomy and freedom of choice of individuals. Furthermore there are issues of data protection in globalisation and the transfer of personal data. (5) The last issue is the digital divide. She stressed that "the Charter of Fundamental Rights is the general framework of Rights that should be taken into account while dealing with the development

¹³ interventions at ETICA-EGAIS-STOA workshop on IT for a Better Future, European Parliament, 31 March 2011, <http://www.etica-project.eu/>

and introduction of new technologies. Articles 1 on Human Dignity, 3 on Integrity of the Person, 6 on Liberty and Security, 7 on Private and Family Life and 8 on Personal Data Protection should be taken into account.” (Venier 2010)

EU Data Protection Supervisor Peter Hustinx (2011) reflected on challenges for the law of the future posed by emerging ICT. ICT makes things more efficient, but also more complex. How to allocate or organise responsibility? Globalisation is also a relevant trend. Responsibility will move from traditional liability to holding the producer of a technology responsible for ensuring privacy by design from the beginning.

Value sensitive design

Privacy Enhancing Technologies (van den Hoven, HIDE & RISE projects). Privacy by Design, Trust by Design, Security by Design and Value Sensitive Design are concepts discussed both by ethicists and by engineers and scientists. Whereas ethicists and social scientists tend to be sceptical about the feasibility or desirability of such value sensitive design, engineers appear to embrace it and develop ways to put it into practice.¹⁴

Some of the values that could be incorporated in ICT design include proportionality, trustworthiness, fool-proof, human-centred design. Proportionality is a requirement for assessing the acceptability of security technologies with privacy implications. Unfortunately, different EU countries differ in their evaluation of proportionality of individual security technologies.¹⁵

Another issue currently examined in EU projects in ICT and ethics is trust of consumers and citizens in ICT security applications, and how to enhance trustworthiness. Are security applications of ICT fool-proof? Will particular applications (biometrics) allow for mistakes? This could be the distinguishing feature between biometrics and other technologies: that biometrics does not allow for mistakes. Once someone’s biometric identity has been stolen, (e.g. fingerprint), this can’t be changed, and the individual will always be confronted with bureaucratic problems.¹⁶

Ambient Intelligence presents several challenges to EU policy-making: (ambient intelligence) technologies should be designed for people and not the other way around. Security, privacy and trust are determining factors for the success of ambient intelligence. Trust and security should be designed into the technologies from the start, which is probably not going to succeed completely. Privacy advocacy groups have already called for a moratorium on use of RFIDs. Major retailers are introducing them without prior standardisation. (Wright et al. 2010)

Caroline Gans-Combe observes co-evolution of IT and ethics. IT decision support tools can be used to identify ethical issues and weigh them.¹⁷

Ambient Intelligence

The new technological embedding of computing into people’s surroundings and the ubiquitous availability of digital information to the users of such environments are becoming part of everyday life. It is called ambient intelligence or ubiquitous computing. It is of high usefulness – and thus it is already part of the ethics discourse since it is of *use and benefit* for humans. Ambient intelligence is often compared with ‘assistive technologies’ but they pose different including legal concerns. (Kosta et al. 2010) Ambient intelligence might be a form of research and technology that changes how we

¹⁴ cf RISE/HIDE workshop 9-10 December 2010

¹⁵ Discussion at RISE/HIDE workshop 9-10 December 2010

¹⁶ von Schomberg, intervention during RISE/HIDE conference, 9-10 December 2010

¹⁷ intervention at ETICA-EGAIS-STOA workshop on IT for a Better Future, European Parliament, 31 March 2011, <http://www.etica-project.eu/>

perceive ourselves and the world around us. It *changes our interaction* with our surroundings when these surrounding become 'intelligent'. When the world around us changes it becomes necessary to consider whether it also calls for a *changed ethical attitude*.

Ambient technologies are user-centrally developed and the assessment calls for more perspectives: the perspective of the user and the perspective of the surroundings which are influenced. A collection of data is produced and these data can be invisible and uncontrollable. They can also be collected without the person even noticing it. The question is raised whether the technologies developed can still be considered 'safe' and respecting human values such as privacy, self control, 'design-for-all' and trust. Many of the nano-based applications are still only planned or being developed. Therefore, reflections about the nature of the ethics are developing along with the technology itself. Reflections on such nanotechnologies originate from scenarios with MINAmI- based applications (Micro-Nano integrated platform for transverse Ambient Intelligence applications) in healthcare, assistive technology, homecare, and everyday life. (Kosta et al 2010)

Emerging ICT can have social impacts, in particular when it has the following characteristics: it allows natural interaction with the user; it is invisible; the technology is in direct contact with humans, the system acquires detailed understanding of the user (much more than today); it is pervasive, autonomous and has power over the user. (Stahl, 2011)

To conclude, contributions to the debates related to nanoelectronics in ethics and social science literature were explored. In general, some insights from computer and IT ethics are also valid to nanoelectronics. Relevant concepts include informatisation and miniaturisation. On a more abstract level, political issues and the debate about the organisation of society in a world that changes rapidly due to several influences including trends in information technology are also relevant. More down to earth discussions on value sensitive design and ambient intelligence are discussed for ICT in general, and also directly relevant to nanoelectronics and its applications.

2.4 What are new issues for the debate and who could do what?

Both new benefits and new ethical dilemmas and societal disruptions are expected from trends in nanoelectronics and nanotechnology for ICT. New issues for the debate are related to research ethics, value sensitive design, ubiquitous computing and related nanotechnologies, and legislation, human rights and the organisation of society as a whole. It depends on the type of issue which actors could contribute to debates or to governing the issue. In this technology focused report, priority is given to narrow research and technology policy. Broader societal concerns are given less attention.

Research ethics

Experts and policy makers have called for accompanying ICT research with research in ethical, legal and social aspects and for targeting research to societal needs. The second recommendation appears to have been implemented more than the first. Several roadmaps and strategy documents indeed target the research to a select list of societal needs defined by the technology promoters. However, the European Technology Platform in Nanoelectronics (ENIAC) does not have an ethics board, unlike the ETP Nanomedicine. This illustrates a general trend that the distance between technological developments and research and debate on ethical and societal issues is considerably larger in ICT than in the life sciences. Whereas for both fields there are separate projects investigating the ethical and societal issues, for nanomedicine and other life sciences it is much more common that technological projects include an ethics or social science part. In addition, the standard ethical guidelines for (EU funded) research are more applicable to biomedical research than to ICT.

The European Commission could adapt the guidelines for ICT research ethics and call for integration of ELSA in EU funded ICT research. Researchers and companies could include ELSA boards in their networks and technology platforms.

Value sensitive design

Among engineers and companies engaged in nanoelectronics and ICT, value sensitive design is becoming increasingly popular. However, ethicists have pinpointed dilemmas including which values would be acceptable in design and who should decide on this. There is a lack of interaction between engineers and ethicists and a lack of public debate.

The European Commission could organise workshops bringing together engineers and ethicists to discuss value sensitive design and initiate public dialogue projects.

Ubiquitous computing and related nanotechnologies

Regulatory and privacy issues related to RFID and the internet of things have entered the political agenda in Europe, but there may be a need for broadening this to encompass more general societal trends influenced by ubiquitous computing.

Parliamentary technology assessment organisations could organise public discussions on ubiquitous computing.

Legislation, human rights and the organisation of society as a whole

The current debates on how ICT relates to privacy and fundamental human rights and how legislation should be adapted to accommodate technological developments are ongoing. Nanotechnology does not play a significant role in those debates yet. It is difficult to imagine ways to include nanotechnology in these debates because the relation between relevant developments in nanotechnology and the societal issues is indirect, via applications in systems that only show themselves to users in the form of concrete products and services. The nano-contents will not be obvious to the user in any case, and most of the foreseen applications of nanoelectronics are not available yet.

3 Ethical and societal aspects of nano-enabled civil security

In general, ethical and societal aspects of civil security research are high on the political and policy agenda in Europe and the focus of several EU funded projects (ESRIF vision 2009). A key issue is what would constitute the right balance between the fundamental rights to security and freedom in specific cases (e.g. biometrics for border control). Other controversial domains where nanotechnology could be applied are forensics and sensing. A specific new trend in nanotechnology which could give rise to new ethical and societal issues is quantum cryptography and encoding materials (on-wire lithography, Roco 2010).

3.1 Which ethical and societal issues are raised by current technical and economic trends in nanotechnology for civil security applications?

By 2007, potential impacts of nanotechnology based security technologies were still unclear. Proponents of security research expected security improvements for the European citizen, but they did not give evidence to corroborate this expectation. The eroding boundary between civil and military research could lead to unexpected security risks. Academic freedom and free trade could be restricted progressively. Some security technologies may not respect privacy and personal data protection legislation. (Nanoforum, 2007)

Nanotechnology was expected to enable next-generation biometrics, being miniaturised, integrated, multifunctional and efficient. Biometrics was defined: “automated measurement of physical or behavioural characteristics to identify a person”. (Ericson, 2007)

Nanotechnology could be applied in security applications in four sectors:

- Detection,
- Protection,
- Incident support, and
- Anti-counterfeiting, authentication and positioning.

Incident support is hardly controversial, but other security applications of nanotechnology may give rise to ethical issues. Different types of nano-based detectors are pursued in research, which can detect chemical, biological, nuclear, radiological and explosive substances (CBRNE) or narcotics. There does not seem to be a distinction between nano-enabled detectors and other detectors. Nanotechnology may also enable neutralisation of CBRNE effects, and be used in decontamination. Other applications are in forensics, personnel detection, equipment and infrastructure protection and condition monitoring. (ObservatoryNano, 2009)

In particular, nanosensors offer potential for explosives detection in the future. Current Technology Readiness Levels range from basic research to the prototype stage. Foreseen applications are in combating crime and terrorism as well as in monitoring industrial production of/with explosives. The technology development is in line with EU security and justice policies. (ObservatoryNano, 2011)

Point One (2008) report a market in the Netherlands for the companies engaged in the Point One PHASE2 resesarch programme of €17.3 billion for transport, logistics and security applications of nanoelectronics, embedded systems and mechatronics in 2005, and expect a growth opportunity of €2.8 billion, mainly in e-government and automotive. According to the report, “the area of transport,

logistics and security systems is characterized by the need for solutions that enable the control of the public environment (around users) at large.” By 2012, Point One expects a market of €200 million for secure public infrastructure by ambient intelligence and nanosensor technologies. By 2016, it expects a market of €100 million for robots with autonomous vision and control in military and civil security missions.

3.2 Which relevant issues are currently being debated by policy makers and stakeholders? Which issues apparent from the technical and economic trends are not discussed sufficiently?

The main emphasis in current policy and stakeholder debates on security is on political and societal aspects of security policies in general. Emerging security technologies have given rise to particular issues. Nanotechnology does not play a dominant role in the current debates. The current debates include political and research ethics issues.

Political and societal issues and dialogue

The Charter of Fundamental Rights of the European Union, several European directives, guidelines and international declarations cover legal and ethical aspects of nanotechnology based security technologies. The main issue that has been in debate for several years is a proper balance between the rights to liberty and to security. Legislation and ethical guidelines for the protection of private and family life, home and communications; personal data protection; and equality and non-discrimination must be taken into account. For some applications, the right to physical and mental integrity; and prohibition of degrading or inhuman treatment are valid. All products must respect legislation aimed at protecting and enhancing environmental quality and consumer protection. Research must balance academic freedom with responsible science and technology development. This includes a new balance between openness and handling classified information for security technologies. (Nanoforum, 2007)

Many Europeans have in the last decade been more concerned with security than with privacy and freedom, according to a number of Eurobarometer surveys. However, public awareness of security measures, security technologies and nanotechnology was low. This means that no conclusions can be drawn from these opinion polls about the acceptance of the particular technologies that are currently used or still under development.

Some NGO's expressed concerns about privacy and human rights aspects of the information society, or advocated (military) arms control and disarmament. By 2007, no NGO appeared to have taken a position explicitly mentioning nanotechnology based security technologies. (Nanoforum, 2007) By 2011, NGO's concerns have focused on body scanners and biometrics in border control, surveillance, “Big Brother” legislation and international exchange of data for fighting crime and terrorism. (e.g. EDRI website) Nanotechnology is still not discussed.

Research ethics

ESRAB (2006) recommended research into ‘ethical aspects of security technologies’ and a ‘review of existing codes of conduct, best practices, etc. as to the ethical use of security technologies and to develop new ones where shortfalls exist’. These are relevant to security applications of nanotechnology. Research in social sciences and humanities must also contribute to the development of new Privacy Enhancing Technologies, and to criteria for assessing if new technologies respect citizens’ rights and current legislation. Such research must also enable early

identification of a need for new or adapted legislation. Public debate must be organized to articulate public acceptance of security measures, technologies and nanotechnologies. Political decision-making must focus on developing new European regulations for handling classified information in EU funded projects, and for regulating and standardising Privacy Enhancing Technologies. There is a need for a more fundamental debate about the right balance between civil and security research and technologies, in order to avoid unnecessary constraints on academic and trade freedom. (Nanoforum, 2007)

The discussions of biometrics in the HIDE project and in the Nanoforum report on nanosecurity (Nanoforum, 2007) have identified ELSA issues. In particular, terahertz detectors lead to severe privacy and human rights issues if used to see through clothes of people. It is not so clear what is the main market for security technologies. Governments may be dominating the research, but small shop-owners wanting to prevent theft might well represent a larger market for the end products.

In 2010, a public debate has started about ethical issues and implications for civil liberties of the EU funded INDECT project, which aims to combine surveillance data from CCTV, internet, and other telecommunication databases and newly developed drones for police crowd control, to automatically detect individuals with suspicious behaviour and compare them with police records. This system is intended not only to solve but also to prevent crime and terrorism. Participants in the discussion are politicians and media in Austria¹⁸, Germany,¹⁹ the Netherlands²⁰, the UK and the European Parliament²¹. A key issue is that even though the project may have been reviewed by an ethics review board before being approved, the current ethical review guidelines only take into account research ethics issues such as informed consent of the persons involved in the research and animal testing. Expected ethical and societal issues which may result in the future from the technologies and systems developed in the project are not taken into account.²²

In the light of this discussion, President Barroso of the European Commission has requested an opinion from the European Group on Ethics in Science and Technology (EGE) on the Ethical Implications of Security Technologies.²³ The European Commission is developing a code of conduct for security technologies.²⁴

To conclude, the political and research ethics debates on security technologies do not focus on nanotechnology. Some of the current concerns address the same research ethics issues as identified in chapter 2 on ICT. There is considerable public debate on border control and surveillance technologies and other security technologies such as body scanners, biometrics and sensors where nanotechnology may be applied. However, nanotechnology is not the key issue in those debates.

¹⁸ <http://derstandard.at/> (key word search: INDECT)

¹⁹ <http://www.piratenpartei.de/>

²⁰ <http://www.solv.nl/weblog/openheid-rond-surveillance-project-indect-gaat-moeizaam/17308>,
<http://weblogs.nrc.nl/media/2009/10/13/indect-bespioneert-europese-burgers/>

²¹ In the period November 2009-November 2010, 13 questions have been asked about the INDECT project by MEPs, <http://www.europarl.europa.eu/sidesSearch/sipadeMapUrl.do?PROG=QP&language=EN&startValue=0>

²² Emilio Mordini, intervention during RISE/HIDE conference, 9-10 December 2010

²³ On 22 march 2011: http://ec.europa.eu/european_group_ethics/index_en.htm

²⁴ René von Schomberg, intervention at ETICA-EGAIS-STOA workshop on IT for a Better Future, European Parliament, 31 March 2011, <http://www.etica-project.eu/>

3.3 What are the issues discussed by ethicists and social scientists writing about nanotechnology? Which new insights do they have to offer for the policy and stakeholder debate?

The concept of security has changed since the age of the Cold War when the threat was mainly related to conflicts between states. In scholarly studies of security the discussion of the New Security focuses on nongovernmental actors such as civil war, transnational crime, infectious diseases, and the proliferation of small arms. Security providers are nongovernmental organizations, private security companies and international regimes. A security threat is defined as an event with potentially negative consequences for the survival or welfare of a state, a society or an individual. (Krahmann 2005)

This influences the way any technology, including nanotechnology, can become part of the quest for security today where security is an article of trade. (Krahmann 2010) However, this section will focus on technologies in connection with surveillance which is only one element of the security discussion. In regard to security practices of surveillance, the State is reshaping its structure through internal reorganization, outsourcing and supra-state security alliances. The practice of surveillance which is a product of having security as the dominant ordering principle, threatens the relationship between the citizen and the state, the private and the public. It raises ethical concerns because new practices always require new reflections. (Bajc 2007) The concept of security is broadened and becomes 'securization', a concept that goes beyond the original meaning of security as national security. Securitization includes also social, environmental and political issues. (Bajc 2010)

The discussion concerning surveillance has had two dominant metaphors: The metaphor of the 'Panopticon' and the metaphor of 'Big Brother'. However, nanotechnology makes the scenarios look somewhat different than what the last decades have foreseen. (Van Den Hoven & Vermaas 2007)

The first metaphor, 'The Panopticon' is the plan for prison architecture devised by Jeremy Bentham at the end of the eighteenth century and given a new lease of life by Michel Foucault in the late seventies with his ideas of discipline (Foucault 1975). The disciplinary power of surveillance is actualised by architecture with a watch tower permitting a hidden inspector to gaze into all cells in a semi-circular prison building. Foucault does not mention databases but the surveillance tower could be a database that stored data concerning what was observed. By not knowing when they are watched prisoners learn to discipline themselves in order not to be seen engaging in forbidden activities and being physically punished. Foucault calls the normalisation of persons in prison *Biopower*: They are induced to adapt their behaviour to the norm. "The system watches you; it fits you into a pattern; the pattern is then fed back into you in the form of options set by the pattern; the options reinforce the pattern; the cycle begins again". The point is surveillance gives power to influence beyond the setting of the prison. As such, searchable databases make possible this kind of normalizing biopower, 'making people up' rather than 'invading their private lives'. Yet the latter is how surveillance is all too often seen. (Lyon 2001)

The second metaphor, George Orwell's 'Big Brother' is critical towards a centralised world dominated by rational bureaucratic control and the possibility of human dignity in such a world. However, today surveillance is conducted by many 'little brothers' instead. (Lyon 2001) Power and surveillance is decentralised and the authoritative imposing of identities to vulnerable people is also decentralised and in many hands. The idea of a 'nano-panopticon' that has been discussed should encompass spatial and temporal aspects of the panopticon. Also, with nanotechnology the focus is not only on the data produced but on the technology itself. The privacy debate has moved from atoms (bricks, walls, curtains) to bits and bytes (information technology), only to veer back to atoms

(nanotechnology). What is now relevant is surfaces, new artefacts, properties of artefacts and materials. (Van Den Hoven et al, 2007)

Citizens of today's technologically advanced society find their everyday lives under scrutiny by many agencies. People are to some extent aware that data relating to their daily activities is collected, stored, checked, exchanged and used. Surveillance today is a central means of social sorting, of classifying and categorizing populations and persons. As suggestion for testing of regulation practices in *privacy issues*, Lyon suggests *three tests*: Participation, personhood and purposes. Every surveillance practice should firstly be confronted with a *participation* test: namely whether it furthered social inclusion and involvement. Secondly, it should be confronted with a *personhood test*, namely the person having a 'good name' that should not be ruined by the surveillance and data handling. Thirdly, it should be confronted with a test of *purposes*, and namely a test of what the personal data are being collected *for*? Is the practice fair in itself? Surveillance systems should be made accountable, and that accountability should start with the reminder that personal data, however abstract, has effects that are felt by persons. Therefore care should be highlighted to countervail against mere control. (Lyon 2001)

Privacy and claiming privacy is not demanding to be 'left alone' or be 'private', but it is to try concretely to prevent others from harming, treating unfairly, discriminating, or making assumptions about someone. By combining the protection of personal data and ethical principles Van den Hoven and Vermaas (2007) list the following:

1. prevention of information-based harm
2. prevention of informational inequality
3. prevention of informational injustice, and
4. respect for moral autonomy

Not *harming* means for example preventing financial and physical damage, *equality* means for example that gathering information about the individual consumer should be an open, transparent, participatory process, and notification should be part of a fair contract. *Injustice* is the control and exploitation of a social good that has a great value to someone else. Also the sharing of personal information with another sphere is problematic: Medical information can to a certain extent be used for other medical purposes without the objection of the person, but not for socio-economic analysis that could end up in discrimination. Library search data can be used for statistics, but not for statistics that criticize the taste of the person. This is informational cross-contamination. Informational injustice is disrespect for boundaries; spheres of justice are spheres of access. *Moral autonomy* should be respected. Modern contingent individuals have cast aside the ideas of historical and religious necessity, living in a highly volatile socio-economic environment, with a great diversity of audiences and settings before which they appear. Therefore they should not be *fixed in their moral identity*. As an author of one's own life, the individual should not be determined by previous actions. Data-protection laws should provide protection hereof. (Van Den Hoven & Vermaas 2007)

In several projects, ethicists and social scientists have analysed some ethical issues raised by security technologies where nanotechnology may be applied. These issues include surveillance, security ethics and again research policy.

Surveillance

The Commission on the Ethics of Science and Technology, Canada advised on the ethics of new surveillance and monitoring technologies (NSMT) including biometrics, video surveillance and RFIDs especially those applied for security. It was more concerned about a proliferation of "little brothers" in the emerging private security sector outside of democratic control than about the governmental

“big brother”. The primary objective should remain the protection of democratic societies against the risk of compromise to its fundamental values. Ethical issues include the need for assessment of the relevance, effectiveness and reliability of NSMT, proportionality of response to insecurity (including compulsory ethics modules in training of private security personnel), social acceptability, consent, respect for the end purpose (avoid function creep), protection of personal information (especially in RFID-applications and in international data exchange). The issues should be resolved in a well-organised public dialogue. (CEST, 2008)

Regarding ICT technologies and nanoelectronics and their increasing capacity for surveillance, three additional issues should be discussed according to Noela Invernizzi (2011):

a) Workplace control - increasing use and performance of these technologies is expected to increase labor control at the workplace. The trend is not new and has had severe implications for labor organization. In addition, continuous individual surveillance, connected with very demanding production goals, has already created a lot of health problems for workers, such as stress and related diseases.

b) Political control versus political participation - the use of these technologies in the politic domain have far-reaching ethical implications. They have allowed interesting ways of civilian organization, as we have recently seen in the Arab world, but also we have seen how easily this networks can be influenced by foreign policy interests (as the US entering in facebook in Egypt and other countries), affecting the countries' sovereignty.

c) The risk of cultural loss and the new possibilities opened for acculturation. ICTs have contributed to a process of globalizing cultural patterns and acculturation through the imposition of dominant patterns around the world. Hard implications on this are foreseen, since it is a new form of cultural colonialism. (Invernizzi, 2011)

Security ethics

In the INEX project, Isabelle Ioannides and Matteo Tondini have found that security professionals' moral point of view is a “preventive logic” aiming to protect their country / the EU from what they consider external threats (migrants, terrorists). Security professionals expect technology to offer useful tools for settling moral dilemmas in execution of a precautionary approach. (Ioannides & Tondini, 2010)

Research ethics

The EU-funded PRISE project proposed privacy enhancing principles for security research funded in EU FP7 including:

- there is a baseline of privacy that is inviolable
- privacy and security is not a zero-sum game
- general access for law enforcement authorities to existing databases is not acceptable
- preservation of privacy is a shared responsibility
- use of PRISE criteria in FP7 project evaluations is an important step
- privacy enhancement is an essential non-functional requirement
- privacy protection requires continuous further development and reassessment of criteria (PRISE, 2008, 2008a)

Altmann (2006) evaluated applications of nanotechnology in CBRNE sensors positively from a perspective of preventive arms control. Such nanosensors could help avoid casualties due to the use of such weapons.

3.4 What are new issues for the debate and who could do what?

The most controversial security applications of nanotechnology are based on nanoelectronics. Therefore, issues raised by security applications overlap with issues raised by ICT applications of nanotechnology. Several security systems and policies have given rise to public debate. However, nanotechnology is not the key issue in those debates. The issues discussed by policy makers and stakeholders in relation to nanotechnology-enabled security technologies are political and research ethics-related. A key political issue is the right balance between the fundamental rights to liberty and security. The research ethics discussion focuses on the problem that the current ethics review (of EU funded projects) is too narrow. These debates are already on the policy agenda and the European Commission has taken initiatives to solicit advice and develop a code of conduct for security technology research. Researchers could follow and participate in the discussion.

Ethicists and social scientists discuss and write about surveillance, security and privacy enhancing design of security technologies. Even though the recommendations from these experts are more general, they should also be taken into account for security applications of nanotechnology.

Surveillance

A current trend in surveillance is the changing practice of security: securitisation. This can be described by two metaphors: the panopticon and big brother. In contemporary interpretations of the panopticon, ICT enabled databases are not so much invading privacy (as in the classical panopticon), but “making people up”. Rather than one governmental big brother, a wide variety of private little brothers are considered to give rise to issues of control.

The *three tests* suggested by Lyon for testing regulation practices in *privacy issues*: Participation, personhood and purposes, could be useful in both regulation of security technologies and security research. The definition by Van den Hoven and Vermaas of privacy as attempt to prevent others from harming, treating unfairly, discriminating, or making assumptions about someone could also be useful for both purposes.

For nano-enabled surveillance technologies, the ethical issues identified by CEST could also be taken into account. These include the need for assessment of the relevance, effectiveness and reliability of technologies, proportionality of response to insecurity, social acceptability, consent, respect for the end purpose, and protection of personal information. In addition the suggestion by Invernizzi to include workplace control, political control versus participation and cultural loss in the discussion could also be taken over.

In this conceptual debate, ethicists should take the lead. Policy makers could also take the suggestions into account in discussions on the implementation of security technologies, and researchers could take them into account in privacy enhancing design of surveillance systems.

Research ethics

The guidelines proposed by the PRISE project could be useful to improve the current research ethics practice for security research. In addition, Altmann’s criteria for preventive arms control could be taken into account in assessing security research. The European Group on Ethics and European Commission could take these suggestions into account. Researchers could also take them into account in security research projects.

4 Civil / military dual use of nanotechnology

There is an eternal tension between civil and military applications of dual use technologies.²⁵ Currently there are two main political and stakeholder debates. The first focuses on the potential abuse of biological and chemical research and industrial facilities, knowledge and products for weapons of mass destruction (WMD) by terrorists or hostile states. The second debate is mainly related to European Union security research funding practices. The current broad definition of dual use in the ethical guidelines could be interpreted such that all security research should be evaluated by an ethics review panel. Other general issues include the appropriate balance between the fundamental rights to security and freedom in specific cases (e.g. restrictions on academic freedom and trade restrictions) and soldier enhancement, implants and brain-machine interactions. New trends in nanotechnology with particular dual use character include metamaterials and quantum computing.

4.1 Which ethical and societal issues are raised by current technical and economic trends in nanotechnology for dual use applications?

In the general sector report on Security (ObservatoryNano, 2009) the current strategy for developing nanotechnology for security demonstrates a narrow focus on terrorism and narcotics. Other security issues including warfare and most crimes are not treated in that report. Dual use is acknowledged in that report, e.g. detection of chemical substances incl. industrial toxins and chemical warfare substances. Nanotechnology also offers opportunities for personal protective clothing and equipment for first responders (NBCR, firefighters). This has so far not given rise to discussion on ethical, legal or social issues.

Recent technological trends including nanobiosensors and nanowires offer dual use potential for medical diagnostics and bioterrorism monitoring.

Foresight of dual use nanotechnology has been discussed for several years. By 2003, nanotechnology was expected to contribute to (US) “national security in an age of asymmetric warfare and terrorism, through global surveillance and universal tactical and strategic awareness. This constitutes a revolution in military affairs, in which the whole idea is to take small groups of people and put enormous capability in their hands through very small systems. Yet this may also lead to a loss of privacy among those whose security is protected, through very large databases, quantum computation, decryption and universal genomics.” (Roco & Bainbridge, 2003)

In Europe, the European Defence Agency EDA’s Joint Investment Programme on Innovative Concepts and Emerging Technologies JIP-ICET called for proposals in a number of areas including “nanotechnologies for soldier protection and sustain”, and “nanostructures electro-optical and others”. The funding of €15.6 M. came from Cyprus, Germany, Greece, Spain, France, Italy, Hungary, Norway, Slovenia, Slovakia and Poland. In total 8 projects were selected, including two related to nanotechnology: Novel nanostructured optical components for CBRN detection and high

²⁵ “Dual use” is traditionally a term that implies that certain technologies or other resources can both be used for civil and for military applications. However, in philosophical debates, “dual use” can also mean that a technology can be used for good and bad purposes, where the distinction between military and civil uses is not made. (C.f. Bruggen, 2010)

performance opto-microwave links (NANOCAP) and Personal biological aerosol tester for exposure control with high efficiency (PATCH). (EDA, 2009)

In the Dutch national nanodialogue, the project Nanorights and Peace tabled discussions on implications of nanotechnology for international peace and security. In one of those discussions, Major-General (ret) Kees Homan and NanoNed chairman prof. Dave Blank discussed the dual use potential of nanotechnology. Homan recalled that military robots will be increasingly enabled by miniaturization in the semiconductor industry following Moore's law. Military robots are used for dirty, dull and dangerous work (3D). Military strategists consider them the ideal response to the increasing lethality of warfare and to address proliferation of weapons of mass destruction (WMD). Several types of military robots are already deployed. Blank expected that intelligence for robots will need supercomputers enabled by nanotechnology (quantum computing). (cited in Malsch, 2010)

Blank discussed existing labs on a chip: complete laboratories on a very small scale. This makes it possible to detect e.g. tumour cells rapidly and respond quickly: an in vitro health test. The next step will be to inject the whole system in a container into the body for in vivo detection and therapy. This technology is inherently dual use. On the one hand, a killing machine could be a 100 nm small container. On the other hand these devices can enable very cheap healthcare for poor people in developing countries. (cited in Malsch, 2010) Walhout²⁶ acknowledges that dual use of for example lab-on-a-chip technology must not be neglected, but thinks that using such technologies for WMD is highly inefficient and therefore a bit unlikely

A symposium on "Avoiding technology surprise for tomorrow's warfighter," (NRC, 2010) organised in the USA identified several nanotechnology trends of concern. Miniaturised sensors and nanophotonics were expected to contribute to the "death of privacy". Nanotechnology was also considered to have a high dual use potential. Nanotechnology was furthermore deemed to contribute to innovation in production and process technologies, but this was not considered to present security risks in the foreseeable future.

Nanotechnology and synthetic biology were considered trends of concern in a discussion on dual use aspects of converging emerging technologies at BIO2010. Synthetic biology raised more concerns than nanotechnology. (Dodson, 2010)

To conclude, three main trends can be distinguished in dual use nanotechnology. The first is a general trend that civil and military research in emerging technologies is overlapping. This trend could lead to reduced transparency in science and to secrecy of research results. The second is the potential that nanotechnology could be abused for WMD. The third is miniaturisation of ICT which can also be applied in military as well as civil applications. In the next section, recent concerns of policy makers and stakeholders related to these trends are examined.

4.2 Which relevant issues are currently being debated by policy makers and stakeholders? Which issues apparent from the technical and economic trends are not discussed sufficiently?

In recent years, nanotechnology has surfaced in several policy and stakeholder debates related to dual use technology. These debates include a general debate on the desirable relation between civil and military research and the debate on weapons and dual use materials of mass destruction. The latter debate has featured high on the international political agenda since 9/11/2001 and includes a

²⁶ Rathenau Institute, personal communication March 2011

wide range of specific issues relevant to research in nanosciences and nanotechnologies, especially nanobiology, nanomedicine and converging technologies.

4.2.1 Relation civil-military security R&D

Discussions of the relationship between civil and military security R&D have entered the agendas of the peace movement as well as defence circles. There is not much interaction between the two.

Alexis Vlandas (2006) tabled a discussion in the NGO Scientists for Global Responsibility (SGR) on governance of nanotechnology to prevent negative environmental, security, health or social impacts. He was especially concerned about secret commercial and military research. Whistleblowers could warn in time against negative developments. SGR has been working on a project warning against military influences on research since 2003. Another issue discussed in the peace movement are the opportunities offered by civil applications of and R&D in nanotechnology for preventive arms control directed at dangerous military developments. (e.g. Altmann, 2006)

In Europe, the European Defence Agency EDA has been promoting better integration between European Defence Research & Technology (R&T) and Civil Security R&D (including in FP7 and later). (EDA, 2009) Similarly, the European Commission's policy for strengthening the European security industry also includes promoting synergies between civil and defence technologies. (EC, 2010a) The European Parliament "strongly supports the establishment of synergies between civil and military capabilities;" ... "the EDA [European Defence Agency] should play an operational role in developing dual technologies and civil and military capabilities; takes the view that, inter alia, the security strand of the Framework Programme for Research and Technological Development could serve as a basis for developing such synergies;" (EP 2010, art 69)

The US based Foresight Institute started a discussion on the expectation that "Nanotechnology-enabled quantum computation may fuel a security race". This is considered to be an argument to convince the US Congress to fund nanotechnology. (Steinberg, 2010)

INES, the International Network of Engineers and Scientists for Global Responsibility started a campaign in January 2011 calling upon researchers to reject research for the military by signing an appeal to the heads of universities and responsible academic bodies. This campaign builds upon a debate in Germany on the "civil clause" in universities' constitutions that has been ongoing for some years since the merger of the Forschungszentrum Karlsruhe (with a civil clause its foundation in the mid-1950s) and the University of Karlsruhe (without a clause) to extend the clause to the whole new Karlsruhe Institute of Technology. (INES, 2011)

4.2.2 Weapons and Materials of Mass Destruction

A key issue in dual use of science and technology is the risk that technology developed for peaceful purposes could be abused by state or non-state actors for weapons of mass destruction (WMD). Since the start of the so-called War on Terror (by the USA) in the aftermath of 9/11/2001, governments have increased their efforts to prevent proliferation of not only weapons of mass destruction, but also the materials and knowledge that can be abused for WMD. The international Weapons of Mass Destruction Commission (WMDC, 2006) proposed a comprehensive approach to ban WMD. Part of their analysis and recommendations is valid for science and technology with a dual use potential including nanotechnology, as presented below.

In 2002, the G8 initiated a Global Partnership Against the Spread of Weapons and Materials of Mass Destruction. One of the instruments used is International Non-proliferation and Disarmament Assistance (INDA). This is mainly applied in Russia, but part of the methodology could also be useful in other countries for assuring a chain of custody over sensitive materials and preventing misapplication of scientific and engineering skills. WMDC recommends that “Biosecurity projects should be developed and financed under the Global Partnership. All countries with facilities working with dangerous pathogens or toxins should be eligible for financial support.” (WMDC, 2006) In 2009, the G8 adopted “recommendations for a coordinated approach in the field of Global Weapons of Mass Destruction knowledge proliferation and scientist engagement” under the Global Partnership. (G8, 2009)

WMDC not only addressed states but also companies, scientists and civil society. Companies are increasingly forced to take their responsibility in the chain of custody of sensitive materials. Scientists are made aware of biosecurity risks and their responsibility through codes of conduct. National and international forums have a role in preparing, evaluating and reviewing the implementation of such codes. In particular, the International Committee of the Red Cross (ICRC), UN Educational, Scientific and Cultural Organization (UNESCO), the states parties to the Biological and Toxin Weapons Convention (BTWC) and International Union of Pure and Applied Chemistry (IUPAC) have taken relevant initiatives.²⁷ (WMDC, 2006)

Until now, nuclear, biological and chemical WMD are regulated separately through international treaties with different regimes and support mechanisms. A more comprehensive approach could be desirable but difficult to achieve in practice. WMDC recommended that the UN Security Council (UNSC) should establish a small sub-unit that could provide professional technical information and advice on matters related to WMD. At the request of UNSC or the UN Secretary General, it should organise ad hoc inspections and monitoring in the field, using a roster of well-trained inspectors that should be kept up to date. The UN machinery works on three levels:

- The deliberative level (UN Disarmament Commission)
- The consensus-building level (UN General Assembly 1st Committee)
- A body negotiating treaties (Conference on Disarmament)

Other relevant institutions are the UN Department for Disarmament Affairs that supports treaties without their own institutional structure including the Non-Proliferation Treaty (NPT) and BTWC, and UN Institute for Disarmament Research (UNIDIR). The WMDC recommended that the UN General Assembly (UNGA) should convene a world summit on disarmament, non-proliferation and terrorist use of WMD. This summit should take decisions to improve the efficiency and effectiveness of the UN machinery.

One existing measure is UNSC resolution 1540 that obliges UN Member States to stop non-state actors from acquiring WMD. This will be discussed later. (WMDC, 2006)

Dual use nanotechnology related to the Chemical Weapons Convention

The Organisation for the Prohibition of Chemical Weapons (OPCW) is responsible for verification of and institutional support for the Chemical Weapons Convention (CWC). A Scientific Advisory Board (SAB) to the OPCW monitors progress in science and technology that is relevant to the CWC (including new dual use risks as well as opportunities for peaceful cooperation and verification of the treaty). In 2008, the SAB reported on 11 relevant trends in science and technology, including in nanotechnology: “Advances in particle engineering and nanotechnology may lead to more effective

²⁷ ICRC: <http://www.icrc.org/eng/resources/documents/misc/gas-protocol-100605.htm> UNESCO Global Ethics Observatory: <http://www.unesco.org/shs/ethics/geo/user/?action=search&lng=en&db=GEO5> BTWC: [http://www.unog.ch/80256EE600585943/\(httpPages\)/04FBBDD6315AC720C1257180004B1B2F?OpenDocument](http://www.unog.ch/80256EE600585943/(httpPages)/04FBBDD6315AC720C1257180004B1B2F?OpenDocument) IUPAC: <http://www.iupac.org/objID/Article/pac7811x2169>

delivery systems.” The SAB concluded that a major offensive programme would be required to convert a new biologically active toxic chemical into a chemical weapon. Another new related trend is the convergence of biology and chemistry. This may give rise to problems of verification of the CWC because there are differences between design criteria underlying the CWC verification regime and the characteristics of the facilities in industry and academia at the forefront of the cross-over between chemistry and biology. There are also legal issues due to overlap between the CWC and the BTWC. The Director General of the OPCW concluded that further study and advice on these trends was needed from the SAB, States Parties to the CWC and stakeholders. (OPCW, 2008)

Biological and Toxin Weapons Convention and scientific and technological convergence

In 2011, the 7th review conference of the Biological and Toxin Weapons Convention (BTWC) will take place in Geneva. During a preparatory conference in Beijing (4-6 November 2010), several proposals were made for strengthening the convention. Three proposals were relevant to science and technology:

- “To improve specific efforts to strengthen education, outreach, awareness raising and codes of conduct amongst those involved with the life sciences. [...]”
- To develop CBMs [Confidence Building Measures] in light of advances in the biological sciences and technology.
- To establish working groups to discuss specific issues such as cooperation, science and technology.” (co-chairs summary, 2010)

The Review Conference will be prepared in a Prep Com (preparatory committee) meeting 13-15 April 2010/11 in Geneva. In conjunction to this several organisations are organising side events, including two on scientific and technological developments, by SIPRI, Sweden and the UK, and by the US National Academies of Science.

Definition of dual use related to research and technology

The definition of “dual use” science and technology is under discussion. “Dual use” is a ground for sending EU FP7 project proposals to ethical review, but the term is not very well-defined. As a result, all projects under the thematic programme “Security” may have to go through ethical review, resulting in long administrative procedures.

Currently, the EC applies the following definition of “dual use” research in its ethical review guidelines: “Generally speaking, dual use is a term often used in politics and diplomacy to refer to technology which can be used for both peaceful and military aims, usually in regard to the proliferation of nuclear weapons.

Ethical issues of dual use might arise in cases where:-

Classified information, materials or techniques are used in research

Dangerous or restricted materials e.g. explosives are used in research

The specific results of the research could present a danger to participants, or to society as a whole, if they were improperly disseminated” The guidelines also specify how to deal with potential dual use. (Cordis, 2010a)

The UK Parliamentary Office of Science and Technology (POST, 2009) examined “The dual use dilemma” in scientific research. “Dual use dilemmas arise when the same scientific work can be used to do good or be misused, and it is unclear how to prevent misuse without foregoing beneficial applications. ‘Misuse’ can be interpreted differently, but is defined here as any unethical intended use of science, in civilian or military settings.” Misuse could be prevented by targeting scientific practice, dissemination of scientific information and the use of technologies. Such measures will have to avoid impeding scientific progress as much as possible. A risk-benefit assessment could be useful in limiting risks of misuse. (POST, 2009)

There is a need for raising awareness of potential implications of nanotechnology for peace and security in education of engineering students. Nanotechnology research should retain its open source character and be accessible to anyone. (Malsch, 2010)

Preventing technology transfer of dual use goods and technologies

A key issue in the international debate on WMD is how to prevent proliferation to states and terrorists. This debate increasingly includes civil technologies and knowledge that could be abused in WMD. Some nanotechnologies are explicitly included. Relevant aspects of some recent key agreements are discussed below. The Wassenaar Arrangement covers conventional dual use technologies, not WMD, but is included here because it is valid for some applications of nanotechnology.

The Wassenaar Arrangement (2003) gives among others guidelines for its 40 member states how to prevent intangible transfer (non-material, e.g. blueprints, classified knowledge) of dual use technologies to suspect states as well as non-state actors. The intangible technology transfers subject to export controls should be specified in national laws and regulations. These laws should not cover basic science or knowledge in the public domain. Because the cooperation of industry, academia and individuals is needed for effective export controls, governments should raise awareness of international technology transfer controls, identify those in possession of controlled technology and promote self-regulation.

UN Security Council resolution 1540 requires states to adopt and enforce laws prohibiting non-state actors to “manufacture, acquire, possess, develop, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery ...” The resolution also requires states to take measures to prevent proliferation of these weapons and means of delivery and related materials. Such measures include export controls as well as measures to prevent proliferation to non-state actors inside the country. (UNSC, 2004)

At EU level, Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfers, brokering and transits of dual-use items (Recast) gives the following definitions:

“1. ‘Dual-use items’ shall mean items, including software and technology, which can be used for both civil and military purposes, and shall include all goods which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices.”
...2. ‘Export’ shall mean: ... (iii) transmission of software or technology by electronic media, including by fax, telephone, electronic mail or any other electronic means to a destination outside the European Community; it includes making available in an electronic form such software and technology to legal and natural persons and partnerships outside the Community. Export also applies to oral transmission of technology when the technology is described over the telephone.” (Council, 2009, Article 2) This Regulation includes an extensive list of dual-use items as well as a catch-all clause (article 4) “requiring authorisation for exports of any items which are or may be intended for use in connection with weapons of mass destruction, as well as conventional arms if these are to be exported to destinations under an arms embargo.”

Controls on technology transfer do not apply to information in the public domain or basis science. Except for nuclear technologies, such controls also do not apply to the minimum necessary information for patent applications. The list explicitly or implicitly includes several nanomaterials and devices or systems incorporating nanotechnologies. E.g. amorphous or nanocrystalline alloy strips with stipulated properties and nano-imprint lithography tools. (Council, 2009)

Amateur science and technology

There is an emerging community of amateur scientists primarily in the USA, but with participants from other countries as well. (OSF, 2010) Most current activity seems to be in amateur biology (DIYBio, 2010), which is at the same time arousing the most concern among policy makers because of the associated biosecurity risks. (Millet, 2010, WWICS, 2010) Another initiative taken by Chris Peterson of the US-based Foresight Institute is the Open Source Sensing Initiative, intended to grow into a bottom-up community based alternative to top-down government programmes for BCRN sensing. This does not seem to be very active. (OSC, 2009)

There are justified concerns over developments in 5-10 years in particular in synthetic biology/nanobiology.²⁸ There is discussion whether or not the necessary equipment would be affordable for amateur scientists. Currently, used DNA synthesizers can be bought for maybe 10,000 €, not outside of a small group. DIY-biology equipment comes at tens to 100s of \$. However, whether it is really feasible in practice is another question. (c.f. discussion in Ledford, 2010)

In 2010, Kellman (International Security and Biopolicy Institute) pointed out the historic connection between international power and the ability to use violence threatening international peace and stability on the one hand and concentrated economic potential and industrial power on the other. New and emerging technologies are contributing to increasing independence of the capacity to change the course of history of state or economic power. Garage companies may in the future acquire the concentrated power to commit mass violence through bioterrorism. The potential perpetrators could in the long term be anyone anywhere, and be unnoticed and disconnected from centres of military and economic power. This risk is currently limited because of the need for investment in high tech research infrastructure. Kellman foresaw a new emerging threat of generalised “disease weapons”, including chemical, biological or nano-agents whereby the distinction between chemical and biological agents is losing its meaning. This gives rise to legal and global governance issues. The BTWC and CWC conventions may have to be adapted and private actors could be given a more important role in protecting the world against WMD next to governments. (Kellman, 2010)

Public perception of dual use science

A large majority of European Union citizens (78%) believes that science and technology could in the future be used by terrorists; only 7% disagree with this statement in the Special Eurobarometer study 340 on Science and Technology. Respondents in Norway (95%) Iceland (93%) and Denmark (91%) agree more and in Romania (65%), Italy (64%) and Turkey (59%) agree less with this statement. Those who are very interested in science (85%), the very informed and those who stayed in full-time education until age 20 (84%) and managers (83%) agree most frequently. (EC, 2010, p 65-66)

To conclude, it appears that the discussion on the relation between civil and military R&D so far has not attracted much attention. The discussion on dual use (nano)technologies in relation to WMD engages a much wider audience, but even there the discussion tends to be limited to politicians and policy makers, the research community and industry. A small group of specialist NGO's and scientists is also contributing to the debates on international level.

²⁸ See the corresponding project at UNICRI: <http://lab.unicri.it/bio.html>

4.3 What are the issues discussed by ethicists and social scientists writing about nanotechnology? Which new insights do they have to offer for the policy and stakeholder debate?

Relevant discussions among ethicists and social scientists focus on three types of issues. These include developments in the relationship between policies for defence and security and research in Europe, dual use aspects of WMD (in particular related to biosecurity) and ethical aspects of military robots enabled by miniaturisation of ICT.²⁹

Trends in relations defence & security research and innovation policies and ERA

The EU funded project SANDERA (James, 2010) has explored trends in the relationship between European defence and civil security research and innovation policies and the European Research Area (ERA) until 2030. Policies of the European Union as well as intergovernmental cooperation in the three policy areas are taken into account. SANDERA has developed four scenarios dominated by different types of relations between the policy domains: indifference, cooperation, integration and competition. By analysing literature from different sources, SANDERA has identified a number of key trends and drivers of changes related to the three policies in the 1990s and 2000s.

“The blurring of the boundary between the defence and security domains represents a potential important driver of change in the relationship between the ERA and other policy domains.” (James, 2010, p7) The project therefore treated the security/defence R&I policy relation as a driver in its analysis and concluded that security R&I (an important thematic programme in FP7) is much closer aligned to the ERA than defence R&I. Security R&I is defined against defence R&I as the “other”. Security research is increasingly mainstreamed in EU policies, including by DG Home Affairs, MARE and TREN. According to insiders, the decision how defence R&I will be related to the future of the ERA will be taken by the end of 2011. To support this decision making, SANDERA developed four scenarios until 2030 focusing on the relationship between the ERA and defence R&I policy. The role of security R&I is explicitly addressed in each scenario. SANDERA distinguished three types of trends and drivers of change: contextual, specific for one policy area and specific for the boundary between policy areas. (James, 2010)

One of the key contextual trends distinguished by SANDERA is a changing knowledge dynamics where emerging technologies including nanotechnology play a role. “... generic technologies will become increasingly important in all areas of life including defence and security applications and have the potential for misuse. Trends indicate that the most rapid technological advances are likely to be in ICT, biotechnology, cognitive sciences, sensors and networks, and smart materials. Nanotechnology is likely to be an important enabler for other developments, for example in electronics, sensors and commodity manufacturing.” (Original source: UK MOD, DCDC Global Strategic Trends Prognosis 2007-2036) “Military applications of nanotechnology could have potential destabilising effects and there may be spill-overs from military use of converging technologies to crime and terrorism.” (Original source: Nordmann et al, 2004, “Converging Technologies; Shaping the Future of European Societies.”) “Terrorists and criminals might abuse new emerging technologies for their purposes. This concerns in particular the output of robotics, nanotechnology in combination with medicine, cognitive sciences, sensors, networks and smart materials. (James, 2010, p 13, original source Ministries of Defence of France, Italy and UK) In addition, the emergence of more countries with high tech R&D capacity and proliferation makes regulation and control of novel technologies more challenging. (Original source: UK MOD DCDC, UK, 2007) SANDERA observed a move towards

²⁹ There is also a more fundamental philosophical discussion on interpretations of the term “dual use” including whether these technologies are primarily developed for military purposes or for civil applications. This discussion goes beyond the scope of this report.

open innovation combining civil and defence research. However, the pace of change depends on the willingness of non-traditional sources of S&T knowledge to engage with the defence sector. These non-traditional actors are operating on the boundary between defence and security, and civil technology development and applications. These new actors are important because there are major cultural differences between universities and the defence sector. The main trend in the 1990s and 2000s was an emerging “new social contract of science,” implying greater emphasis on the societal relevance of research in the ERA. EU science and technology policy may in the coming 20 years develop along a continuum between the ERA as end in itself and the ERA as a means to societal Grand Challenges. (James, 2010)

Dual use and biosecurity

The literature on national security, research and ethics reflects that some technologies are under an absolute ban (Atlas 2009): The Biological and Toxin Weapons Convention (BTWC) imposes a ban on biological warfare and the development of biological weapons. However there is a lack of verification and compliance protocols. The States Parties to the BTWC are obliged to incorporate the prohibitions imposed by the convention in their national legislation. E.g. in the US there is a separate act, the Biological Weapons Anti-Terrorism Act. Certain knowledge that has little peaceful application potential is prohibited. However, there is a risk that knowledge that is prophylactic or protective could lead to the development of biological weapons. The question is raised whether scientific knowledge is *value-free* as is it often thought. If so there should not be any limits to it, since it is only the use of science that is harmful. But if there is ‘dangerous research’ then it should not be conducted and knowledge that falls in this category should not be shared.

The problem is that the research of concern is within the life sciences. It is very often aimed at protecting humankind from disease or otherwise improving the quality of life. Such knowledge is not thought of as being neutral, but as being ‘good’. Research is also a global endeavor and not limited geographically to an area that falls under one legislator. This type of research would often fall into the category of ‘sensitive but not classified’.

The US National Science Advisory Board for Biosecurity (NSABB, 2007) has sought to delineate a threshold that would identify the subset of dual use life science research. NSABB considers this to be research with the highest potential for yielding knowledge, products or technology that could be misapplied to threaten public health or other aspects of national concern. Such research *could rise* to the same level of concern as the legal concept of ‘clear and present or clear and imminent danger’ by meeting the following criteria: Research that (1) enhanced the harmful consequences of a biological agent or toxin; (2) disrupted immunity or the effectiveness of an immunization without clinical and/or agricultural justification; (3) conferred to a biological agent or toxin, resistance to clinically and/or agriculturally useful prophylactic or therapeutic interventions against that agent or toxin, or facilitated their ability to evade detection methodologies; (4) increased the stability, transmissibility, or the ability to disseminate a biological agent or toxin; (5) altered the host range or tropism of a biological agent or toxin; (6) enhanced the susceptibility of a host population; or (7) generated a novel pathogenic agent or toxin, or reconstituted an eradicated or extinct biological agent.

Codes of conduct for life sciences

In order for the life sciences not to become the death sciences *codes of conduct* are recommended. The scientists should assess their research efforts for dual use and report and behave as appropriate. They should be aware of the possibilities for dual use and how knowledge can cause harm. Scientist should also serve as role models. (Atlas 2009)

The *advantage* of codes of conduct for science is that these codes raise awareness regarding social responsibility and may help win public trust. There may also be several process benefits of the development and implementation of the codes in terms of deliberation and communication for example between organizations. The *limitations* of the codes are such things as the universal formulations of principles: When the codes cover several research disciplines and lack detail and thus become too general and common sense. Also the codes are considered to be without effect if they are not enforced, by self-governance of the members, professional societies, funding bodies, or by law. (Selgelid 2009)

The codes of conduct must strike a balance between the *promotion of scientific progress* on the one hand, and the *promotion of security* on the other hand. Self-governance is the solution to the reluctance from scientists to have too much governmental interference in their work. However, self-governance is problematic when researchers lack expertise in the area of assessing security dangers of their research. (Selgelid 2009)

Definitions of dual use

A clear definition of the concept of 'dual use' is sought in the philosophical literature. Such a definition would help scientists and policy makers when considering whether a given technology or area of research is potentially harmful in one of its uses even though it was not intended for this purpose. If the definition is too narrow in scope it may overlook dangerous technologies. However, the definition could also be too wide including research that only has a remote chance of being used by terrorists. This would lead to an administrative overload for the researchers and interfere with innovation and progress.

According to Resnik, NSABB proposed a definition of 'dual use research of concern' as 'research that, based on current understanding, can be reasonably anticipated to provide knowledge, products, or technologies that could be directly misapplied by others to pose a threat to public health, agriculture, plants, animals, the environment, or material'. Concepts that could need further clarification are 'reasonably anticipate' an outcome and 'threat'. What is reasonable: non-zero, 5 or 10%? And what is a threat: the loss of one human life, ten or one hundred? Or is it a million dollar economic loss? (Resnik 2008)

Other key issues in dual use are: controlling access to materials and technologies, providing training for investigators, weighing the risks and the benefits of publishing dual use research, and safeguarding the freedom of inquiry. (Resnik 2008)

Van der Bruggen (2011) proposed a definition of dual use for biosecurity purposes that could be suitable also for other dual use technologies:

"A dual use problem arises when

- research, based on current understanding, can be reasonably anticipated to provide knowledge, products, or technologies that could be misapplied and;
- there is a recognizable threat and a not negligible chance of such misuse and;
- there are serious consequences for society and science (public health and safety, agriculture, plants, animals, the environment, or material)."

Trends in dual use technologies

Nixdorf & Dando (2009, p 37, 41) were concerned about dual use potential for biological weapons of several new trends in nanotechnology including: artificial viruses (polymer based complexes of nanoparticle size containing DNA), aerosol delivery of nanoparticles, including nasal and respiratory tract delivery, crossing the blood-brain barrier.

Benjamin Wittes (2010) warned that new technologies including gene technologies and ICT could in the coming decades empower individuals with access to the means to develop and distribute biological weapons. Governments do not have suitable means to counter this emerging threat and might respond by severe restrictions on civil liberties without actually increasing security. Proper response might require constitutional change. Responsibility for security will be distributed over a range of private and university actors.

Dando & Pearson (2011) analysed the provision of scientific and technological advice to the BTWC. The authors noted a significant increase in the pace of advances in life sciences relevant to the convention. This includes both life sciences that could pose new biosecurity risks and developments in detection and countermeasures. Synthetic Biology is explicitly mentioned. Dando & Pearson recommended that “The 7th Review Conference should agree that a meeting of Science and Technology Experts should be tasked by a future Annual Meeting of States Parties to consider the implications for all aspects of the Convention of the current and likely developments of a particular topic assigned by the Annual Meeting.”

Ethics of military robots

Miniaturisation including nanoelectronics is expected to contribute to developments in robotics. Robotics is inherently dual use because they can be used for civil and military purposes. Recently, a debate has emerged on ethics of military robots. The implications of this debate for policy makers and stakeholders in nanoelectronics are indirect. The use of drones marks a new area in warfare. In the area of ICT one can not distinguish between R&D for civil applications and for military purpose. Nanoelectronic will be used in i-phones as well as in drones.

According to Homan, ethics of warfare is governed by Just War Theory, including Jus ad Bellum governing political decision making before armed conflict. The availability of military robots may lower the threshold to go to war.³⁰ Jus in Bello governs conduct of armed forces during a war. Legal accountability for actions by military robots must be clarified. Among ethicists, there is a discussion on the ethics of military robots. Whereas Sharkey (2008) considered robots a threat to humanity, Arkin (2008) believed that combat robots can be programmed to be more ethical than human soldiers. Coker (2008) responded that robots function in a meaningless world without ethics. War becomes more and more like a video game. Homan was in favour of Unmanned Aerial Vehicles deployed for intelligence, surveillance and reconnaissance. Human oversight will always be needed. The threatening dehumanization of warfare must be averted. Robots cannot replace the soldier on the ground in winning the hearts and minds of the local population in current asymmetric conflicts. (Homan cited in Malsch, 2010) These issues are also discussed by Sparrow (2007) and Asaro (2007) and Altmann (2009).

It would be beyond the scope of this report to explore the ethics of military robots more in depth. It is just included here to raise awareness of the potential unintended consequences of developing applications of nanoelectronics in miniaturising robots or aiming for smarter robots. Such dual use aspects have for instance been tabled by the Rathenau Institute for medical and military robots in September 2009.³¹

4.4 What are new issues for the debate and who could do what?

³⁰ The same problem applies to all new technologies that provide people with a sense of invulnerability. (JM de Cozar, personal communication)

³¹ <http://www.rathenau.nl/themas/project/sociale-robots.html>

There are four general current debates that may also be relevant to governance of dual use nanotechnology: on the relation between civil and military R&D, on definitions of dual use, on non-proliferation of dual use goods and technologies, and on military robots.

Dual use aspects of nanotechnology are primarily an issue for policy makers and politicians. Researchers and companies can only play subsidiary roles including respecting the law, raising awareness of legal requirements and ethical norms among students and voluntarily taking responsibility for new emerging threats by informing authorities or starting public debates.

Relation civil-military R&D

European policy makers and industry engaged in military R&D tend to be in favour of better integration of civil and military security R&D. The research and industrial community engaged in nanoelectronics and ICT research with potential security applications appears to be avoiding this discussion. This may be because they do not want to do defence related research or because they want no restrictions on their academic freedom to publish their results. It is expected that a decision will be taken on whether or not defence R&D will become part of the future European Framework Programme for Research.

Policy makers could open up consultations regarding this to a wider audience including civil society, the research community and industry. Other actors could actively engage themselves in this debate.

Definitions of dual use

The demand for new definitions of dual use originates from policy makers responsible for (bio)security and protection against WMD, and for ethics review of FP7 security projects.

The European Group on Ethics could take this discussion into account in their requested opinion on ethics of security research.

Non-proliferation

Current legislation and treaties on export controls of dual use goods and technologies exclude knowledge in the public domain and basic science. Some nanotechnologies are listed. This list may be updated as technology progresses. An emerging concern is potential proliferation of (nano)technology to terrorists through amateur scientists. In the short term this risk appears to be not very high because this group is small and the necessary research infrastructure too expensive. However, some experts expect the likelihood of such scenarios to increase in 5-10 years.

Policy makers could install a monitoring body to assess progress in relevant technologies on a regular basis, as proposed by scientists for life sciences relevant to the BTWC convention.

Military Robots

Nano-enabled miniaturisation of robotics has both civil and military applications, but policy makers and researchers engaged in such research for civil applications may not be aware of the dual use aspects. It could be advisable to organise discussions on such dual use aspects in relevant conferences or projects.

Acknowledgement

This report was written in the framework of the ObservatoryNano project, funded by the European Union, grant no. 218528. Comments by the following nanoethics and ELSA experts are gratefully acknowledged: Johann Ach, Jürgen Altmann, Christopher Coenen, José Manuel de Cozar Escalante, Ulrich Fiedeler, Khara Deanne Grieger, Noela Invernizzi, Alfred Nordmann, Olga Pombo, Pere Ruiz Trujillo and Bart Walhout. The contents of this report are the sole responsibility of the authors and can not be attributed to the European Commission in any way.

References

- Aarts, Emile & Grotenhuis, Frits, 2010, "Ambient Intelligence," in Oomen, Palmyre, Wobbes, Theo & Bemelmans, Theo, "Nanotechnologie: betekenis, beloftes en dilemma's," Valkhof Pers, Nijmegen, 2010, www.thijmgenootschap.nl (in Dutch)
- Aarts, Emile & Markopoulos, Panos & de Ruyter, Boris, 2010, "The Persuasiveness of Ambient Intelligence" Data-Centric Systems and Applications, 2007, Security, Privacy, and Trust in Modern Data Management, Part V, Pages 367-381
- Action Grid, 2010, white paper "Linking Biomedical Informatics, Grid Computing and Nano-informatics", Action-Grid project on Grid Computing, Biomedical Informatics and Nano-informatics (2008-10) <http://www.action-grid.eu/>
- Altmann Jürgen, 2006, "Military Nanotechnology; Potential Applications and Preventive Arms Control", in Contemporary Security Studies, Routledge, Oxon, 2006
- Altmann Jürgen, 2009, "Preventive Arms Control for Uninhabited Military Vehicles," in Capurro, R. & Nagenborg, M. "Ethics and Robotics," Heidelberg, Germany, AKA
- Arkin, Ronald C. 2008, Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative / Reactive Robot Architecture, in HRI '08, Proceedings of the 3rd ACM/IEEE international conference on Human Robot Interactions, ACM, New York, 2008, <http://portal.acm.org/citation.cfm?id=1349839&dl=ACM>
- Asaro, P, (2007), *Robots and Responsibility from a Legal Perspective*, Proceedings of the IEEE 2007 International Conference on Robotics and Automation, Workshop on RoboEthics, April 14, 2007, Rome, Italy
- Atlas, Ronald M., 2009, "Responsible Conduct by Life Scientists in an Age of Terrorism", Sci Eng Ethics (2009) 15:293-301
- Bajc, Vida, 2007, "Introduction: Debating Surveillance in the Age of Security", The American Behavioral Scientist. Thousand Oaks: Aug 2007. Vol. 50, Iss. 12; pg 1567, 25 pgs
- Bell, Curtis, 2010, Neurons for Peace: take the pledge, brain scientists, in New Scientist 2746, 8 February 2010, <http://www.newscientist.com/article/mg20527465.900-neurons-for-peace-take-the-pledge-brain-scientists.html?DCMP=OTC-rss&nsref=comment-analysis> ; <http://www.neuroplasticarts.org/2010/03/neuroethics.html>
- Bruggen, Koos van der: "Part A: Possibilities or Intentions: The concept of Dual Use reconsidered," in Miller, Seumas, Selgelid, Michael and Bruggen, Koos van der, "Report on Biosecurity and Dual Use Research; A report for the Dutch Research Council," 3TU Centre for Ethics, January 2011, www.ethicsandtechnology.eu
- Burgess, J. Peter & Rodin, David, 2008: "The Role of Law, Ethics and Justice in Security Practices," PRIO Papers, International Peace Research Institute, Oslo, www.prio.no (last accessed 29-10-2010)
- Capurro, Rafael, 2011, intervention at ETICA-EGAIS-STOA workshop on IT for a Better Future, European Parliament, 31 March 2011, <http://www.etica-project.eu/>

CDPD, 2010, "Bilan du débat public sur le développement et la régulation des nanotechnologies; 15 octobre 2009-24 février 2010 dressé par le Président de la Commission nationale du débat public, 9 avril 2010," <http://www.debatpublic-nano.org/> (last accessed 3-3-2011)

CEST, 2008, "Position Statement: In search of a balance; An ethical look at new surveillance and monitoring technologies for security purposes," CEST, Quebec, 2008, http://www.ethique.gouv.qc.ca/index.php?option=com_docman&Itemid=72 (last accessed 02-02-2011)

CNIL website, "Invasion of the Chips!" CNIL, <http://www.cnil.fr/english/topics/invasion-of-the-chips/> (last accessed 3-3-2011)

Co-chairs summary, "International Workshop on Strengthening International Efforts to Prevent the Proliferation of Biological Weapons: The Role of the Biological and Toxin Weapons Convention," Beijing 4-6 November 2010, [http://www.unog.ch/80256EDD006B8954/\(httpAssets\)/2150469CC970F39AC12577D700543C6E/\\$file/Co-Chairs%20Summary%20-%20RL%20master.doc](http://www.unog.ch/80256EDD006B8954/(httpAssets)/2150469CC970F39AC12577D700543C6E/$file/Co-Chairs%20Summary%20-%20RL%20master.doc) (last accessed 25-02-2011)

Coker, Christopher, 2008, "Ethics and War in the 21st Century, Routledge, Oxon, 2008 <http://books.google.nl/books?hl=nl&lr=&id=1DODjBGnAPE&oi=fnd&pg=PP1&ots=w8loO5xGm1&sig=IQiegkirdIAepPPQOqLIOW5Ad8#v=onepage&q&f=false> (last accessed 7-3-2011)

Cordis website, ICT Ethics guidelines, http://cordis.europa.eu/fp7/ethics-ict_en.html (last accessed 20-07-2010)

Cordis website, dual use ethics guidelines, <ftp://ftp.cordis.europa.eu/pub/fp7/docs/dual-use.doc> (last accessed 19-07-2010a)

Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfers, brokering and transits of dual-use items (Recast)

Czarkowski, Marek, 2008, "The Dilemma of Dual Use Biological Research: Polish Perspective", *Sci Eng Ethics* (2010) 16:99-110

Dando, Malcolm & Pearson, Graham, "Review Conference Paper No. 27. The provision of scientific and technological advice to the Biological and Toxin Weapons Convention," Bradford Disarmament Research, February 2011, <http://www.brad.ac.uk/acad/sbtwc/briefing/RCPapers.htm> (last accessed 25-02-2011)

DIYBio, 2010, Do It Yourself Biology website <http://www.diybio.org/> (last accessed 01-09-2010)

Dodson, Allan, 2010, "The convergence of emerging technologies," *FAS Biosecurity Blog*, 6 May 2010, <http://www.fas.org/blog/bio/2010/05/the-convergence-of-emerging-technologies/#more-3435> (last accessed 3-3-2011)

Ducatel K, Bogdanowicz, M, Scapolo, F, Leijten, J & Burgelman, J-C, 2001, "Scenarios for Ambient Intelligence in 2010," ISTAG, European Commission, IST programme & IPTS, <http://www.ist.hu/doctar/fp5/istagscenarios2010.pdf> (last accessed 07-02-2011)

EC, 2009, report FP7 workshop on advanced nanoelectronics technologies, 11 September 2009, European Commission, Brussels, ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/nanoelectronics/011209-wshop-rep-ai-v7b-clean_en.pdf (last accessed 18-01-2011) http://cordis.europa.eu/fp7/ict/nanoelectronics/documents_en.html

EC, 2009a, "When your yogurt pot starts talking to you: Europe prepares for the internet revolution," Europa press release 18 June 2009, <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/952&format=HTML&aged=0&language=EN&guiLanguage=en> (last accessed 25-01-2011)

EC, 2009b, "Moving the frontiers of ICT – a strategy for research on future and emerging technologies in Europe," COM(2009) 184, http://cordis.europa.eu/fp7/ict/programme/fet/flagship/home_en.html (last accessed 7-3-2011)

EC, 2010, Special Eurobarometer 340, Science and Technology, European Commission, June 2010, http://ec.europa.eu/public_opinion/archives/eb_special_en.htm

EC, 2010a, Strengthening the industrial base, Security Industrial Policy, European Commission DG Enterprise, http://ec.europa.eu/enterprise/policies/security/industrial-policy/industrial-base/index_en.htm (last accessed 19-07-2010)

EDA Annual report 2009: <http://www.eda.europa.eu/genericitem.aspx?id=621> (last accessed 19-07-2010)

EDRI website, Digital Civil Rights in Europe, <http://edri.org/>

EOS, 2010, "EU policies on privacy and data protection and their impact on the implementation of security solutions," European Organisation for Security, September 2010, www.eos-eu.com

EP, 2010: "European Parliament resolution of 10 March 2010 on the implementation of the European Security Strategy and the Common Security and Defence Policy 92009/2198(INI)), European Parliament, Strasbourg, 10 March 2010, <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2010-0061&language=EN&ring=A7-2010-0026> (last accessed 28-09-2010)

Ericson, Lars, 2007, Introduction: Nanotechnology and Biometrics, presentation at Biometric Consortium Conference, 13 September 2007, http://www.biometrics.org/bc2007/presentations/Thu_Sep_13/Session_II/13_Ericson_NANO.pdf

ESRAB, "Meeting the Challenge; The European security research agenda," European Commission, Brussels, September 2006, http://ec.europa.eu/enterprise/security/articles/article_06_09_25_tc_en.htm

ESF, 2006, "Nanoscience and the long term future of the information society (NSIT)," European Science Foundation Forward Look, Strassbourg, <http://www.esf.org/publications/forward-looks.html>

ESF, 2010, "European Code of Conduct for Research Integrity," ESF, Strassbourg, July 2010, www.esf.org

ESRIF, "Final Report," European Commission, December 2009, <http://www.esrif.eu/> (last accessed 27-01-2011)

Est, Rinie van, Stemerding, Dirk, Keulen, Ira van, Geesink, Ingrid, Schuijff, Mirjam, 2010, "Making Perfect Life. Monitoring Report – Phase II" ETAG, Brussels, 10-11-2010, <http://www.rathenau.nl/publicaties/making-perfect-life-monitoring-report-phase-ii.html>

FESTOS, "Wild card scenarios; four stories on future threats," FESTOS project 2011, www.festos.org (last accessed 02-02-2011)

Fiedeler, Ulrich, 2008, *Stand der Technik neuronaler Implantate*, Nr. Wissenschaftliche Berichte: FZKA 7387, Karlsruhe: Forschungszentrum Karlsruhe <http://bibliothek.fzk.de/zb/abstracts/7387.htm> , <http://www.itas.fzk.de/deu/lit/2008/fied08a.pdf>

Fiedeler, Ulrich, 2008a, Technology Assessment of Nanotechnology: Problems and Methods in Assessing Emerging Technologies, in: Erik Fisher/Cynthia Selin/Jameson Wetmore (Hg.): *Excavating Futures of Nanotechnology: The Yearbook of Nanotechnology in Society*: Springer, 241-263

Forge, John, 2009, "A Note on the Definition of "Dual Use"", *Sci Eng Ethics* (2010) 16:111-118

Friedewald, Michael, Raabe, Oliver, Koch, Daniel J, Georgieff, Peter, Neuhäusler, Peter, 2009, Ubiquitous Computing, TAB Report no 131, Berlin 2009, <http://www.tab-beim-bundestag.de/en/publications/reports/ab131.html> (last accessed 18-01-2011)

G8, 2009, "Annex B Recommendations for a coordinated approach in the field of Global Weapons of Mass Destruction knowledge proliferation and scientist engagement," G8 summit 2009, <http://www.partnershipforglobalsecurity.org/Official%20Documents/G-8%20Global%20Partnership/G-8%20Summit%20Documents/index.asp> (last accessed 2-3-2011)

Gordeyev, Sergey & Crawley, Tom, 2011, "ObservatoryNano Briefing No. 11. Nanosensors for Explosives Detection." ObservatoryNano project, March 2011, <http://www.observatorynano.eu/project/filesystem/files/ObservatoryNANO%20Briefing%20No.11%20Nanosensors%20for%20Explosives%20Detection.pdf>

Hof, Christian van 't, 2007, "RFID and Identity Management in Daily Life; striking the balance between convenience, choice and control," STOA study, IP/A/STOA/2006-22, European Parliament, Brussels, <http://www.itas.fzk.de/eng/etag/document/2007/etag07a.pdf> (last accessed 18-01-2011)

Hoven, Jeroen van den & Vermaas, Pieter E., 2007, "Nano-Technology and Privacy: On Continuous Surveillance Outside the Panopticon", *Journal of Medicine and Philosophy*, 32:283-297, 2007

HTSM, 2010, "High Tech Systems & Materials Vision Document," Point-One, Eindhoven, May 2010, <http://www.point-one.nl/>

Hustinx, Peter, 2011, intervention at ETICA-EGAIS-STOA workshop on IT for a Better Future, European Parliament, 31 March 2011, <http://www.etica-project.eu/>

INES, 2011, "Reject research for the military. It is time to act: International Appeal to the heads of universities and responsible academic bodies," INES website 26 January 2011, <http://www.inesglobal.com/commit-universities-to-peace.phtml> (last accessed 03-02-2011)

Invernizzi, Noela, 2011, personal communication.

Ioannides, Isabelle & Tondini, Matteo, 2010, INEX D3.5. Policy Recommendations. Implications of Ethical Dilemma's of Internal / External Security. INEX project, 18-11-2010, http://www.inexproject.eu/index.php?option=com_docman&task=cat_view&Itemid=72&gid=54&orderby=dmdate_published&ascdesc=DESC

ISTAG, ISTAG Recommendations on Future and Emerging Technologies. Report of the ICT Advisory Group (ISTAG) – October 2009, European Commission, DG INFSO, http://cordis.europa.eu/fp7/ict/istag/reports_en.html

James, Andrew D. 2010, "Scenario Report SANDERA; The future impact of security and defence policies on the European Research Area," SANDERA project, Manchester Institute of Innovation Research, Manchester, 22 December 2010, www.sandera.net

Jarmon, Leslie & Keating, Elizabeth & Toprac, Paul, 2007, "Examining the societal impacts of nanotechnology through simulation: Nano Scenario", *Simulation Gaming* 2008 39: 168, <http://sag.sagepub.com/content/39/2/168>

Kellman, Barry, "lecture on "The prohibition of Chemical and Biological Weapons under International Criminal Law – Challenges and Perspectives", International Criminal Law Network's Fall Lecture, Tuesday November 9, 2010, www.icln.net see also: <http://www.biopolicy.org/current-postings>

Koepsell, David, 2009, "Let's Get Small: An introduction to Transitional Issues in Nanotech and Intellectual Property", *Nanoethics* (2009) 3:157-166

Kosta, Eleni & Pitkänen, Olli & Niemelä, Marketta & Kaasinen, Eija, 2009, "Mobile-Centric Ambient Intelligence in Health- and Homecare Anticipating Ethical and Legal Challenges", *Sci Eng Ethics* (2010) 16:303-323

Krahmann, Elke, 2010, "Beck and beyond: Selling security in the world risk society", *Review of International Studies* (2011), 37, 349-372

Krahmann, Elke, 2005, "From State to Non-State Actors: The Emergence of Security Governance", *New Threats and New Actors in International Security*, 2005, Chapter 1

Ledford, Heidi, 2010, "Garage biotech: Life hackers," in *Nature* **467**, 650-652 (2010), <http://www.nature.com/news/2010/101006/full/467650a.html>

Lyon, David, 2001, "Facing the future: Seeking ethics for everyday surveillance", *Ethics and Information Technology* 3: 171-181, 2001

Malanowski, Norbert & Zweck, Axel, 2007, "Bridging the gap between foresight and market research: Integrating methods to assess the economic potential of nanotechnology", *ScienceDirect, Technological Forecasting & Social Change* 74 (2007) 1805-1822

Malsch, Ineke & Hvidtfelt-Nielsen, Kristian, 2010, "Nanobioethics," *Second Annual Report on Ethical and Social Aspects of Nanotechnology*, ObservatoryNano project, online publication, 2010, <http://www.observatorynano.eu/project/catalogue/4NB/>

Malsch, Ineke, 2010, *Nanotechnology, Peace and Security: Don't be Naïve*, *Nanoforum* 24-11-2010,

<http://www.nanoforum.org/nf06~modul~showmore~folder~99999~scc~news~scid~4165~.html?action=longview&>

Millet, Piers D, 2010, International Perspectives; Introductory Comments, paper presented at FBI-DIYBio workshop Washington DC, 22 July 2010,

[http://www.unog.ch/80256EDD006B8954/\(httpAssets\)/2C8C2466169C45F5C1257770004E66B7/\\$file/International+perspectives+-+Millett.pdf](http://www.unog.ch/80256EDD006B8954/(httpAssets)/2C8C2466169C45F5C1257770004E66B7/$file/International+perspectives+-+Millett.pdf) (www.unog.ch) (last accessed 01-09-2010)

Mordini, Emilio & Wright, David & Wadhwa, Kush & De Hert, Paul & Mantovani, Eugenio & Jesper Thestrup & Van Steendam, Guido & D' Amico, Antonio & Vater, Ira, 2009, "Senior citizens and the ethics of e-inclusion", Ethics Inf Technol DOI 10.1007/s10676-009-9189-7

Nanoforum, 2007: Nanotechnology for Civil Security, http://www.nanoforum.org/nf06~modul~showmore~folder~99999~scid~476~.html?action=longview_publication& (last accessed 19-07-2010)

Nixdorf, Kathryn & Dando, Malcolm, 2009, Developments in Science and Technology; Relevance for the BWC, in BWPP Biological Weapons Reader 2009, Bioweapons Prevention Project, http://www.bwpp.org/documents/BWPP%20BW%20Reader_final+.pdf , www.bwpp.org (last accessed 01-09-2010)

Nordmann, Alfred et al. 2004, Converging technologies – shaping the future of European societies. Report by the High Level Expert Group. European Commission, 2004.

Nordmann, Alfred & Rip, Arie, 2009, "Mind the gap revisited," in Nature Nanotechnology **4**, 273-274 (2009), <http://www.nature.com/nnano/journal/v4/n5/full/nnano.2009.26.html>

NRC, 2010, "Avoiding Technology Surprises for Tomorrow's Warfighter," National Research Council, http://books.nap.edu/catalog.php?record_id=12919 (last accessed 25-02-2011)

NSABB, 2007, "Proposed Framework for the Oversight of Dual Use Life Sciences Research: Strategies for Minimizing the Potential Misuse of Research Information," http://oba.od.nih.gov/biosecurity/biosecurity_documents.html

ObservatoryNano, 2009, "General Sector Reports: Security," ObservatoryNano May 2009, <http://www.observatorynano.eu/project/catalogue/2SE/> (last accessed 27-01-2011)

ObservatoryNano, 2009a, "General Sector Reports: Information and Communication," ObservatoryNano, April 2009, <http://www.observatorynano.eu/project/catalogue/2IC/>

OPCW, 2008, "Note by the director-general; Report of the Scientific Advisory Board on developments in science and technology," OPCW 2nd Review Conference, 7-18 April 2008, <http://www.opcw.org/about-opcw/subsidiary-bodies/scientific-advisory-board/related-documents/> (last accessed 2-3-2011)

Opstelten, Ivo, 2010, Kabinetsformatie 2010; 32417 Nr 14, Brief van de informateur, Tweede Kamer der Staten Generaal, Den Haag, 30 September 2010, <https://zoek.officielebekendmakingen.nl/kst-32417-14.html?zoekcriteria=%3fzkt%3dEenvoudig%26pst%3d%26vrt%3dnanotechnologie%26zkd%3dInDeGeheleText%26dpr%3dAfgelopenDag%26sdt%3dDatumBrief%26ap%3d%26pnr%3d1%26rpp%3d10&resultIndex=0&sorttype=1&sortorder=4>

OSC, 2009, Open Source Sensing Initiative website <http://opensourceensing.org/> (last accessed 01-09-2010)

OSF, 2010, Open Science Fund website, <http://opensciencefund.org/>

P4L, 2010, Photonics4Life website: <http://www.photonics4life.eu/>

Point-One, 2008, "From Good to Great in Dutch Technologies, Phase 2; A joint initiative of Point-One and Programme for High Tech Systems," Point-One & HTS, Eindhoven, 2008, <http://www.point-one.nl/> (last accessed 7-3-2011)

POST, 2009, The dual-use dilemma, POSTNOTE 340, July 2009, Parliamentary Office of Science and Technology, London, UK, <http://www.parliament.uk/documents/post/postpn340.pdf> (last accessed 01-09-2010)

PRISE, 2008, "PRISE Concluding Conference Statement Paper," http://www.prise.oew.ac.at/docs/PRISE_Statement_Paper.pdf (last accessed 18-01-2011)

- PRISE 2008a, "PRISE D6.2 Criteria for privacy enhancing security technologies," http://www.prise.oeaw.ac.at/docs/PRISE_D_6.2_Criteria_for_privacy_enhancing_security_technologies.pdf (last accessed 18-01-2011)
- Resnik, David B., 2008, "What is "Dual Use" Research? A Response to Miller and Selgelid", *Sci Eng Ethics* (2009) 15: 3-5
- Roco, Mikhail & Bainbridge, William Sims, 2003, "Nanotechnology: Societal Implications – Maximizing Benefit for Humanity," Report of National Nanotechnology Initiative Workshop, 3-5 December 2003, Arlington, VA, USA, http://www.nano.gov/nni_societal_implications.pdf (last accessed 29-10-2010)
- Roco, Mihail C. Mirkin, Chad A. & Hersham, Mark C. (eds) "Nanotechnology Research Directions for Societal Needs in 2020; Retrospective and Outlook," Springer, 2010, www.wtec.org/nano2
- Rogerson, Simon, 2011, "Why care about the Ethical Issues of Emerging ICTs?", intervention at ETICA-EGAIS-STOA workshop on IT for a Better Future, European Parliament, 31 March 2011, <http://www.etica-project.eu/>
- Schermer, Maartje, 2009, "The Mind and the Machine. On the Conceptual and Moral Implications of Brain-Machine Interaction", *Nanoethics* (2009) 3:217-230
- von Schomberg, René, 2007, "From the ethics of technology towards an ethics of knowledge policy: implications for robotics", *AI & Soc* (2008) 22:331-348
- von Schomberg, René, 2010, remarks during RISE/HIDE workshop, December 2010, www.sciencemag.org/cgi/content/full/322/5909/1800?ijkey=kd8Pitxace/l6&keytype=ref&siteid=sci
- Selgelid, Michael J., 2009, "Dual-Use Research Codes of Conduct: Lessons from the Life Sciences", *Nanoethics* (2009) 3:175-183
- Sharkey, N. (2008) The ethical frontiers of robotics. *Science* Vol 322 No 5909 pp 1800-1801 <http://www.sciencemag.org/cgi/content/full/322/5909/1800?ijkey=kd8Pitxace/l6&keytype=ref&siteid=sci>
- Sparrow, R. (2007), Killer Robots, *Journal of Applied Philosophy*, Vol.24:1, 62-77
- Stahl, Bernd, 2011, "The ETICA project," Intervention during ETICA-EGAIS-STOA workshop on IT for a Better Future, European Parliament, 31 March 2011, <http://www.etica-project.eu/>
- Steinberg, Alvin, 2010, "Nanotechnology-enabled quantum computation could fuel a security race," Foresight Institute weblog, 24 December 2010, <http://www.foresight.org/nanodot/?p=4331>
- Swierstra, Tsjalling & Boenink, Marianne, 2009, "Converging Technologies, Shifting Boundaries", *Nanoethics* (2009) 3:213-216
- Tavani, Herman 2001 The state of computer ethics as a philosophical field of inquiry: Some contemporary perspectives, future projections and current resources. *Ethics and Informations Technology 3: 97-108 Kluwer Academic Publishers.*
- Tavani, Herman 2008 ICT ethics bibliography 2006-2008: A list of recent books. *Ethics and Information Technology 10: 85-88 Springer*
- UNSC, 2004, Security Council resolution 1540, United Nations, www.un.org/sc/1540
- Vallor, Shannon, 2008, "The Ethics of IT", *Metascience* (2008) 17:283-286
- Venier, Silvia, 2010, Solutions for new trade-off model privacy-security, Current trends in nanotechnology, ICT, privacy and security, ObservatoryNano interview with Dr Silvia Venier, 15 July 2010, <http://www.observatorynano.eu/project/document/3282/>
- Vlandas, Alexis, 2006, "Managing nanotechnology," in SGR Newsletter 32, 2006, <http://www.sgr.org.uk/resources/managing-nanotechnology> (last accessed 1-3-2011)
- Wassenaar Arrangement, 2003, Best practices for implementing intangible transfer of technology controls, http://www.wassenaar.org/guidelines/docs/ITT_Best_Practices_for_public_statement.pdf (last accessed 19-07-2010)
- Whitehouse, Diana, 2011, intervention at ETICA-EGAIS-STOA workshop on IT for a Better Future, European Parliament, 31 March 2011, <http://www.etica-project.eu/>

Wittes, Benjamin, 2010, Innovation's Darker Future: Biosecurity, Technologies of Mass Empowerment and the Constitution, The future of the constitution series, number 3, Brookings Institution, Washington DC, http://www.brookings.edu/papers/2010/1208_biosecurity_wittes.aspx

WMDC, 2006, "Weapons of Terror; Freeing the World of Nuclear, Biological and Chemical Arms," Weapons of Mass Destruction Commission, www.wmdcommission.org

Wright, D, Gutwirth, S, Friedewald, M, Vildjiounaite, E, Punie, Y (eds) 2010, Safeguards in a world of ambient intelligence, Springer, <http://www.springer.com/computer/database+management+%26+information+retrieval/book/978-1-4020-6661-0> (last accessed 18-01-2011)

WWICS, 2010, Biosecurity; How synthetic biology is changing the way we look at biology and biological threats, Woodrow Wilson International Center for Scholars, Washington DC, 11 March 2010, <http://www.synbioproject.org/events/archive/biosecurity/>

Annex 1: list of issues identified in technical and economic reports by ObservatoryNano, Nov 2008, May 2009, Dec 2009

Table 4.1: Ethical and societal issues in the technical trend reports

Topic of the report	Identified issues
Agricultural production	<ul style="list-style-type: none"> - Sensor networks (for crops and livestock): potential ethical issues: privacy, dual use, balance security-freedom (not typical for agricultural applications); - Disease and pest control in crop plants: risks of residue and unintended consequences for human health and the environment, precaution; - Applying sensors and diagnostic devices for monitoring the physiological status of livestock: could reduce the need for "stamping out" infectious disease, potential benefit for animal welfare; - Intellectual property issues (proprietary technologies and knowledge may hinder innovation in e.g. nano-emulsion technology); - Genetic engineering of crops and livestock is controversial; - Agriculture as means to produce nanomaterials: competition with food-crops may lead to increased food prices and hunger (cf biodiesel), distributive justice; - Chances for green/sustainable production of (nano)materials offer potential benefits for society and the environment; - Enabling informed consumer choice for food with nano-ingredients (labelling, information); - Regulating nanotechnology in agrifood (e.g. EU Novel Food Regulation); - Improving shelf life of food by nano-enhanced packaging: sustainability, regulation /safety, privacy (RFID) issues.
Textiles technology and sector	<ul style="list-style-type: none"> - Chances for greening textiles production offer potential benefits for society and the environment (chemicals/materials/energy saving; reduced waste); - Potential unknown health/safety risks, need for life cycle analysis, precaution; - Antimicrobial applications: offers benefits as well as potential risks for health and the environment. Need for life cycle analysis, precaution; - Fear of side effects of nano-products (environmental / toxicity / allergy

	<p>issues) to some extent for Clothing, domestic and medical uses, precaution;</p> <ul style="list-style-type: none"> - Intellectual property issues (e.g. preference to licence, rather than implement) especially for medical and military uses (Cientifica, 2006); - Medical e-textiles: preventive healthcare applications change definitions of health, raising ethical issues of enhancement, choices in use of limited healthcare resources and privacy issues (also for sports).
Regenerative medicine	<ul style="list-style-type: none"> - Nanoscaffolds, tissue engineering, lab on a chip to experiment with stem cells / tissue engineering in vitro; - General biomedical ethics issues apply (c.f. NanoMed Roundtable); - Possibly enhancement issues?
Drug delivery	<ul style="list-style-type: none"> - Expected impact on the structure of the pharmaceutical industry sector: Who gains, who pays (market failure); - Patenting issues; - Risk management issues.
Diagnostics	<ul style="list-style-type: none"> - Nanobiosensors / nanowires: dual use medical / bioterrorism monitoring; - Theranostics: has potential, many questions remain (e.g. loss of control of the patient over own body).
Implants, surgery & coatings	<ul style="list-style-type: none"> - Biocompatible coatings / implant materials, electrodes in neuroimplants, battery / energy supply (transfer body heat to electricity), optical fibres for compatibility with external electromagnetic field (MRI etc), “smart knees” combined with artificial intelligence to prevent falling, implanted drug delivery system.
Novel bionano-structures	<ul style="list-style-type: none"> - Self-assembly; - Synthetic cells e.g. for drug discovery: elements, liposomes, polymers, nanoemulsions, novel fabrication techniques and nanomaterials to create cell like structures, synthetic membranes. C.f. discussion on ethical aspects of synthetic biology; - Nanosomes for cosmetics and therapeutics; - Molecular switches and molecular motors (basic research phase).
Cosmetics	<ul style="list-style-type: none"> - Nanoparticles as UV filters (TiO₂, ZnO, organic alternatives); - Nanotechnology for delivery - Risk debate, regulation, labelling (EU cosmetics regulation will be in place from 2012?)
Construction sector	<ul style="list-style-type: none"> - Precaution (worker safety)? - Use of raw materials / commodities markets? (Sustainability, distributive justice); - Sustainability issues, incl. energy saving, emission reduction in manufacturing building materials or in use; - Cooperation with or impact on socio-economic development of developing countries, distributive justice
Security	<ul style="list-style-type: none"> - Focus on terrorism, excluding other security issues including warfare and crime (but includes narcotics); - Dual use is acknowledged (detection of chemical agents incl. industrial toxins); - Cf HIDE project discussion of biometrics / Nanoforum report on nanosecurity – elsa issues; - Terahertz detectors lead to severe privacy and human rights issues if used to see through clothes of people; - What is the main market for security technologies (small shop-owners

	<ul style="list-style-type: none"> wanting to prevent theft?). - Personal Protective clothing / equipment for first responders (NBCR, firefighters): no ELSA issues identified (November 2009 report)
Environment – groundwater remediation	<ul style="list-style-type: none"> - Potential benefits for sustainable development; - Life cycle analysis needed to avoid unintended consequences, precaution. - Field testing of nano Zero Valent Iron nZVI: uncertainty about risks, possible conflicts with stakeholders (Nov 2009 report)
Environment – chemical and gas sensor	<ul style="list-style-type: none"> - Privacy issues; - Other ethical or ELSA issues depend on the application.
Chemistry & materials	<ul style="list-style-type: none"> - Precaution, risk governance
ICT- Displays	<ul style="list-style-type: none"> - Ubiquitous computing issues (privacy); - Human-machine interactions; - Life cycle analysis, precaution.

No issues were identified for ICT – Power components, Energy (incl. solar cells), Automotive & Aeronautics.

Annex 2: relevant issues in policy / stakeholder debate

Topic	Organisations	weblinks
Soldier Enhancement / human machine interactions	EGE report ICT implants	http://www.itas.fzk.de/eng/etag/etag.htm ; http://www.europarl.europa.eu/stoa/default_en.htm ; http://www.rathenau.nl/ http://ec.europa.eu/european_group_ethics/index_en.htm http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2006-0216+0+DOC+PDF+V0//EN&language=EN http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2009-0255+0+DOC+PDF+V0//EN&language=EN http://www.demos.co.uk/publications/betterhumanscollection http://ieet.org/index.php/IEET/HETHR http://www.wired.com/wired/archive/15.01/humanintro.html
Nanoelectronics, ICT, ambient intelligence and privacy	STOA, Rathenau, ITAS	www.rathenau.nl
Ethical and Societal aspects of civil security research	ESRIF vision 2009, EU funded projects: HIDE, RISE, DETECTOR, INEX, Nanoforum, CPSI Nanopodium project Nanorecht & Vrede	www.hideproject.org www.riseproject.eu www.detector.bham.ac.uk www.inexproject.eu www.nanoforum.org www.cpsi-fp7.eu
Balance security-freedom in specific cases (e.g. biometrics for border)	RISE and HIDE projects	www.hideproject.org www.riseproject.eu

control, restrictions on academic freedom and trade restrictions)		
Civil/military dual use (Biological and Chemical industry and WMD / definition dual use in case of civil security research)	KNAW code of conduct Biosecurity 3TU project BWPP / Pax Christi International	www.know.nl/biosecurity www.ethicsandtechnology.eu/research/projects/biosecurity_and_dual_use_research www.bwpp.org www.paxchristi.net
Robot ethics	Ethicbot project	http://ethicbots.na.infn.it/documents.php
Human rights / human dignity and ICT	EGE report ICT implants	http://ec.europa.eu/european_group_ethics/index_en.htm